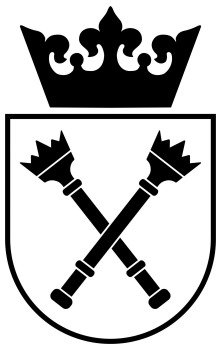
Uniwersytet Jagielloński w Krakowie

Wydział Matematyki i Informatyki



Wybrane zastosowania teorii liniowych grup algebraicznych

Justyna Porzycka

Numer albumu: 1187285

Praca magisterska
na kierunku Matematyka Komputerowa

Praca wykonana pod kierunkiem
prof. dr hab. Zbigniew Hajto
Instytut Informatyki i Matematyki Komputerowej

Kraków 2024

Spis treści

Wstęp

Celem poniższej pracy jest zdefiniowanie pojęć związanych z geometrią algebraiczną oraz przedstawienie ich w kontekście różniczkowej teorii Galois. Różniczkowa teoria Galois, będąca uogólnieniem klasycznej teorii Galois, stanowi narzędzie pozwalające na głębsze zrozumienie związków pomiędzy strukturami algebraicznymi i różniczkowymi.

Rozdział pierwszy wprowadza podstawowe pojęcia z geometrii algebraicznej oraz definicję liniowych grup algebraicznych. Grupy te mogą być postrzegane jako abstrakcyjne zbiory afiniczne. Rozdział drugi jest poświęcony różniczkowej teorii Galois, w tym zdefiniowaniu rozszerzenia Picarda-Vessiota. Różniczkowa teoria Galois bada strukturę grup automorfizmów pewnych rozszerzeń ciał różniczkowych. W rozdziale trzecim omówiono praktyczne zastosowania tej teorii. Przedstawiono, w jaki sposób różniczkowe grupy Galois mogą być widziane jako liniowe grupy algebraiczne oraz związek z twierdzeniem fundamentalnym różniczkowej teorii Galois. Dodatkowo, zdefiniowane zostały rozszerzenia Liouville'a oraz omówiono kryteria rozwiązalności różniczkowych grup Galois, co z kolei znajduje zastosowanie w rozwiązywaniu liniowych równań różniczkowych drugiego rzędu. Rozdział ten ukazuje, jak teoretyczne koncepcje mogą być zastosowane w praktycznych problemach matematyki i fizyki.

W tekście stawiany jest nacisk na precyzyjne zdefiniowanie i omówienie kluczowych pojęć oraz na ukazanie wzajemnych relacji pomiędzy różnymi obszarami matematyki. W poniższej pracy scalono podejście z kilku prac wymienionych w literaturze oraz zamieszczono niektóre dowody, które w tych pracach przedstawione zostały skrótowo bądź były pominięte.

W pracy zakłada się znajomość podstawowych pojęć z klasycznej algebry, które można znaleźć na przykład w książce autorstwa Serge'a Langa [5].

1 Zbiory afiniczne i liniowe grupy algebraiczne

1.1 Definicja przestrzeni afinicznej i zbiorów afinicznych

Niech C będzie ciałem algebraicznie domkniętym oraz niech $C[X_1, ..., X_n]$ będzie pierścieniem wielomianów n zmiennych $X_1, ..., X_n$ nad ciałem C. Przestrzenią afiniczną wymiaru n nazywamy zbiór

$$\mathbb{A}^n_C := C^n = \{(v_1, ..., v_n) : v_i \in C, i = 1, ..., n\}.$$

Odwzorowanie ewaluacji ϕ:

$$\phi : C[X_1, ..., X_n] \times \mathbb{A}^n_C \longrightarrow C$$

$$f : (v_1, ..., v_n) \mapsto f(v_1, ..., v_n)$$

Definicja 1.1.1. *Dla dowolnego $T \subseteq C[X_1, ..., X_n]$, zbiorem zer dla T nazywamy zbiór:*

$$\{P = (v_1, ..., v_n) \in \mathbb{A}^n_C : f(P) = 0 \ \forall_{f \in T}\}.$$

Definicja 1.1.2. *Dla danego wielomianu $f \in C[X_1, ..., X_n]$ definiujemy zbiór:*

$$\mathcal{V}(f) = \{P \in \mathbb{A}^n_C : f(P) = 0\}$$

Analogicznie, dla zbioru $T \subset C[X_1, ..., X_n]$ definiujemy:

$$\mathcal{V}(T) = \{P \in \mathbb{A}^n_C : f(P) = 0 \ \forall_{f \in T}\}$$

Definicja 1.1.3. *Podzbiór $Y \subset \mathbb{A}^n_C$ nazywamy **afinicznym zbiorem algebraicznym** (lub krócej: zbiorem afinicznym) w $\mathbb{A}^n_C$, jeśli istnieje zbiór $T \subset C[X_1, ..., X_n]$, taki że zachodzi:*

$$Y = \mathcal{V}(T)$$

Okazuje się, że nie musimy rozważać dowolnych podzbiorów $T \subset C[X_1, ..., X_n]$. Możemy ograniczyć się do generowanych przez nie ideałów, to znaczy:

$$J := (T) \subset C[X_1, ..., X_n].$$

Co więcej, ponieważ $C[X_1, ..., X_n]$ jest pierścieniem noetherowskim, istnieje skończona liczba wielomianów $f_1, ..., f_m$, taka że:

$$J = (f_1, ..., f_m)$$

Lemat 1.1.4. *Niech A będzie pierścieniem noetherowskim, a $J \subset A$ ideałem generowanym przez zbiór $T \subset A$, to znaczy $J = (T)$. Można wtedy ze zbioru T wybrać skończony układ generatorów dla J.*

Dowód. Niech $\mathcal{S}$ będzie zbiorem ideałów generowanych przez podzbiory skończone T, to znaczy

$$\mathcal{S} = \{(S') \mid S' \subset T \text{ oraz } S' \text{ jest skończony}\}.$$

Ponieważ A jest pierścieniem noetherowskim, to każda niepusta rodzina ideałów A posiada element maksymalny w sensie inkluzji. Niech zatem $M = (S'_0)$ gdzie S'_0 jest pewnym skończonym podzbiorem T będzie elementem maksymalnym w $\mathcal{S}$. Dla każdego elementu $s \in T$ zachodzi $M \subset (S'_0, s)$. Z maksymalności M wynika, że $M = (S'_0, s)$, czyli $s \in M$. Ponieważ s może być dowolnym elementem z T, mamy $T \subset M$, a stąd $J = (T) \subseteq M \subseteq J$. Zatem J jest generowany przez skończony podzbiór T. □

Lemat 1.1.5. *Dla T i J takich jak wyżej, zachodzi:*

$$\mathcal{V}(T) = \mathcal{V}(J) = \mathcal{V}(f_1, ..., f_m).$$

Dowód. Oczywistym jest, że $\mathcal{V}(J) \subseteq \mathcal{V}(T)$. Niech $f \in J$. Z lematu 1.1.5 wynika, że istnieją $q_1, ..., q_l \in T$ (generatory dla J) oraz $p_1, ..., p_l \in C[X_1, ..., X_n]$, takie że

$$f = q_1 p_1 + ... + q_l p_l$$

Jeśli $P \in \mathcal{V}(T)$, to $q_1(P) = ... = q_l(P) = 0$, czyli również $f(P) = 0$ i $P \in \mathcal{V}(J)$. Zatem $\mathcal{V}(T) \subseteq \mathcal{V}(J)$. Analogicznie pokazujemy, że $\mathcal{V}(J) = \mathcal{V}(f_1, ..., f_m)$. □

Zatem podzbiór $Y \subset \mathbb{A}^n_C$ jest zbiorem afinicznym w $\mathbb{A}^n_C$, jeśli jest zbiorem rozwiązań pewnego skończonego układu równań wielomianowych z $C[X_1, ..., X_n]$.

Wniosek 1.1.6. *Przyporządkowanie $\{$ideały w $C[X_1, ..., X_n]\} \mapsto \{$zbiory afiniczne w $\mathbb{A}^n_C\}$ jest surjektywne.*

Przykład 1.1.7. *Najprostszymi przykładami zbiorów afinicznych w $\mathbb{A}^n_C$ są te definiowane przez układy równań liniowych (tak zwane podprzestrzenie afiniczne). Zbiory te są izomorficzne z przestrzeniami afinicznymi.*

Okazuje się, że zbiory postaci $\mathcal{V}(I)$ generowane przez ideały w $C[X_1, ..., X_n]$ spełniają aksjomaty zbiorów domkniętych, a związaną z nimi topologię nazywamy *topologią Zariskiego*. Fakt ten umożliwia badanie afinicznych zbiorów algebraicznych jako obiektów topologicznych nad dowolnym ciałem.

Definicja 1.1.8. ***Topologia Zarskiego***

1. *Zbiorami domkniętymi w topologii Zariskiego są zbiory postaci:*

$$\mathcal{V}(I) = \{P \in \mathbb{A}^n_C : f(P) = 0 \ \forall_{f \in I}\},$$

gdzie I jest ideałem w $C[X_1, ..., X_n]$.

2. *Bazę dla zbiorów otwartych stanowią zbiory postaci:*

$$D(f) = \{P \in \mathbb{A}_C^n : f(P) \neq 0\},$$

gdzie f jest dowolnym wielomianem. Są to zatem zbiory wszystkich punktów przestrzeni afinicznej dla których wielomian f się nie zeruje. W dalszej części nazywane będą ***zbiorami otwartymi głównymi****.*

Pokażemy, że zbiory postaci:

$$\mathcal{V}(I) = \{x \in \mathbb{A}_C^n : f(x) = 0 \forall_{f \in I}\}$$

dla pewnego ideału I, faktycznie spełniają aksjomaty zbiorów domkniętych:

1. $\mathbb{A}_C^n = \mathcal{V}(0)$ oraz $\varnothing = \mathcal{V}(C[X_1, ..., X_n])$,
2. Skończona suma zbiorów domkniętych jest zbiorem domkniętym,
3. Dowolny iloczyn zbiorów domkniętych jest zbiorem domkniętym.

Dowód.

1. Ideał zerowy zawiera dokładnie jeden element - wielomian stale równy 0. Stąd dowolny $x \in \mathbb{A}_C^n$ należy do $\mathcal{V}(0)$, czyli $\mathcal{V}(0) = \mathbb{A}_C^n$.

   $\mathcal{V}(C[X_1, ..., X_n])$ to zbiór wszystkich $x \in \mathbb{A}_C^n$ będących rozwiązaniami dowolnego wielomianu z $C[X_1, ..., X_n]$. Musi być zbiorem pustym, na przykład dlatego, że do $C[X_1, ..., X_n]$ należą wielomiany stałe.

