

Grupy i algebry Liego, wykład 11

W. Hebisch

13 grudnia 2025

1 Struktura algebr

Przypominam że na wykładzie 7 i 8 zdefiniowaliśmy przestrzenie pierwiastkowe dla działania algebry nilpotentnej na przestrzeni V . Dziś będziemy potrzebować wariant tego dla działania ad gdy N jest nilpotentną podalgebrą A .

Lemat 1.1 *Niech A będzie skończenie wymiarową algebrą Liego nad ciałem algebraicznie domkniętym K zaś N nilpotentną podalgebrą A . Piszemy*

$$A_\lambda = \{a \in A : \forall n \in N \exists k (\text{ad}_n - \lambda)^k(a) = 0\}$$

gdzie λ przebiega funkcje z N w K (jeśli K jest charakterystyki 0 to można ograniczyć λ do funkcji liniowych, czyli do przestrzeni dualnej do N). Wtedy

$$A = \bigoplus_\lambda A_\lambda.$$

Ponadto $N \subset A_0$, $[A_\alpha, A_\beta] \subset A_{\alpha+\beta}$.

Dowód: Sam rozkład to wynik w wykładu 7. To że $N \subset A_0$ wynika bezpośrednio z definicji nilpotentności N . A więc pozostaje pokazać że jeśli $a \in A_\alpha$, $b \in A_\beta$, $n \in N$ to $(\text{ad}_n - \alpha(n) - \beta(n))^m([a, b]) = 0$ dla $m = 2 \dim(A)$. Jednakże mamy wariant wzoru Leibniza:

$$(\text{ad}_n - \alpha(n) - \beta(n))^m([a, b]) = \sum_{k=0}^m \binom{m}{k} [(\text{ad}_n - \alpha(n))^k(a), (\text{ad}_n - \beta(n))^{m-k}(b)].$$

Ten wariant łatwo pokazać przez indukcję i z niego wynika równość wyżej: co najmniej jedna z liczb k i $m - k$ jest większa lub równa $\dim(A)$, co oznacza że jeden z argumentów komutatora znika, czyli cała suma znika. $\square$

Rozkład wyżej wymaga ciała algebraicznie domkniętego, ale przestrzeń A_0 jest dobrze zdefiniowana nad dowolnym ciałem.

Lemat 1.2 *Niech A będzie skończenie wymiarową algebrą Liego nad ciałem K zaś N nilpotentną podalgebrą A . Wtedy*

$$A = A_0 \oplus V$$

gdzie A_0 jest jak wyżej. Przy tym $[A_0, A_0] \subset A_0$, $[A_0, V] = V$.

Dowód: Niech $W_0 = A$, $W_{i+1} = [N, W_i]$. Bierzemy $V = W_{\dim(A)}$. Zauważmy że jeśli K jest ciałem algebraicznie domkniętym to działa Lemat 1.1. Dla ustalonego $\alpha \neq 0$ istnieje $n \in N$ taki że $\alpha(n) \neq 0$, wtedy ad_n jest odwracalny na A_α , czyli $[N, A_\alpha] = A_\alpha$. A więc dla

$$U = \bigoplus_{\alpha \neq 0} A_\alpha$$

mamy $[N, U] = U$. Wynika stąd że dla każdego i mamy $U \subset W_i$. Dla $n \in N$ operator ad_n jest nilpotentny na A_0 , a więc na mocy twierdzenia Engela można wybrać bazę A_0 tak by wszystkie ad_n miały postać trójkątną górną z zerami na diagonalu. Wtedy iterowany komutator $[N, \dots, [N, A_0]] = 0$, skąd wynika że dla $n \geq \dim(A_0)$ mamy $A_0 \cap W_n = \{0\}$. To oznacza że $V = W_{\dim(A)} = U$ i że $A = A_0 \oplus V$. Relacja $[A_\alpha, A_\beta] \subset A_{\alpha+\beta}$ oznacza że $[A_0, V] \subset V$.