2. Weźmy dwa ideały $I, J \in C[X_1, ..., X_n]$. Chcemy pokazać, że $\mathcal{V}(I) \cup \mathcal{V}(J)$ również będzie postaci $\mathcal{V}(L)$ dla pewnego ideału L. Wiemy, że iloczyn ideałów $IJ = \{\sum_{i=1}^k f_i g_i : f_i \in I, g_i \in J, k \in \mathbb{N}_1\}$ również jest ideałem. Pokażemy, że $\mathcal{V}(I) \cup \mathcal{V}(J) = \mathcal{V}(IJ)$.

   Niech $x \in \mathcal{V}(I)$, czyli x jest rozwiązaniem dowolnego wielomianu f z I. Wtedy jeśli $f_1, ..., f_k \in I$, to x jest również rozwiązaniem wielomianu $\sum_{i=1}^k f_i g_i$ gdzie $g_1, ..., g_k \in J$. Analogicznie dla $x \in \mathcal{V}(J)$.

   Jeśli x nie należy do $\mathcal{V}(I) \cup \mathcal{V}(J)$, to znaczy, że istnieje pewien wielomian $f \in I$ oraz wielomian $g \in J$, taki że $f(x) \neq 0$ oraz $g(x) \neq 0$. Zatem $(fg)(x) \neq 0$, z czego wynika, że $x \notin \mathcal{V}(IJ)$.

3. Chcemy pokazać, że przecięcie $\bigcap_{I \in \mathcal{A}} \mathcal{V}(I)$, gdzie $\mathcal{A}$ jest dowolnie dużym zbiorem ideałów, jest również postaci $\mathcal{V}(L)$ dla pewnego ideału L. Mamy ciąg równoważności:
   $x \in \bigcap_{I \in \mathcal{A}} \mathcal{V}(I) \iff \forall I \in \mathcal{A} : x \in \mathcal{V}(I) \iff \forall I \in \mathcal{A}\, \forall f \in I : f(x) = 0 \iff \forall f \in \bigcup \mathcal{A} : f(x) = 0 \iff x \in \mathcal{V}(\bigcup \mathcal{A})$.

   Z twierdzenia Hilberta o bazie, ideał generowany przez zbiór $\bigcup \mathcal{A}$ jest skończenie generowany.

□

Definicja 1.1.9. *Niech X będzie dowolnym podzbiorem $\mathbb{A}^n_C$. Definiujemy odpowiadający mu ideał $\mathcal{I}(X) \subset C[X_1, ..., X_n]$ w następujący sposób:*

$$\mathcal{I}(X) = \{f \in C[X_1, ..., X_n] : f(x) = 0 \ \forall_{x \in X}\}.$$

Jest to zbiór wszystkich wielomianów zerujących się na zbiorze X.

Definicja 1.1.10. *Dla ideału I w pierścieniu przemiennym R definiujemy jego **radykał** $\sqrt{I}$:*

$$\sqrt{I} = \{a \in R : a^n \in I \, dla \ pewnego \ n \geqslant 1\}.$$

***Ideałem radykalnym** nazywamy ideał J dla którego $J = \sqrt{J}$. To znaczy, że jeśli dla pewnego $n > 0$, a^n należy do J, to również a należy do J.*

Lemat 1.1.11. *Ideał J pierścienia R jest ideałem radykalnym, wtedy i tylko wtedy, gdy pierścień ilorazowy R/J nie zawiera elementów nilpotentnych.*

Dowód. ($\Rightarrow$) Niech $J \subseteq R$ będzie ideałem radykalnym. Załóżmy, że dla pewnego $x \in R$ zachodzi:

$$(x + J)^n = 0_{R/J}$$

mamy wtedy, że

$$x^n + J = 0_{R/J}$$

czyli

$$x^n \in J \Rightarrow x \in J \Rightarrow x + J = 0_{R/J}.$$

($\Leftarrow$) Załóżmy, że pierścień ilorazowy R/I nie zawiera elementów nilpotentnych oraz niech $x^n \in J$. Wtedy:

$$0_{R/J} = J = x^n + J = (x + J)^n \Rightarrow x + J = 0_{R/J} \Rightarrow x \in J$$

□

Przykład 1.1.12. *Przykładem ideału radykalnego jest dowolny ideał pierwszy.*

Przykład 1.1.13. *Niech X będzie dowolnym podzbiorem $\mathbb{A}^n_C$. Ideał:*

$$\mathcal{I}(X) = \{f \in C[X_1, ..., X_n] : f(x) = 0 \ \forall_{x \in X}\}.$$

jest przykładem ideału radykalnego, ponieważ jeśli $f^n(x) = 0$ dla pewnego $n \geqslant 1$, to również $f(x) = 0$.

Twierdzenie 1.1.14. ***(Twierdzenie Hilberta o zerach)*** *Niech C będzie ciałem algebraicznie domkniętym, a $C[X_1, ..., X_n]$ pierścieniem wielomianów n zmiennych $X_1, ..., X_n$. Zachodzi:*

1. *dowolny ideał maksymalny $\mathcal{M}$ jest postaci:*

$$\mathcal{M} = (X_1 - x_1, ..., X_n - x_n) = \mathcal{I}(P),$$

   dla pewnego punktu $P = (x_1, ..., x_n) \in \mathbb{A}^n_C$,

2. *dla każdego właściwego ideału $I \subset C[X_1, ..., X_n]$, zbiór $\mathcal{V}(I)$ jest niepusty,*

3. *dla każdego ideału $I \subset C[X_1, ..., X_n]$ zachodzi*

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

Dowód powyższego twierdzenia można znaleźć w [1, str. 7].

Uwaga 1.1.15. *Założenie o domkniętości ciała jest konieczne. Weźmy na przykład ideał właściwy $(X^2 + 1)$ w $\mathbb{R}[X]$. Wtedy $\mathcal{V}(X^2 + 1) = \varnothing$. Dla ciała niekoniecznie algebraicznie domkniętego można udowodnić jedynie równoważność powyższych stwierdzeń.*

Wniosek 1.1.16. *Mamy zatem wzajemną jednoznaczność między zbiorem ideałów radykalnych w $C[X_1, ..., X_n]$, a zbiorem afinicznych podzbiorów algebraicznych w $\mathbb{A}^n_C$ zdefiniowaną przez przyporządkowania $\mathcal{V}(.)$ oraz $\mathcal{I}(.)$.*

Definicja 1.1.17. *Niepusta przestrzeń topologiczna jest **nierozkładalna**, jeśli nie można jej przedstawić jako sumy dwóch domkniętych podzbiorów właściwych lub, równoważnie, wszystkie podzbiory otwarte są gęste. Niepusty podzbiór afiniczny jest nierozkładalny, gdy nie można go przedstawić jako sumy dwóch różnych od niego podzbiorów afinicznych.*

Twierdzenie 1.1.18. *Afiniczny zbiór X w $\mathbb{A}^n_C$ jest nierozkładalny, wtedy i tylko wtedy gdy generowany przez niego ideał $\mathcal{I}(X)$ jest ideałem pierwszym.*

Dowód. ($\Leftarrow$) Załóżmy, że $X \subset \mathbb{A}^n_C$ jest rozkładalny. Można więc wybrać dwa zbiory afiniczne X_1, X_2 różne od X, takie że $X = X_1 \cup X_2$. Istnieją zatem punkty $x_1 \in X_1 \backslash X_2$, $x_2 \in X_2 \backslash X_1$ oraz wielomiany $f_1 \in \mathcal{I}(X_1)$, $f_2 \in \mathcal{I}(X_2)$, takie że $f_1(x_2) \neq 0$ oraz $f_2(x_1) \neq 0$, czyli żaden z tych wielomianów nie może należeć do $\mathcal{I}(X)$. Jednak ich iloczyn należy do $\mathcal{I}(X)$, zatem ideał $\mathcal{I}(X)$ nie może być ideałem pierwszym, co daje sprzeczność.

($\Rightarrow$) Analogicznie, załóżmy, że $X \subset \mathbb{A}^n_C$ jest nierozkładalny i weźmy $f_1, f_2 \in C[X_1, ..., X_n]$, takie że ich iloczyn $f_1 f_2$ należy do $\mathcal{I}(X)$. Zatem każdy $x \in X$ jest zerem dla f_1 lub dla f_2, z czego wynika, że $X \subset \mathcal{V}(I_1) \cup \mathcal{V}(I_2)$, gdzie I_1 jest ideałem generowanym przez f_1, I_2 przez f_2. Ale skoro X jest nierozkładalny, to musi w całości zawierać się albo w $\mathcal{V}(I_1)$ albo w $\mathcal{V}(I_2)$, skąd wynika, że albo f_1 albo f_2 należy do $\mathcal{I}(X)$, czyli $\mathcal{I}(X)$ jest ideałem pierwszym. $\square$

Ponieważ $\mathcal{I}(\mathbb{A}^n_C) = (0)$ jest ideałem pierwszym, przestrzeń $\mathbb{A}^n_C$ jest nierozkładalna. Wobec definicji 1.1.17 mamy zatem następujący:

Wniosek 1.1.19. *Zbiory otwarte w topologii Zariskiego są gęste w* $\mathbb{A}^n_C$.

Wniosek 1.1.20. *Z twierdzenia Hilberta o zerach, wniosku 1.1.16 oraz twierdzenia 1.1.18 wynika, że odwzorowania* $\mathcal{V}(.)$ *oraz* $\mathcal{I}(.)$ *wyznaczają wzajemnie jednoznaczną odpowiedniość między następującymi zbiorami:*

1. $\{$ *ideały radykalne w* $C[X_1, ..., X_n]\} \leftrightarrow \{$ *zbiory domknięte w* $\mathbb{A}^n_C$ $\}$
2. $\{$ *ideały pierwsze w* $C[X_1, ..., X_n]\} \leftrightarrow \{$ *nierozkładalne zbiory domknięte w* $\mathbb{A}^n_C$ $\}$
3. $\{$ *ideały maksymalne w* $C[X_1, ..., X_n]\} \leftrightarrow \{$ *punkty w* $\mathbb{A}^n_C$ $\}$

We wcześniejszych rozważaniach używaliśmy faktu, że pierścień $C[X_1, ..., X_n]$ jest pierścieniem noetherowskim. Istnieje kilka równoważnych definicji takiego pierścienia, jedna z nich brzmi następująco:

Definicja 1.1.21. *Pierścień* R *jest pierścieniem noetherowskim, jeśli każdy wstępujący ciąg jego ideałów*

$$I_1 \subset I_2 \subset ... \subset I_n \subset ...$$

stabilizuje się, to znaczy istnieje n_0 *dla którego zachodzi* $I_{n_0+k} = I_{n_0}$ *dla każdego* $k \geqslant 0$.

Dla każdego zstępującego ciągu zbiorów afinicznych

$$X_1 \supset X_2 \supset ... \supset X_n \supset ...$$

mamy odpowiadający mu wstępujący ciąg ideałów

$$I_1(X_1) \subset I_2(X_2) \subset ... \subset I_n(X_n) \subset ...$$

Jeśli $X_n \supsetneq X_{n+1}$ jest zawieraniem właściwym, to $I_n(X_n) \subsetneq I_n(X_{n+1})$ również jest zawieraniem właściwym. Zatem każdy zstępujący ciąg zbiorów afinicznych stabilizuje się. Z lematu Kuratowskiego-Zorna wynika, że każdy niepusty zbiór Σ zbiorów afinicznych w $\mathbb{A}^n_C$ ma element minimalny (żaden inny element zbioru Σ nie zawiera się w nim właściwie). Fakt ten pozwoli wykazać co następuje:

Twierdzenie 1.1.22. *Każdy zbiór afiniczny* $X \subset \mathbb{A}^n_C$ *można rozłożyć na sumę nierozkładalnych zbiorów afinicznych:*

$$X = X_1 \cup ... \cup X_r,$$

gdzie $X_i \not\subset X_j$ *dla* $i \neq j$. *Rozkład ten jest jednoznaczny z dokładnością do kolejności składowych sumy.*

Dowód. Wykażemy najpierw istnienie takiego rozkładu. Niech Σ będzie zbiorem wszystkich zbiorów afinicznych niedających się rozłożyć w ten sposób. Załóżmy, że $\Sigma \neq \varnothing$. Z wcześniejszych rozważań wynika, że w Σ istnieje element minimalny X. Skoro $X \in \Sigma$, to jest rozkładalny. Istnieją zatem $X_1, X_2 \subsetneq X$, takie że $X = X_1 \cup X_2$. Z minimalności X oraz tego, że $X_1, X_2 \subsetneq X$ wynika $X_1, X_2 \notin \Sigma$. Zatem X_1, X_2 mogą być rozłożone na sumę nierozkładalnych zbiorów afinicznych, co znaczy że X również ma taki rozkład. Otrzymujemy sprzeczność z $X \in \Sigma$.

Pozostaje wykazać, że rozkład ten jest jednoznaczny. Załóżmy, że istnieje inny rozkład

$$X = Y_1 \cup ... \cup Y_l,$$

taki że Y_i są nierozkładalne dla $i = 1, ..., l$ oraz $Y_i \not\subset Y_j$ dla $i \neq j$. Wtedy:

$$X_i = X_i \cap X = \bigcup_{m=1}^{l} (X_i \cap Y_m).$$

Skoro X_i jest nierozkładalny, to dla pewnego m mamy $X_i \cap Y_m = X_i$, czyli $X_i \subset Y_m$. Analogicznie można pokazać, że dla pewnego j zachodzi $Y_m \subset X_j$, więc $i = j$ oraz $X_i = Y_j$. □

1.2 Funkcje wielomianowe i morfizmy zbiorów afinicznych

Definicja 1.2.1. ***Dziedziną całkowitości*** *(pierścieniem całkowitym) nazywamy niezerowy pierścień przemienny z jedynką bez dzielników zera.*

Definicja 1.2.2. *Niech $V \subset \mathbb{A}^n_C$ będzie zbiorem afinicznym. Funkcja $f : V \to C$ jest* ***funkcją wielomianową*** *na V, jeśli istnieje wielomian $F \in C[X_1, ..., X_n]$, taki że $f(x) = F(x)$ dla każdego $x \in V$.*

Zauważmy, że wielomian F nie musi być jednoznacznie wyznaczony przez wartości jakie przyjmuje na zbiorze V. Dla $F, G \in C[X_1, ..., X_n]$ zachodzi:

$$F|_V = G|_V \iff (F - G)|_V = 0 \iff F - G \in \mathcal{I}(V).$$

Definicja 1.2.3. ***Pierścieniem współrzędnych*** *dla zbioru algebraicznego $V \subseteq \mathbb{A}^n_C$ nazywamy iloraz*

$$C[V] = C[X_1, ..., X_n] \Big/ \mathcal{I}(V).$$

Niech $f, g \in C[X_1, ..., X_n]$. Zachodzi relacja $f \sim g \pmod{\mathcal{I}(V)}$, jeśli $f(x) = g(x)$ dla wszystkich $x \in V$. Mamy:

$$C[V] = \{f \mid f : V \to C \text{ jest funkcją wielomianową}\}.$$

Z twierdzenia 1.1.18 wynika, że trzy następujące warunki są równoważne:

1. V jest nierozkładalny
2. $\mathcal{I}(V)$ jest pierwszy
3. $C[V]$ jest dziedziną całkowitości

Wcześniej rozważaliśmy związek między podzbiorami przestrzeni afinicznej $\mathbb{A}^n_C$, a ideałami w pierścieniu $C[X_1, ..., X_n]$. Pierścień $C[V]$ gra podobną rolę dla zbioru V jak $C[X_1, ..., X_n]$ dla $\mathbb{A}^n_C$. Dzięki temu, że jeśli zbiór afiniczny V jest nierozkładalny to $C[V]$ jest dziedziną całkowitości, możemy zdefiniować ciało funkcji dla V:

Definicja 1.2.4. *Niech V będzie nierozkładalnym zbiorem afinicznym.* ***Ciałem funkcji*** *dla V nazywamy ciało ułamków pierścienia $C[V]$ i oznaczamy przez $C(V)$. Elementy ciała $C(V)$ nazywamy* ***funkcjami wymiernymi*** *na V.*

Każda funkcja wymierna $f \in C(V)$ może być zapisana jako $f = \frac{g}{h}$, gdzie $g, h \in C[V]$. W ogólności nie jest to jednoznaczne przedstawienie ($C[V]$ niekoniecznie musi być pierścieniem z jednoznacznością rozkładu). Wartość funkcji f w punkcie P może być dobrze zdefiniowana jedynie w przypadku, gdy istnieje reprezentacja $f = \frac{g}{h}$, taka że $h(P) \neq 0$.

Definicja 1.2.5. *Jeśli dla funkcji $f \in C(V)$ i punktu P istnieje reprezentacja $f = \frac{g}{h}$, taka że $h(P) \neq 0$, to funkcję f nazywamy* ***funkcją regularną*** *w punkcie P.*

Definicja 1.2.6. ***Dziedziną funkcji*** *$f \in C(V)$ nazywamy zbiór wszystkich punktów w których f jest regularna:*

$$dom(f) = \{P \in V : \ f \text{ jest regularna w } P\}.$$

Uwaga 1.2.7. *Niech $V \subset \mathbb{A}^n_C$ będzie zbiorem afinicznym. Możemy rozważać topologię Zariskiego na V indukowaną przez topologię zadaną na $\mathbb{A}^n_C$. Zbiory domknięte będą postaci $\mathcal{V}(I) := \{P \in V : f(P) = 0$ dla każdego f należącego do pewnego ideału I w $C[V]\}$.*

Twierdzenie 1.2.8. *Niech V będzie zbiorem afinicznym nierozkładalnym. Dla funkcji wymiernej $f \in C(V)$ zachodzą następujące własności:*

1. *$dom(f)$ jest otwartym i gęstym podzbiorem V,*
2. *$dom(f) = V \iff f \in C[V]$,*
3. *jeśli $h \in C[V]$ oraz $V_h = \{P \in V : h(P) \neq 0$, to $dom(f) \supset V_h \iff f \in C[V][\frac{1}{h}]$.*

Dowód powyższych własności można znaleźć w [1, str. 10].

Z punktu drugiego twierdzenia 1.2.8 wynika, że funkcje wielomianowe są jedynymi funkcjami wymiernymi wszędzie regularnymi. Jeśli U jest otwartym podzbiorem nierozkładalnego zbioru algebraicznego V, to mówimy że $f \in C(V)$ jest regularna w U jeśli jest regularna w każdym punkcie tego zbioru. Zbiór funkcji wymiernych, regularnych w U tworzy podpierścień w $C(V)$. Oznaczamy go przez $\mathcal{O}_V(U)$.

Definicja 1.2.9. *Pierścieniem lokalnym zbioru algebraicznego V w punkcie P nazywamy pierścień*

$$\mathcal{O}_P := \{f \in C(V) \ : \ f \text{ jest regularna w } P\}.$$

Uwaga 1.2.10. *Jeśli V jest nierozkładalnym zbiorem afinicznym, to $C[V] = \bigcap_{P \in V} \mathcal{O}_P$. Dowód tego faktu można znaleźć w [1, str. 11].*

Jeśli V jest zbiorem afinicznym, a U jest jego otwartym podzbiorem, to funkcja $f : U \to C$ jest regularna w $x \in V$ jeżeli istnieją $g, h \in C[V]$ oraz otwarty podzbiór $U_0 \subset U$ zawierający x, taki że dla każdego $y \in U_0$ zachodzi $h(y) \neq 0$ oraz $f(y) = \frac{g(y)}{h(y)}$. Funkcja f jest regularna w zbiorze otwartym $U' \subset U$, jeżeli jest regularna w każdym punkcie tego zbioru.

Uwaga 1.2.11. *Zauważmy, że zbiory otwarte główne (czyli zbiory punktów dla których pojedynczy wielomian $f \in C[X_1, ..., X_n]$ się nie zeruje), mogą być traktowane jako zbiory afiniczne w przestrzeni $\mathbb{A}_C^{n+1}$. Jeśli $D(f) = \{P \in \mathbb{A}_C^n : f(P) \neq 0\}$ dla pewnego $f \in C[X_1, ..., X_n]$, to punkty w $D(f)$ odpowiadają jeden do jeden punktom zbioru domkniętego postaci*

$$\mathcal{V}(g) = \{(x_1, ..., x_n, x_{n+1}) \ : \ g(x_1, ..., x_n, x_{n+1}) = f(x_1, ..., x_n)x_{n+1} - 1 = 0\}.$$

Zatem $D(f)$ ma strukturę zbioru afinicznego, a jego pierścieniem współrzędnych jest $C[D(f)] = C[X_1, ..., X_n, \frac{1}{f}]$, to znaczy pierścień $C[X_1, ..., X_n]$ zlokalizowany w systemie multiplikatywnym $\{1, f, f^2, f^3, ...\}$.

Bardziej ogólnie, jeśli V jest dowolnym zbiorem afinicznym, $f \in C[V]$, to algebra funkcji regularnych na zbiorze otwartym głównym $D(f)$ jest algebrą $C[V]$ zlokalizowaną w systemie multiplikatywnym potęg f, oznaczaną przez $C[V]_f$.