Rozważmy teraz przypadek ogólnego K . Wtedy W_i możemy wyliczać nad K . Niech $\bar{K}$ będzie algebraicznym domknięciem K i $A_{\bar{K}}$ będzie algebrą otrzymaną z A przez rozszerzenie skalarów do $\bar{K}$. Oczywiście podprzestrzenie W_k wyliczane nad K są podzbiorami W_k wyliczanego nad $\bar{K}$. Ponadto baza W_k wyliczanego nad K pozostaje bazą W_k wyliczanego nad $\bar{K}$. A więc $V = A \cap V_{\bar{K}}$ i podobnie dla A_0 , co daje $A = A_0 \oplus V$ i $[A_0, A_0] \subset A_0$ i $[A_0, V] = V$ $\square$

Definicja. Powiemy że podalgebra $C \subset A$ jest podalgebrą Cartana wtedy i tylko wtedy gdy C jest nilpotentna i $A_0 = C$ gdzie A_0 jest przestrzenią z rozkładu wyżej.

Komentarz: Równoważnie C jest podalgebrą nilpotentną i jest swoim własnym normalizatorem, tzn. $C = N(C)$ gdzie normalizator definiujemy wzorem

$$N(C) = \{x \in A : \text{ad}_x(C) \subset C\}.$$

Inny warunek, równoważny gdy ciało K ma co najmniej $\dim(A)$ elementów to warunek że C jest podalgebrą nilpotentną i istnieje element w $T \in C$ taki że ad_T daje na A/C operator odwracalny.

Definicja wyżej jest dostosowana do badania dowolnych skończenie wymiarowych algebr Liego nad dostatecznie dużymi ciałami. Przy badaniu algebr półprostych często używa się inną definicję.

Lemat 1.3 *Niech A będzie skończenie wymiarową algebrą Liego nad ciałem R . Jeśli S/R jest rozszerzeniem ciał i C jest podalgebrą Cartana w A wtedy i tylko wtedy gdy C_S jest podalgebrą Cartana w A_S .*

Dowód Zauważmy że C jest nilpotentna wtedy i tylko wtedy gdy C_S jest nilpotentna. W dowodzie lematu 1.2 pokazaliśmy że rozkład wyliczony nad R po rozszerzeniu skalarów da rozkład wyliczany nad domknięciem algebraicznym R . Ten sam argument działa dla dowolnych rozszerzeń ciał. Ale równość $A_0 = C$ oznacza że C jest podalgebrą Cartana, co daje wynik. $\square$

Lemat 1.4 *Niech A będzie skończenie wymiarową algebrą Liego nad ciałem R nieskończonym lub skończonym mocy q z $q \geq \dim(A)$. Wtedy A zawiera podalgebrę Cartana. Ponadto każda podalgebra Cartana zawiera element c taki że ad_c jest odwracalny na A/C .*

Dowód Najpierw udowodnimy drugą część gdy ciało algebraicznie domkniętego. Niech $\alpha \neq 0$. Wtedy istnieje $c \in C$ taki że $\alpha(c) \neq 0$. Oznacza to że ad_c jest odwracalny na A_α . Mianowicie, mamy

$$\text{ad}_c = \alpha(c)(I + \frac{1}{\alpha(c)}(\text{ad}_c - \alpha(c)I))$$

Operator $N = \frac{1}{\alpha(c)}(\text{ad}_c - \alpha(c)I)$ jest nilpotentny na A_α , więc szereg $\sum_{k=0}^{\infty} (-1)^k N^k$ redukuje się do skończonej sumy która daje odwrotność $I + N$, a więc i ad_c na A_α .