Definicja 1.2.12. *Niech $V \subset \mathbb{A}_C^n$ oraz $W \subset \mathbb{A}_C^m$ będą zbiorami afinicznymi. Funkcję $\phi : V \to W$ nazywamy **morfizmem zbiorów afinicznych**, jeżeli istnieją funkcje $\phi_1, ..., \phi_m \in C[V]$, takie że dla wszystkich punktów $x = (x_1, ..., x_n) \in V$ zachodzi:*

$$\phi(x_1, ..., x_n) = (\phi_1(x), ..., \phi_m(x)) \in W \subset \mathbb{A}_C^m.$$

Lemat 1.2.13. *Morfizm zbiorów afinicznych $\phi : V \to W$ jest ciągły w topologii Zariskiego.*

Dowód. Trzeba pokazać, że jeśli $Z \subset W$ jest zbiorem domkniętym, to $f^{-1}(Z)$ również. Niech $Z = \{h_1 = ... = h_r = 0\}$. Wtedy $f^{-1}(Z) = \{h_1 \circ f = ... = h_r \circ f = 0\}$ i także jest zbiorem domkniętym. □

Niech $V \subset \mathbb{A}_C^n$, $W \subset \mathbb{A}_C^m$ oraz $X \subset \mathbb{A}_C^l$ będą zbiorami afinicznymi. Niech ponadto $\phi : V \to W$ będzie morfizmem zbiorów afinicznych. Dla $g \in C[W]$ definiujemy $\phi^*(g) = g \circ \phi$. Ponieważ g jest funkcją wielomianową, to $g \circ f$ również jest funkcją wielomianową.

Mamy odwzorowanie:

$$\phi^* : \ C[W] \to C[V]$$

$$g \mapsto \phi^*(g) = g \circ \phi$$

Jeśli $\phi : V \to W$ $\psi : W \to X$ są morfizmami zbiorów afinicznych oraz $h \in C[X]$, to mamy:

$$(\psi \circ \phi)^*(h) = h \circ (\psi \circ \phi) = (h \circ \psi) \circ \phi = \phi^*(h \circ \psi) = \phi^*(\psi^*(h)),$$

zatem:

$$(\psi \circ \phi)^* = \phi^* \circ \psi^* : C[X] \to C[V].$$

Odwzorowanie ϕ^* jest homomorfizmem pierścieni:

$$\phi^*(g_1 + g_2) = (g_1 + g_2) \circ \phi = (g_1 \circ \phi) + (g_2 \circ \phi) = \phi^*(g_1) + \phi^*(g_2),$$

$$\phi^*(g_1 \cdot g_2) = (g_1 + g_2) \cdot \phi = (g_1 \circ \phi) \cdot (g_2 \circ \phi) = \phi^*(g_1) \cdot \phi^*(g_2).$$

Co więcej, dla każdej stałej $c \in C$ mamy $\phi^*(c) = c$, zatem każdy morfizm zbiorów afinicznych $\phi : V \to W$ definiuje homomorfizm C-algebr $\phi^* : C[W] \to C[V]$. Prawdziwy jest również następujący lemat:

Lemat 1.2.14. *Jeśli $\phi^* : C[W] \to C[V]$ jest homomorfizmem C-algebr, to istnieje dokładnie jeden morfizm zbiorów afinicznych $f : V \to W$, taki że $\phi = f^*$.*

Dowód powyższego lematu można znaleźć w [3, str. 42].

Wniosek 1.2.15. *Istnieje bijekcja między zbiorami:*

$$\{f \mid f : V \to W \text{ - } \textit{morfizm zbiorów afinicznych}\} \leftrightarrow$$

$$\leftrightarrow \{\phi \mid \phi^* : C[W] \to C[V] \text{ - } \textit{homomorfizm } C\textit{-algebr}\}$$

$$f \mapsto f^*.$$

Definicja 1.2.16. *Morfizm zbiorów afinicznych $\phi : V \to W$ jest izomorfizmem, jeśli istnieje morfizm $\psi : W \to V$, taki że $\phi \circ \psi = id_W$ oraz $\psi \circ \phi = id_V$. Zbiory afiniczne V, W są izomorficzne, gdy istnieje izomorfizm $\phi : V \to W$.*

Lemat 1.2.17. *Odwzorowanie wielomianowe $\phi : V \to W$ jest izomorfizmem zbiorów afinicznych wtedy i tylko wtedy gdy $\phi^* : C[W] \to C[V]$ jest izomorfizmem C-algebr.*

Dowód. Wynika to z faktu, że $\psi^* \circ \phi^* = (\phi \circ \psi)^*$. □

1.3 Abstrakcyjne zbiory afiniczne

Definicja 1.3.1. *Niech X będzie przestrzenią topologiczną. Funkcję $\mathcal{F}$ która zbiorowi otwartemu $U \subset X$ przyporządkowuje C-algebrę $\mathcal{F}(U)$ funkcji o wartościach w C na U nazywamy* ***snopem funkcji****, gdy spełnione są następujące warunki:*

1. *jeśli $U_0 \subset U$ są dwoma zbiorami otwartymi oraz $f \in \mathcal{F}(U)$, to zawężenie $f_{|_{U_0}}$ należy do $\mathcal{F}(U_0)$,*

2. *niech zbiór $\{U_i\}_{i\in I}$ będzie pokryciem otwartym zbioru U oraz dane będą funkcje $f_i \in \mathcal{F}(U_i)$, takie że dla każdej pary indeksów $i, j \in I$ zachodzi $f_i = f_j$ na zbiorze $U_i \cap U_j$. Wtedy istnieje funkcja $f \in \mathcal{F}(U)$, taka że jej zawężenie do dowolnego U_i równe jest f_i.*

Definicja 1.3.2. *Parę $(X, \mathcal{O}_X)$, gdzie X jest przestrzenią topologiczną, a $\mathcal{O}_X$ jest zdefiniowanym na niej snopem funkcji, nazywamy* ***przestrzenią geometryczną****.*

Definicja 1.3.3. *Niech $(X, \mathcal{O}_X)$ i $(Y, \mathcal{O}_Y)$ będą przestrzeniami geometrycznymi. Morfizmem przestrzeni geometrycznych nazywamy ciągłe odwzorowanie*

$$\phi \ : \ (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y),$$

takie że dla dowolnego podzbioru otwartego $U \subset Y$ oraz każdej funkcji $f \in \mathcal{O}_Y(U)$, funkcja $\phi^*(f) := f \circ \phi$ należy do $\mathcal{O}_X(\phi^{-1}(U))$.

Przykład 1.3.4. *Niech V będzie nierozkładalnym zbiorem afinicznym. Każdemu niepustemu zbiorowi otwartemu $U \subset V$ przyporządkowujemy pierścień regularnych funkcji wymiernych $\mathcal{O}_V(U)$. Wtedy $(V, \mathcal{O}_V(U))$ jest przestrzenią geometryczną. Istotnie, jeśli $U_0 \subset U$ oraz $f \in \mathcal{O}_X(U)$ (czyli f jest regularna w każdym punkcie U), to f jest regularna w każdym punkcie U_0 i $f_{|_{U_0}} \in \mathcal{O}_X(U_0)$. Skoro V jest zbiorem nierozkładalnym, to zbiory otwarte w V są w nim gęste, a dwie funkcje wymierne równe na takim zbiorze otwartym są równe.*

Uwaga 1.3.5. *Niech $(X, \mathcal{O}_X)$ będzie przestrzenią geometryczną, a Z podzbiorem X z topologią indukowaną. Możemy wtedy dla dowolnego zbioru otwartego $V \subset Z$ zdefiniować $\mathcal{O}_Z(V)$ w następujący sposób: odwzorowanie $f : V \to C$ należy do $\mathcal{O}_Z(V)$ wtedy i tylko wtedy, gdy istnieje pokrycie otwarte $V = \cup_i V_i$ w Z, takie że dla każdego indeksu i zachodzi $f|_{V_i} = g_i|_{V_i}$ dla pewnego $g_i \in \mathcal{O}_X(U_i)$, gdzie U_i jest otwartym podzbiorem X zawierającym V_i. Zauważmy, że jeśli Z jest zbiorem otwartym w X, to podzbiór $V \subset Z$ jest otwarty w Z wtedy i tylko wtedy, gdy jest otwarty również w X. Mamy w tej sytuacji równość $\mathcal{O}_X(V) = \mathcal{O}_Z(V)$.*

Uwaga 1.3.6. *Niech X będzie przestrzenią topologiczną, a $X = \cup_i U_i$ będzie jej pokryciem zbiorami otwartymi. Jeśli dane mamy snopy funkcji $\mathcal{O}_{U_i}$ na U_i dla każdego i, zgadzające się na przecięciach $U_i \cap U_j$ dla dowolnych i oraz j, to możemy zdefiniować $\mathcal{O}_X$ na X 'sklejając' snopy $\mathcal{O}_{U_i}$. Niech $U \subset X$ będzie podzbiorem otwartym. Wtedy $\mathcal{O}_X(U)$ zawiera wszystkie funkcje na U, których restrykcje do zbiorów $U \cap U_i$ należą do $\mathcal{O}_{U_i}(U \cap U_i)$.*

Niech $(X, \mathcal{O}_X)$ będzie przestrzenią geometryczną i niech $x \in X$. Przez v_x oznaczamy odwzorowanie idące ze zbioru funkcji o wartościach w C na zbiorze X do zbioru C, takie że:

$$v_x(f) = f(x).$$

Definicja 1.3.7. *Przestrzeń geometryczna $(X, \mathcal{O}_X)$ nazywana jest **abstrakcyjnym zbiorem afinicznym**, jeśli spełnia następujące warunki:*

1. *$\mathcal{O}_X(X)$ jest skończenie generowaną C-algebrą, a odwzorowania z X do zbioru $Hom_C(\mathcal{O}_X(X), C)$ morfizmów C-algebr, zdefiniowane jako $x \mapsto v_x$ są bijekcjami,*

2. *dla każdej $f \in \mathcal{O}_X(X), f \neq 0$ zbiór*

$$X_f := \{x \in X \ : \ f(x) \neq 0\}$$

jest otwarty oraz każdy otwarty zbiór w X jest sumą pewnych zbiorów postaci X_f,

3. *$\mathcal{O}_X(X_f) = \mathcal{O}_X(X)_f$, gdzie $\mathcal{O}_X(X)_f$ oznacza C-algebrę $\mathcal{O}_X(X)$ zlokalizowaną w f.*

Twierdzenie 1.3.8. *Każdy abstrakcyjny zbiór afiniczny jest izomorficzny (jako przestrzeń geometryczna) z afinicznym zbiorem wraz ze snopem funkcji regularnych.*

Dowód. Niech $(X, \mathcal{O}_X)$ będzie abstrakcyjnym zbiorem afinicznym. Z podpunktu c) definicji 1.3.7 wiemy, że $\mathcal{O}_X(X)$ jest skończenie generowaną C-algebrą, możemy więc zapisać

$$\mathcal{O}_X(X) = C[X_1, ..., X_n]/I,$$

dla pewnego ideału I. Elementami $\mathcal{O}_X(X)$ są funkcje na X o wartościach z ciała C, czyli $\mathcal{O}_X(X)$ nie zawiera niezerowych elementów nilpotentnych. Z lematu 1.1.11 wynika więc, że ideał I jest ideałem radykalnym, to znaczy $I = \sqrt{I}$.Korzystając z twierdzenia Hilberta o zerach (twierdzenie 1.1.14 c)), możemy utożsamić $\mathcal{O}_X(X)$ z pierścieniem funkcji regularnych na $\mathcal{V}(I)$:

$$\mathcal{O}_X(X) = C[X_1, ..., X_n]/\sqrt{I} = C[X_1, ..., X_n]/\mathcal{I}(\mathcal{V}(I)) = C[\mathcal{V}(I)].$$

Weźmy morfizm $\phi : C[\mathcal{V}(I)] \to C$. Z pierwszego twierdzenia o izomorfizmie wiemy, że z

$$C[\mathcal{V}(I)]/ker\phi \cong C.$$

Skoro C jest ciałem, to $ker\phi$ musi być ideałem maksymalnym w $C[\mathcal{V}(I)]$. Zatem morfizmowi ϕ odpowiada ideał maksymalny w $C[\mathcal{V}(I)]$. Ponownie korzystając z twierdzenia Hilberta o zerach (twierdzenie 1.1.14 a)), wiemy że każdemu ideałowi maksymalnemu odpowiada punkt z $\mathcal{V}(I)$. Stąd i z własności 1. definicji 1.3.7 mamy odpowiedniość:

$$\{x \in X\} \leftrightarrow \{\phi \mid \phi : C[\mathcal{V}(I)] \to C\} \leftrightarrow \{v \in \mathcal{V}(I)\}.$$

Utożsamiamy więc $\mathcal{V}(I)$ oraz X jako zbiory. Bazą topologii Zariskiego na $\mathcal{V}(I)$ są zbiory otwarte główne, zatem z podpunktu 2. definicji 1.3.7 wynika, że zbiory $\mathcal{V}(I)$ i X są w istocie homeomorficzne. Dzięki własności 3. możemy utożsamić $\mathcal{O}_X(X_f)$ z pierścieniem funkcji regularnych na zbiorze otwartym głównym X_f. To wystarczy, by utożsamić $\mathcal{O}_X(U)$ z pierścieniem funkcji regularnych na U, gdzie U jest dowolnym zbiorem otwartym. □

Uwaga 1.3.9. *Można również pokazać, że każdy zbiór afiniczny ze snopem funkcji regularnych jest abstrakcyjnym zbiorem afinicznym. Powyższy argument pokazuje, że zbiór afiniczny jest w całości opisany przez swoją algebrę funkcji regularnych i odwrotnie.*

1.4 Liniowe grupy algebraiczne

Definicja 1.4.1. *Niech C będzie ciałem algebraicznie domkniętym oraz $G \subseteq \mathbb{A}^n_C$ będzie zbiorem afinicznym wyposażonym w strukturę grupy, to znaczy działanie $\phi : G \times G \to G$ gdzie $\phi(x, y) = xy$, element odwrotny $e \in G$ oraz $\sigma : G \to G$, gdzie $\sigma(x) = x^{-1}$ spełniają aksjomaty grupy. Zbiór G nazywamy afiniczną grupą algebraiczną nad ciałem C jeśli odwzorowania ϕ oraz σ są morfizmami zbiorów afinicznych.*

Uwaga 1.4.2. *Przez $M(n, C)$ oznaczać będziemy zbiór wszystkich macierzy $n \times n$ o elementach z C. Zbiór ten możemy utożsamić z przestrzenią afiniczną wymiaru n^2.*

Definicja 1.4.3. ***Pełną grupą liniową*** *$GL(n, C) \subset M(n, C)$ nazywamy grupę wszystkich odwracalnych macierzy $n \times n$ o elementach z C z działaniem mnożenia macierzy.*

Twierdzenie 1.4.4. *Niech C będzie ciałem algebraicznie domkniętym. Grupa $GL(n, C) \subset M(n, C)$ jest izomorficzna jako abstrakcyjny zbiór afiniczny z podzbiorem afinicznym w przestrzeni $\mathbb{A}^{n^2+1}$.*

Dowód. Zauważmy, że skoro $GL(n, C)$ jest podzbiorem $M(n, C)$, gdzie wyznacznik jest różny od zera, to $GL(n, C)$ możemy traktować jako zbiór otwarty główny w przestrzeni $\mathbb{A}^{n^2}$. Zauważmy jednak, że naturalna projekcja $M(n, C) \times \mathbb{A}^1 \to M(n, C)$ jest bijekcją między zbiorem afinicznych zbiorów afinicznych postaci

$$X := \{(A, \lambda) : \lambda detA = 1\},$$

a zbiorem $GL(n, C)$. Zbiór $GL(n, C)$ będzie zatem afinicznym zbiorem w przestrzeni $\mathbb{A}^{n^2+1}$. Pierścieniem współrzędnych tego zbioru afinicznego stanowią zawężenia funkcji X_{ij} o n^2 zmiennych razem z $\frac{1}{det(X_{ij})}$,

$$C[X_{11}, ..., X_{nn}, t] \Big/ (tdet - 1) \cong C[X_{11}, ..., X_{nn}][det^{-1}].$$

Można łatwo pokazać, że macierz odwrotna jest dana przez wzięcie wielomianu na każdym elemencie macierzy, podobnie jak wynik mnożenia. Zatem operacje mnożenia i odwrotność macierzy są morfizmami zbiorów afinicznych. □

Uwaga 1.4.5. *Dowolna podgrupa afinicznej grupy algebraicznej, domknięta w topologii Zariskiego również jest afiniczną grupą algebraiczną.*

Definicja 1.4.6. ***Liniową grupą algebraiczną*** *nazywamy domkniętą podgrupę $GL(n, C)$.*

Przykład 1.4.7. *Przykładami liniowych grup algebraicznych są:*

1. $SL(n, C) := \{A \in GL(n, C) : detA = 1)$ *- specjalna grupa liniowa,*
2. $T(n, C) := \{(a_{ij}) \in GL(n, C) : a_{ij} = 0, i > j\}$ *- grupa macierzy trójkątnych górnych,*
3. $U(n, C) := \{(a_{ij}) \in GL(n, C) : a_{ii} = 1, a_{ij} = 0, i > j\}$ *- grupa macierzy trójkątnych górnych unipotentnych,*
4. $D(n, C) := \{(a_{ij}) \in GL(n, C) : a_{ij} = 0, i \neq j\}$ *- grupa diagonalna.*

Niech G będzie liniową grupą algebraiczną. Istnieje tylko jedna nierozkładalna składowa grupy G zawierająca element neutralny e. W istocie, niech $X_1, ..., X_m$ będą rozłącznymi, nieredukowalnymi składowymi zawierającymi e. Obraz nierozkładalnego zbioru afinicznego $X_1 \times ... \times X_m$ poprzez morfizm produktowy jest nierozkładalnym podzbiorem $X_1 \cdots X_m$ grupy G, który ponownie zawiera e. Zatem $X_1 \cdots X_m$ jest zawarte w pewnym X_i. Z drugiej strony, każda ze składowych $X_1, ..., X_m$ również jest zawarta w $X_1 \cdots X_m$. Zatem m musi być równe 1.

Definicja 1.4.8. *Opisaną powyżej składową grupy G zawierającą element neutralny e nazywamy składową jedynki grupy G i oznaczamy przez G^0.*

2 Rożniczkowe grupy Galois

2.1 Ciało różniczkowe i derywacja

Definicja 2.1.1. ***Derywacją pierścienia*** *A nazywamy odwzorowanie $d : A \to A$, takie że zachodzi*

$$d(a + b) = da + db$$

oraz

$$d(ab) = d(a)b + ad(b).$$

Przez a' oznaczamy $d(a)$, kolejne derywacje oznaczamy przez $a'', a''', ..., a^{(n)}$.

Definicja 2.1.2. ***Pierścieniem różniczkowym*** *nazywamy przemienny pierścień z jednością wraz z derywacją.* ***Ciałem różniczkowym*** *nazywamy pierścień różniczkowy który jest ciałem.*

Przykład 2.1.3. *Pierścień wszystkich funkcji klasy C^∞ na prostej rzeczywistej ze zwykłą pochodną jest pierścieniem różniczkowym.*

Przykład 2.1.4. *Niech A będzie pierścieniem różniczkowym, a $A[X]$ będzie pierścieniem wielomianów jednej zmiennej nad A. Derywacja w $A[X]$ powinna spełniać:*

$$(\sum a_i X^i)' = \sum (a_i' X^i + a_i i X^{i-1} X').$$

Możemy wtedy rozszerzyć derywację w A do $A[X]$ przypisując X' dowolną wartość w $A[X]$. Analogicznie postępujemy dla ciała. Iteracyjnie możemy również nadać strukturę różniczkową pierścieniowi $A[X_1, ..., X_n]$.

Przykład 2.1.5. *Niech A będzie pierścieniem różniczkowym. Możemy zdefiniować derywację w pierścieniu $M(n, A)$. Niech $B \in M(n, A)$. Wówczas $d(B)$ będzie równe macierzy uzyskanej poprzez zaaplikowanie derywacji z pierścienia A do każdego elementu macierzy B. Wtedy $M(n, A)$, gdzie $n \geqslant 2$, jest pierścieniem nieprzemiennym z derywacją.*

W dowolnym pierścieniu różniczkowym, elementy jądra odwzorowania d, czyli takie dla których derywacja równa jest zero, tworzą podpierścień C, nazywany **pierścieniem stałych**. Jeśli A jest ciałem, to C również.