Jeśli $\text{ad}(c)$ jest odwracalny na V_α , to wyznacznik $d_\alpha(c)$ ograniczenia $\text{ad}(c)$ do V_α jest niezerowy. $d_\alpha(c)$ jest wielomianem na C , niezerowym skoro istnieje c w którym on jest niezerowy. Produkt $p(c) = d_\alpha(c)$ po niezerowych α daje wyznacznik ad_c ograniczonego do

$$V = \oplus_{\alpha \neq 0} A_\alpha$$

czyli również wyznacznik ad_c działającego na A/C . $p(c)$ jako produkt niezerowych wielomianów jest niezerowy, a zakładamy tu że ciało jest algebraicznie domknięte, więc istnieje $c \in C$ takie że $p(c) \neq 0$. Wtedy ad_c działający na A/C ma niezerowy wyznacznik, a więc jest odwracalny. Daje to drugą część dla algebraicznie domkniętego R . Ogólnie, jeśli R jest dowolne to możemy wyliczać wielomian $p(c)$ nad R , a więc jest on niezerowy. Wyznacznik ma stopień równy wymiarowi przestrzeni, w naszym przypadku wymiarowi A/C , który jest mniejszy niż $\dim(A)$. Jako że ciało R ma co najmniej $\dim(A)$ elementów, to niezerowy wielomian nie może dać funkcji zerowej na C , a więc istnieje $c \in C$ takie że $p(c) \neq 0$, co daje drugą część w pełnej ogólności.

By pokazać istnienie algebr Cartana dla $T \in A$ rozpatrujemy przestrzeń

$$T_0 = \{a \in A : \exists k \text{ ad}_T(x)^k = 0\}.$$

W notacji używanej wcześniej byłoby to A_0 , ale w przypadku T_0 interesuje nas zależność od T i dlatego tak piszemy a nie A_0 . Dla konsekwencji niżej będziemy też pisać T_λ .

Wybieramy T tak by wymiar l przestrzeni T_0 był minimalny. Twierdzimy że T_0 jest podalgebrą Cartana w A . Po pierwsze, l nie zależy od tego czy je wyliczamy dla $T \in A$ czy $T \in A_S$. Mianowicie, wymiar T_0 to krotność wartości własnej 0 w wielomianie charakterystycznym T , czyli $\dim(T_0) \geq k$ wtedy i tylko wtedy gdy współczynniki przy λ^i w $\det(\text{ad}_T - \lambda)$ znikają dla $i = 0, \dots, k$. Współczynnik $c_i(T)$ przy λ^i to wielomian od współrzędnych T stopnia $\dim(A) - i$. Zauważmy że $c_0(T)$ znika tożsamościowo, bo T jest w jądrze ad_T czyli $c_0(T) = \det(T) = 0$. Dla $i > 0$, jeśli $c_i(T)$ znika na A to ponieważ ciało R ma co najmniej $\dim(A)$ elementów a stopień $c_i(T)$ jest mniejszy niż $\dim(A)$, to $c_i(T)$ znika jako wielomian, czyli znika też na A_S .

A więc istnienie $T \in C$ takie że wymiar T_0 jest minimalny gdy minimum liczymy dla A_S gdzie S jest domknięciem algebraicznym R . Na mocy już udowodnionej części wystarczy pokazać że $(T_0)_S$ jest podalgebrą Cartana w A_S . Dla ciała algebraicznie domkniętego stosuje się Lemat 1.1 (jednowymiarowa algebra rozpinana przez T jest nilpotentną podalgebrą A), czyli