2.2 Rozszerzenia różniczkowe i pierścień operatorów różniczkowych

Definicja 2.2.1. *Niech A, B będą pierścieniami różniczkowymi. Inkluzję $A \subset B$ nazywamy **rozszerzeniem pierścieni różniczkowych**, jeśli derywacja w B zawęża się do derywacji w A. Analogicznie definiujemy **rozszerzenie ciał różniczkowych** $K \subset L$.*

Definicja 2.2.2. *Niech L będzie rozszerzeniem różniczkowym ciała K. Dowolny automorfizm $\phi : L \to L$ będziemy nazywać **K-automorfizmem**, gdy $\phi|_K = id_K$. Jeśli ponadto ϕ zachowuje pochodną, to znaczy dla każdego $a \in L$ zachodzi:*

$$\phi(da) = d\phi(a),$$

*to ϕ nazywamy **K-automorfizmem różniczkowym**.*

Definicja 2.2.3. *Niech L będzie rozszerzeniem różniczkowym ciała K oraz $a \in L$. Niezerowy, unormowany wielomian $P \in K[X]$ nazywamy wielomianem minimalnym elementu a, jeśli a jest pierwiastkiem P oraz każdy wielomian $g \in K[X]$ różny od P dla którego zachodzi $g(a) = 0$ ma stopień wyższy od stopnia P.*

Definicja 2.2.4. *Niech L będzie rozszerzeniem algebraicznym ciała K. Element $a \in L$ nazywamy **elementem rozdzielczym** nad ciałem K, jeśli jego wielomian minimalny nie ma pierwiastków wielokrotnych. Rozszerzenie L ciała K nazywamy rozdzielczym jeśli każdy element $a \in L$ jest rozdzielczy nad K.*

Twierdzenie 2.2.5. *(O elemencie prymitywnym) Niech $a_1, ..., a_n$ są rozdzielcze względem ciała K. Istnieje wtedy element α rozdzielczy względem K, taki że $K\langle a_1, ..., a_n\rangle = K\langle\alpha\rangle$.*

Dowód tego faktu można znaleźć w [5, str. 243].

Twierdzenie 2.2.6. *Jeśli L jest rozdzielczym rozszerzeniem różniczkowym ciała K, to derywacja w K rozszerza się jednoznacznie na L. Ponadto każdy K-automorfizm jest K-automorfizmem różniczkowym.*

Dowód. Jeśli $K \subset L$ jest rozszerzeniem skończonym, to z twierdzenia 2.2.5 wynika, że istnieje α, takie że zachodzi $L = K\langle\alpha\rangle$. Niech $P(X)$ będzie wielomianem minimalnym elementu α nad K. Różniczkując $P(\alpha) = 0$, otrzymujemy $P^{(d)}(\alpha) + P'(\alpha)\alpha' = 0$, gdzie $P^{(d)}$ oznacza wielomian uzyskany z P poprzez różniczkowanie jego współczynników, a P' oznacza zróżniczkowany wielomian. Zatem $\alpha' = \frac{-P^{(d)}(\alpha)}{P'(\alpha)}$ oraz derywacja rozszerza się jednoznacznie.

Mamy $L \cong K[X]\big/(P)$. Możemy rozszerzyć derywację z K na $K[X]$ poprzez zdefiniowanie $X' := -P^{(d)}(X)h(X)$ dla $h(X) \in K[X]$, takiego że $h(X)P'(X) \equiv 1 \mod P$. Jeśli $h(X)P'(X) = 1 + k(X)P(X)$, to zachodzi

$$\begin{aligned} d(P(X)) &= P^{(d)}(X) + P'(X)d(X) \\ &= P^{(d)}(X) + P'(X)(-P^{(d)}(X)h(X)) \\ &= P^{(d)}(X)(1 - P'(X)h(X)) \\ &= -P^{(d)}(X)k(X)P(X). \end{aligned}$$

Zatem (P) jest różniczkowym ideałem, a $K[X]\big/(P)$ jest pierścieniem różniczkowym.

Jeśli σ jest K-automorfizmem L, to $\sigma^{-1}d\sigma$ również jest derywacją L, rozszerzając jednoznacznie tą z K otrzymujemy $\sigma^{-1}d\sigma = d$, zatem $d\sigma = \sigma d$, czyli σ jest K-automorfizmem różniczkowym. □

Uwaga 2.2.7. *Od tego momentu wszystkie rozważane ciała będą charakterystyki zerowej.*

Definicja 2.2.8. *Niech K będzie ciałem różniczkowym z nietrywialną derywacją.* ***Różniczkowym operatorem liniowym $\mathcal{L}$*** *ze współczynnikami w K nazywamy wielomian zmiennej D:*

$$\mathcal{L} = a_n D^n + a_{n-1}D^{n-1} + ... + a_1 D + a_0,$$

gdzie $a_i \in K$.

Pierścień liniowych operatorów różniczkowych ze współczynnikami w K jest nieprzemiennym pierścieniem $K[D]$ wielomianów o zmiennej D ze współczynnikami w K, gdzie D spełnia:

$$Da = a' + aD,$$

dla $a \in K$. Z operatorem różniczkowym $\mathcal{L} = a_n D^n + a_{n-1} D^{n-1} + ... + a_1 D + a_0$ kojarzymy równanie różniczkowe:

$$\mathcal{L}(Y) = a_n Y^n + a_{n-1} Y^{n-1} + ... + a_1 Y + a_0 = 0.$$

Rozważmy liniowe równanie różniczkowe rzędu n nad różniczkowym ciałem K z ciałem stałych C:

$$\mathcal{L}(Y) = a_n Y^n + a_{n-1} Y^{n-1} + ... + a_1 Y + a_0 = 0, a_i \in K.$$

Jeśli $K \subset L$ jest rozszerzeniem różniczkowym, to zbiór rozwiązań $\mathcal{L}(Y) = 0$ w L jest przestrzenią C_L-wektorową, gdzie C_L oznacza ciało stałych dla L. Można wykazać, że wymiar tej przestrzeni jest równy co najwyżej n.

Definicja 2.2.9. *Niech $y_1, ..., y_n \in K$. Wyznacznik*

$$W = W(y_1, y_2, ..., y_n) = \begin{vmatrix} y_1 & y_2 & ... & y_n \\ y_1' & y_2' & ... & y_n' \\ . & . & ... & . \\ . & . & ... & . \\ . & . & ... & . \\ y_1^{n-1} & y_2^{n-1} & ... & y_n^{n-1} \end{vmatrix}$$

nazywamy ***wrońskianem*** *dla $y_1, ..., y_n$.*

Twierdzenie 2.2.10. *Niech K będzie ciałem różniczkowym z ciałem stałych C oraz niech $y_1, ..., y_n \in K$. Wtedy $y_1, ..., y_n$ są liniowo niezależne nad C wtedy i tylko wtedy, gdy $W(y_1, y_2, ..., y_n) \neq 0$.*

Dowód powyższego twierdzenia można znaleźć w [1, str. 126]

Twierdzenie 2.2.11. *Niech $\mathcal{L}(Y) = 0$ będzie liniowym równaniem różniczkowym rzędu n nad ciałem różniczkowym K. Jeśli $y_1, ..., y_{n+1}$ są rozwiązaniami $\mathcal{L}(Y) = 0$ w rozszerzeniu różniczkowym L ciała K, to*

$$W(y_1, y_2, ..., y_{n+1}) = 0.$$

Dowód. Niech $y_1, ..., y_{n+1}$ będą rozwiązaniami $\mathcal{L}(Y) = 0$. We wrońskianie

$$W(y_1, y_2, ..., y_n, y_{n+1}) = \begin{vmatrix} y_1 & y_2 & ... & y_n & y_{n+1} \\ y_1' & y_2' & ... & y_n' & y_{n+1}' \\ . & . & ... & . & \\ . & . & ... & . & \\ . & . & ... & . & \\ y_1^{n-1} & y_2^{n-1} & ... & y_n^{n-1} & y_{n+1}^{n-1} \\ y_1^n & y_2^n & ... & y_n^n & y_{n+1}^n \end{vmatrix}$$

ostatnim wierszem jest $(y_1^{(n)}, ..., y_{n+1}^{(n)})$, co stanowi kombinacje liniową poprzednich.

□

Wniosek 2.2.12. *Równanie $\mathcal{L}(Y) = 0$ rzędu n ma co najwyżej n rozwiązań w L liniowo niezależnych nad ciałem stałych.*

Definicja 2.2.13. *Niech $\mathcal{L}(Y) = 0$ będzie liniowym równaniem różniczkowym rzędu n nad ciałem różniczkowym K oraz niech $y_1, ..., y_n$ będą rozwiązaniami $\mathcal{L}(Y) = 0$, liniowo niezależnymi nad ciałem stałych w rozszerzeniu różniczkowym L ciała K. Wtedy zbiór:*

$$\{y_1, ..., y_n\}$$

*nazywamy **fundamentalnym zbiorem rozwiązań** dla $\mathcal{L}(Y) = 0$ w L. Każde inne rozwiązanie $\mathcal{L}(Y) = 0$ jest kombinacją liniową $y_1, ..., y_n$ ze stałymi współczynnikami.*

2.3 Rozszerzenie Picarda-Vessiota i rożniczkowe grupy Galois

Definicja 2.3.1. *Niech $\mathcal{L}(Y) = 0$ będzie liniowym równaniem różniczkowym rzędu n nad ciałem różniczkowym K. Rozszerzenie różniczkowe $K \subset L$ nazywamy **rozszerzeniem Picarda-Vessiota** dla $\mathcal{L}$, jeśli:*

1. *$L = K\langle y_1, ..., y_n\rangle$, gdzie $y_1, ..., y_n$ jest bazowym zbiorem rozwiązań $\mathcal{L}(Y) = 0$ w L,*
2. *każda stała ciała L należy do K, to znaczy $C_L = C_K$.*

Definicja 2.3.2. *Jeśli $K \subset L$ jest rozszerzeniem różniczkowym, to grupa $G(L|K)$ różniczkowych K-automorfizmów ciała L nazywana jest **różniczkową grupą Galois** rozszerzenia $K \subset L$. Jeśli dodatkowo L jest rozszerzeniem Picarda-Vessiota ciała K dla $\mathcal{L}(Y) = 0$, to grupa $G(L|K)$ różniczkowych K-automorfizmów ciała L nazywana jest **grupą Galois równania** $\mathcal{L}(Y) = 0$ **nad** K. Oznaczamy ją przez $Gal_K(\mathcal{L})$.*

Przykład 2.3.3. *Rozważmy rozszerzenie różniczkowe $L = K\langle\alpha\rangle$, gdzie $\alpha' = a \in K$, takie że a nie jest pochodną w K. Mówimy wtedy, że L jest uzyskane z K przez **rozszerzenie całkowe**. Chcemy udowodnić, że α jest elementem przestępnym nad K, $K \subset K\langle\alpha\rangle$ jest rozszerzeniem Picarda-Vessiota oraz że $G(K\langle\alpha\rangle|K)$ jest izomorficzna z grupą addytywną $C = C_K$.*

Załóżmy, że α jest elementem algebraicznym nad K oraz niech $P(X) = X^n + \sum_{i=1}^{n} b_i X^{n-i}$ będzie wielomianem minimalnym elementu α nad K. Wtedy $0 = P(\alpha) = \alpha^n + \sum_{i=1}^{n} b_i \alpha^{n-i} \Rightarrow 0 = n\alpha^{n-1}a + b_1'\alpha^{n-1} +$ wyrazy stopnia mniejszego niż $n-1 \Rightarrow na + b_1' = 0 \Rightarrow a = (\frac{-b_1}{n})'$, co daje sprzeczność.

Pokażemy teraz, że $K\langle\alpha\rangle$ nie zawiera nowych stałych. Załóżmy, że wielomian $\sum_{i=0}^{n} b_i\alpha^{n-i}$, gdzie $b_i \in K$ jest stały. Różniczkując, otrzymujemy $0 = b_0'\alpha^n + (nb_0a + b_1')\alpha^{n-1} +$ wyrazy stopnia mniejszego niż $n-1 \Rightarrow b_0' = nb_0a + b_1' = 0 \Rightarrow a = \frac{-b_1'}{nb_0} = (\frac{-b_1}{nb_0})'$, co daje sprzeczność z tym, że a nie jest pochodną

w K. Załóżmy, że funkcja wymierna $\frac{f(\alpha)}{g(\alpha)}$ jest stała, g jest minimalny, stopnia większego lub równego 1. Różniczkując, otrzymujemy

$$0 = \frac{f(\alpha)'g(\alpha)a - f(\alpha)g(\alpha)'a}{g(\alpha)^2} \Rightarrow \frac{f(\alpha)}{g(\alpha)} = \frac{f(\alpha)'}{g(\alpha)'},$$

gdzie $g(\alpha)'$ jest niezerowym wielomianem stopnia niższego niż stopień g, ponieważ $g(\alpha)$ nie jest stałą oraz g jest unormowany. Daje to sprzeczność.

Zauważmy, że 1 oraz α są rozwiązaniami dla $Y'' - \frac{a'}{a}Y' = 0$, liniowo niezależnymi nad ciałem stałych. Zatem $K \subset K\langle\alpha\rangle$ jest rozszerzeniem Picarda-Vessiota.

Różniczkowy K-automorfizm ciała $K\langle\alpha\rangle$ przenosi α na $\alpha + c$, gdzie $c \in C$, a odwzorowanie $\alpha \mapsto \alpha + c$ indukuje różniczkowy K-automorfizm ciała $K\langle\alpha\rangle$, dla każdego $c \in C$. Zatem

$$G(K\langle\alpha\rangle|K) \cong C \cong \left\{ \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \right\} \subset GL(2, C).$$

Przykład 2.3.4. *Rozważmy rozszerzenie różniczkowe $L = K\langle\alpha\rangle$, takie że $\alpha'/\alpha = a \in K\backslash\{0\}$. Mówimy wtedy, że L jest uzyskane z K przez* ***rozszerzenie wykładnicze****. Oczywistym jest, że $K\langle\alpha\rangle = K(\alpha)$, a $\{\alpha\}$ jest fundamentalnym zbiorem rozwiązań równania różniczkowego $Y' - aY = 0$. Zakładamy, że $C_L = C_K$. Wykażemy, że jeśli α jest elementem algebraicznym nad K to $\alpha^n \in K$ dla pewnego n naturalnego.*

Załóżmy zatem, że α jest elementem algebraicznym nad K oraz niech $P(X) = X^n + a_{n-1}X^{n-1} + ... + a_0$ będzie jego wielomianem minimalnym. Różniczkując, otrzymujemy

$$\begin{aligned} 0 &= P(\alpha)' \\ &= P^{(d)}(\alpha) + P'(\alpha)\alpha' \\ &= P^{(d)}(\alpha) + P'(\alpha)a\alpha \\ &= an\alpha^n + \sum_{k=0}^{n-1}(a_k' + aka_k)\alpha^k. \end{aligned}$$

Wtedy P dzieli ostatni wielomian oraz $a_k' + aka_k = ana_k \Rightarrow a_k' = a(n-k)a_k$, gdzie $0 \leqslant k \leqslant n-1$. Zatem $(\alpha^{n-k}/a_k)' = 0$. W szczególności, $\alpha^n = ca_0$ dla pewnego $c \in C_L = C_K$. Wtedy $P(X)$ dzieli $X^n - ca_0 \in K[X]$, czyli $P(X) = X^n - ca_0$.

Dla $\sigma \in G(L|K)$ zachodzi

$$\sigma(\alpha)' = \sigma(\alpha') = \sigma(a\alpha) = a\sigma(\alpha) \Rightarrow (\sigma(\alpha)/\alpha)' = 0 \Rightarrow \sigma(\alpha) = c\alpha,$$

dla pewnego $c \in C_L = C_K$. Jeśli α jest elementem przestępnym nad K, to dla każdego $c \in C_K$ możemy zdefiniować różniczkowy K-automorfizm ciała L jako $\alpha \mapsto c\alpha$. Jeśli $\alpha^n = b \in K$, to

$$(c\alpha)^n = \sigma(\alpha)^n = \sigma(\alpha^n) = \sigma(b) \Rightarrow c^n = 1,$$

skąd wynika, że c jest n-tym pierwiastkiem z jedności, a $Gal(L|K)$ jest skończoną grupą cykliczną.

3 Teoria Galois rozszerzeń Picarda-Vessiota

3.1 Różniczkowe grupy Galois jako liniowe grupy algebraiczne

Twierdzenie 3.1.1. *Niech K będzie ciałem różniczkowym z ciałem stałych C, a $L = K < y_1, ..., y_n >$ będzie rozszerzeniem Picarda-Vessiota ciała K. Wtedy istnieje zbiór S wielomianów $F(X_{ij})$, $1 \leqslant i, j \leqslant n$ ze współczynnikami w C, taki że zachodzi:*

1. *jeśli σ jest K-automorfizmem L oraz $\sigma(y_j) = \sum_{i=1}^{n} c_{ij} y_i$, to $F(c_{ij}) = 0$ dla każdego $F \in S$,*
2. *dla macierzy $c_{ij} \in GL(n, C)$, takiej że dla każdego $F \in S$ zachodzi $F(c_{ij}) = 0$, istnieje różniczkowy K-automorfizm σ ciała L, taki że $\sigma(y_j) = \sum_{i=1}^{n} c_{ij} y_i$.*

Dowód powyższego twierdzenia można znaleźć w [1, str. 145].

Wniosek 3.1.2. *Istnieje zatem zbiór S wielomianów z $C[X_{11}, ..., X_{nn}]$, taki że $G(L|K) = \{(c_{11}, ..., c_{nn}) \in GL(n, C) : f(c_{11}, ..., c_{nn}) = 0, f \in S\}$. Zatem $G(L|K)$ jest domkniętą w topologii Zariskiego podgrupą $GL(n, C)$, czyli liniową grupą algebraiczną.*

3.2 Twierdzenie fundamentalne różniczkowej teorii Galois

Niech $K \subset L$ będzie rozszerzeniem Picarda-Vessiota oraz niech F będzie podciałem różniczkowym, to znaczy $K \subset F \subset L$. Wtedy również $F \subset L$ jest rozszerzeniem Picarda-Vessiota (dla tego samego równania różniczkowego, zdefiniowanego nad F), z grupą Galois $G(L|F) = \{\sigma \in G(L|K) : \sigma_{|F} = Id_F\}$. Jeśli H jest podgrupą $G(L|K)$, to przez L^H oznaczamy podciało L ustalone przez działanie H, to znaczy $L^H = \{x \in L : \sigma(x) = x, \forall \sigma \in H\}$.

Twierdzenie 3.2.1. *Niech $K \subset L$ będzie rozszerzeniem Picarda-Vessiota z grupą Galois $G(L|K)$.*

1. *Istnieje wzajemnie jednoznaczna, odwracające inkluzję odpowiedniość*

$$H \mapsto L^H, \ F \mapsto G(L|K)$$

między domkniętymi w topologii Zariskiego podgrupami $H \in G(L|K)$, a podciałami różniczkowymi $K \subset F \subset L$.

2. *Podciało różniczkowe F jest rozszerzeniem Picarda-Vessiota ciała K wtedy i tylko wtedy, gdy podgrupa $H = G(L|F)$ jest podgrupą normalną w $G(L|K)$. Co więcej, restrykcja*

$$G(L|K) \to G(F|K)$$

$$\sigma \mapsto \sigma_{|F}$$

indukuje izomorfizm $G(L|K)/G(L|F) \cong G(F|K)$.

Dowód tego twierdzenia można znaleźć w [1, str. 158].

3.3 Rozszerzenia Liouville'a

Celem tego rozdziału jest scharakteryzowanie liniowych równań różniczkowych rozwiązalnych za pomocą kwadratur. Będzie to analogią do charakteryzacji równań algebraicznych rozwiązalnych przez pierwiastniki. Zostaną również przytoczone konieczne definicje dotyczące rozwiązalności grupy.

Definicja 3.3.1. *Rozszerzenie różniczkowe ciał $K \subset L$ nazywamy **rozszerzeniem Liouville'a** jeśli istnieje ciąg różniczkowych ciał pośrednich $K = F_1 \subset ... \subset F_n = L$, takich że F_{i+1} jest uzyskane z F_i albo przez rozszerzenie całkowe albo rozszerzenie wykładnicze.*

Definicja 3.3.2. *Niech G będzie grupą oraz $\alpha, \beta \in G$. **Komutatorem** elementów α, β nazywamy $(\alpha, \beta) = \alpha\beta\alpha^{-1}\beta^{-1}$. Wprost z definicji wynika, że zachodzi $\gamma(\alpha, \beta)\gamma^{-1} = (\gamma\alpha\gamma^{-1}, \gamma\beta\gamma^{-1})$ dla $\gamma \in G$. **Komutantem zbiorów** A, B nazywamy podgrupę $[A, B] \subset G$ generowaną przez wszystkie komutatory (α, β), takie że $\alpha \in A, \beta \in B$. **Komutantem grupy** G nazywamy $[G, G]$ i oznaczamy przez $G^{(1)}$. Indukcyjnie, n-ty komutant grupy G definiujemy jako $G^{(n+1)} = [G^{(n)}, G^{(n)}]$.*

Uwaga 3.3.3. *Niech G będzie grupą oraz niech H będzie podgrupą G zawierającą $G^{(1)}$, $p, g \in G$. Wtedy G/H jest przemienna, ponieważ jeśli $gH, pH \in G/H$, to zachodzi:*

$$gHpH = gpH = gp(p^{-1}, g^{-1})H = pgH = pHgH.$$

Z kolei jeśli G/H jest przemienna (gdzie H jest normalna), to H zawiera $G^{(1)}$ ponieważ

$$pgp^{(-1)}g^{(-1)}H = gpp^{(-1)}g^{(-1)}H = H.$$

Definicja 3.3.4. *Grupa G jest rozwiązalna, jeśli istnieje $n \in \mathbb{N}$ takie że $G^{(n)} = \{e_G\}$.*

Definicja 3.3.5. *Ciąg $G = G_0 \supset G_1 \supset ... \supset G_m = \{e_G\}$ podgrup grupy G nazywamy łańcuchem normalnym, jeśli G_{i+1} jest podgrupą normalną G_i dla $0 \leqslant i \leqslant m-1$.*

Twierdzenie 3.3.6. *Niech G będzie grupą. Następujące warunki są równoważne:*

1. *G jest rozwiązalna,*
2. *istnieje ciąg $G = G_0 \supset G_1 \supset ... \supset G_m = \{e_G\}$ podgrup normalnych grupy G, takich że G_i/G_{i+1} jest przemienna dla $0 \leqslant i \leqslant m-1$,*
3. *istnieje łańcuch normalny $G = G_0 \supset G_1 \supset ... \supset G_m = \{e_G\}$ podgrup grupy G, taki że G_i/G_{i+1} jest przemienna dla $0 \leqslant i \leqslant m-1$.*

Dowód. Dla $1 \Rightarrow 2$ weźmy $G_i = G^{(i)}$. Jeśli $G = G_0 \supset G_1 \supset ... \supset G_m = \{e_G\}$ jest ciągiem podgrup normalnych grupy G, to oczywistym jest, że G_{i+1} jest normalna w G_i $(0 \leqslant i \leqslant m-1)$, skąd wynika $2 \Rightarrow 3$. Ostatecznie, przy założeniach z podpunktu 3, skoro G_i/G_{i+1} jest przemienna to z uwagi 3.3.3 wynika, że G_{i+1} zawiera $G_i^{(1)}$. Indukcyjnie otrzymujemy $G^{(i)} \subset G_i$ dla każdego i. □

Uwaga 3.3.7. *Przykładem grupy nierozwiązalnej jest specjalna grupa liniowa $SL(n, C) = G$, gdzie $n > 1$ oraz C zawiera co najmniej 4 elementy. W [5, str. 539, 541] można znaleźć dowód, że $SL(n, C)$ dla $n > 1$ równa jest swojemu komutantowi, skąd mamy że $G^{(i)} = G$ dla dowolnego $i \in \mathbb{N}$.*

Kolejne twierdzenie klasyfikuje podgrupy liniowej grupy specjalnej $SL(2, C)$. W pracy Kovacica [7] znajduje zastosowanie w rozwiązywaniu liniowych równań różniczkowych drugiego rzędu. Po zmianie zmiennych eliminującej Y', równanie ma postać $Y'' + RY = 0$ gdzie $R \in C$. Okazuje się, że różniczkowa grupa Galois takiego równania przyjmuje jedną z czterech postaci. Trzy z nich to podgrupy $SL(2, C)$. Ostatnią możliwością jest sama grupa $SL(2, C)$.

Twierdzenie 3.3.8. *Niech G będzie podgrupą grupy $SL(2, C)$. Zachodzi jedna z następujących możliwości:*

1. *G jest triangularyzowalna,*
2. *G jest sprzężona z podgrupą grupy*

$$D^+ = \left\{ \begin{pmatrix} c & 0 \\ 0 & c^{-1} \end{pmatrix} : c \in C, c \neq 0 \right\} \cup \left\{ \begin{pmatrix} 0 & c \\ -c^{-1} & 0 \end{pmatrix} : c \in C, c \neq 0 \right\}$$

   oraz 1. *nie zachodzi,*

3. *G jest skończona oraz* $1., 2.$ *nie zachodzą,*

4. $G = SL(2, C)$.

Dowód powyższego twierdzenia można znaleźć w [1, str. 104].

Uwaga 3.3.9. *Twierdzenie 3.3.6 znajduje zastosowanie przy określaniu czy dana grupa jest rozwiązalna. Na przykład dla grupy G z punktu* 2. *twierdzenia 3.3.8 weźmy podgrupę* $G_1 = \left\{ \begin{pmatrix} c & 0 \\ 0 & c^{-1} \end{pmatrix} : c \in C, c \neq 0 \right\}$. *Jest to podgrupa o indeksie* 2, *zatem jak łatwo można sprawdzić,* G_1 *jest podgrupą normalną w* G, *a* G/G_1 *jest przemienna. Podobnie z* $G_2 = \{e_G\} \subset G_1$ *i* G_1/G_2. *Zatem z twierdzenia 3.3.6 wynika, że G jest rozwiązalna.*

Twierdzenie 3.3.10. *Niech L będzie rozszerzeniem Liouville'a różniczkowego ciała K oraz niech* $C_L = C_K$. *Wtedy różniczkowa grupa Galois* $G(L|K)$ *jest rozwiązalna.*

Dowód na podstawie przykładów 2.3.3 oraz 2.3.4 można znaleźć w [1, str. 159].

Definicja 3.3.11. *Niech* $K \subset L$ *będzie rozszerzeniem ciał różniczkowych. Jeśli dla każdego* $a \in L \backslash K$ *istnieje* $\sigma \in G(L|K)$, *takie że* $\sigma(a) \neq a$, *to rozszerzenie nazywamy* ***normalnym****.*

Twierdzenie 3.3.12. *Niech* $K \subset L$ *będzie rozszerzeniem normalnym ciał różniczkowych. Załóżmy, że istnieją elementy* $u_1, ..., u_n \in L$, *takie że dla każdego różniczkowego automorfizmu* σ *ciała L zachodzi:*

$$\sigma u_j = a_{1j}u_1 + ... + a_{j-1,j}u_{j-1} + a_{jj}u_j, \ j = 1, ..., n, \tag{1}$$

gdzie a_{ij} *są stałymi w L, zależnymi od* σ. *Wtedy* $K\langle u_1, ..., u_n\rangle$ *jest rozszerzeniem Liouville'a ciała K.*

Dowód powyższego twierdzenia można znaleźć w [1, str. 159].

3.4 Uogólnione rozszerzenia Liouville'a

Definicja 3.4.1. *Rozszerzenie różniczkowe ciał* $K \subset L$ *nazywamy* ***uogólnionym rozszerzeniem Liouville'a*** *jeśli istnieje ciąg różniczkowych ciał pośrednich* $K = F_1 \subset ... \subset F_n = L$, *takich że* F_{i+1} *jest uzyskane z* F_i *przez rozszerzenie całkowe, rozszerzenie wykładnicze lub* F_{i+1} *jest algebraiczne nad* F_i. *Rozwiązanie równania różniczkowego zdefiniowanego nad ciałem różniczkowym K jest* ***typu Liouville'a****, jeśli należy do uogólnionego rozszerzenia Liouville'a ciała K.*

Twierdzenie 3.4.2. *Niech K będzie ciałem różniczkowym z domkniętym algebraicznie ciałem stałych C oraz niech L będzie rozszerzeniem Picarda-Vessiota ciała K. Załóżmy, że składowa jedynki* G_0 *grupy* $G = G(L|K)$ *jest rozwiązalna. Wtedy L może być uzyskane z K przez skończone rozszerzenie normalne, po którym następuje rozszerzenie Liouville'a.*

Dowód można znaleźć w [1, str. 160].

Prawdziwe jest również twierdzenie odwrotne:

Twierdzenie 3.4.3. *Niech K będzie ciałem różniczkowym z domkniętym algebraicznie ciałem stałych C oraz niech L będzie rozszerzeniem Picarda-Vessiota ciała K. Załóżmy, że istnieje różniczkowe ciało M, takie że $L \subset M$ oraz M jest uogólnionym rozszerzeniem Liouville'a bez nowych stałych. Wtedy składowa jedynki G_0 grupy $G = G(L|K)$ jest rozwiązalna. Zatem korzystając z twierdzenia 3.4.2, L może być uzyskane z K przez skończone rozszerzenie normalne, po którym następuje rozszerzenie Liouville'a.*

Dowód można znaleźć w [1, str. 161].

Zakończenie

Teoria Picarda-Vessiota jest bezpośrednim uogólnieniem klasycznej wielomianowej teorii Galois. W przypadku rozszerzeń algebraicznych ciał różniczkowych obie teorie są całkowicie zgodne. Twierdzenie 2.2.6 wskazuje, że w obu przypadkach grupy Galois są identyczne. Ponadto, różniczkowa teoria Galois umożliwia badanie rozszerzeń przestępnych, które w naturalny sposób pojawiają się w zastosowaniach związanych z całkowalnością systemów dynamicznych. Rozszerzenia Liouville'a (rozdział 3) formalizują pojęcie rozwiązań równań różniczkowych w kwadraturach i znajdują liczne zastosowania w mechanice teoretycznej.

Powyższe zastosowania można znaleźć między innymi w rozdziale 10 (napisanym przez Juana Moralesa-Ruiza) książki [8] oraz monografii [9], jak również w klasycznej monografii Michèle Audin [10].

Literatura

[1] T. Crespo, Z. Hajto: *Algebraic Groups and Differential Galois Theory*, Graduate Studies in Mathematics 122. Providence, American Mathematical Society (2011)

[2] A. Białynicki-Birula: *Wykłady z geometrii algebraicznej*, Instytut Matematyczny Polskiej Akademii Nauk, Tom 1, Warszawa (2013)

[3] K. Hulek: *Elementary Algebraic Geometry*, Student Mathematical Library. 20. Providence, American Mathematical Society (2003)

[4] M.F.Atiyah, I. G. Macdonald: *Introduction to Commutative Algebra*, Reading, Mass.-Menlo Park, Calif.-London-Don Mills, Ont.: Addison-Wesley Publishing Company (1969)

[5] S. Lang: *Algebra. 3rd revised ed.*, Graduate Texts in Mathematics. 211. New York, NY: Springer. xv, 914 p. (2002)

[6] P. Tauvel, R.W.T Yu: *Lie algebras and algebraic groups*, Springer Monographs in Mathematics. Berlin: Springer (ISBN 3-540-24170-1/hbk). xvi, 653 p. (2005)

[7] J. J. Kovacic: *An algorithm for solving second order linear homogeneous differential equations*, JYACC Inc., 919 Third Avenue, New York, NY 10022 (1986)

[8] T. Crespo, Z. Hajto: *Introduction to differential Galois theory (Monograph with an appendix by Juan J. Morales-Ruiz)* Cracow University of Technology Press, Cracow (2007)

[9] J.J. Morales: *Differential Galois Theory and Non-Integrability of Hamiltonian Systems* Birkhäuser, Basel (1999)

[10] Michèle Audin: *Hamiltonian Systems and Their Integrability* American Mathematical Society, Société Mathématique de France (2008)