$$A = (T_0) \oplus V$$

gdzie

$$V = \oplus_{\lambda \neq 0} T_\lambda.$$

Na mocy Lematu 1.1 T_0 jest podalgebrą, ponadto $[T_0, T_\lambda] \subset T_\lambda$ i konsekwentnie $[T_0, V] \subset V$. Dla elementu $U \in T_0$ niech $w(U)$ oznacza wyznacznik $\text{ad}(U)$ obciętego do V . Zauważmy że $T \in T_0$ i $w(T) \neq 0$. A więc w nie znika tożsamościowo. Jeśli $w(U) \neq 0$ to U jest odwracalny na V , czyli $U_0 \subset T_0$. Jednakże wymiar T_0 jest minimalny możliwy, więc dla takich U mamy $U_0 = T_0$. Niech teraz $v(U)$ będzie dowolnym elementem macierzy dającej $\text{ad}(U)^n$ obcięty do T_0 . Pokazaliśmy że $w(U) \neq 0$ implikuje $v(U) = 0$, czyli $wv = 0$. Jednakże pierścień wielomianów nie ma dzielników zera i $w \neq 0$, czyli $v = 0$. Skoro v był dowolnym elementem macierzy $\text{ad}(U)^n$ obciętego do T_0 , to $\text{ad}(U)^n = 0$ na T_0 czyli $T_0 \subset U_0$. Oznacza to że algebra $C = T_0$ jest nilpotentna. $T \in C$, w więc w rozkładzie z lematu 1.1 dla C mamy $A_0 \subset T_0 = C$. Nilpotentność C daje $C \subset A_0$, czyli łącznie $C = A_0$, a więc drugi warunek definicji podalgebry Cartana jest spełniony. $\square$

Jeśli N spełnia $N = A_0$ to $A/N \approx V$ gdzie $V = \oplus_{\lambda \neq 0} A_\lambda$. Jeśli dla $T \in N$ mamy $\lambda(T) \neq 0$ to ad_T jest odwracalny na A_λ , czyli wyznacznik $w_\lambda(T)$ operatora ad_T obciętego do A_λ nie jest zerowy. Wyznacznik w operatora ad_T obciętego do V jest produktem wyznaczników w_λ , więc jest niezerowym wielomianem. A więc istnieje $T \in N$ taki że $w(T) \neq 0$. Ale to oznacza że ad_T jest odwracalny na V , czyli również na A/N , czyli N jest podalgebrą Cartana. $\square$

Uwaga: Z naszej definicji widać że podalgebra Cartana jest takiej postaci jak w dowodzie twierdzenia o istnieniu, tzn. istnieje $T \in C$ taki że

$$C = \{a \in A : \exists_k \text{ad}_T^k(a) = 0\}.$$

Takie T nazywa się *elementami regularnymi*.

Uwaga: Często stosuje się inne definicje i argumentując jak w powyższych lematkach można pokazać że dla algebr skończenie wymiarowych i ciała które ma co najmniej $\dim(A)$ elementów dają one ten sam wynik.

W naszym instytucie badano grupy będące produktami półprostymi grupy abelowej i nilpotentnej, zapisywane zwykle AN . Taka grupa jest rozwiązalna. Naturalne jest pytanie czy dowolną grupę rozwiązalną da się tak zapisać, a jeśli nie to jak "daleko" jest dowolna grupa rozwiązalna od grup tej postaci. Podalgebra Cartana daje tu odpowiedź: mamy

$$A = C + [A, A]$$

i $N = [A, A]$ jest nilpotentna. A więc ogólnie zamiast abelowego C musimy dopuszczać nilpotentne C . Może się też zdarzyć że $C \cap [A, A] \neq \{0\}$ czyli suma nie jest prosta. Ale dla wielu rozumowań ten rozkład jest prawie tak dobry jak suma prosta. Jednym z naturalnych założeń jest że niezerowe zespolone λ odpowiadające nietrywialnym A_λ są zawarte w zbiorze S zamkniętym na dodawanie i nie zawierającym zera ("stożku właściwym"). Wtedy $V = \oplus_{\lambda \neq 0} A_\lambda$ jest ideałem nilpotentnym w A i rozkład

$$A = C \oplus V$$

jest przedstawieniem A jako produktu półprostego algebr. Zauważmy że dla algebry rzeczywistej λ występują w parach sprzężonych, suma A_λ dla dwu sprzężonych λ daje podprzestrzeń rzeczywistą i V również jest rzeczywiste. Ponadto warunek na stożek zależy tylko od części rzeczywistych λ .

Pokazaliśmy istnienie podalgebr Cartana, naturalne jest pytanie o jednoznaczność. Widać że może istnieć wiele różnych podalgebr Cartana. Pokażemy że w przypadku ciała algebraicznie domkniętego charakterystyki 0 wszystkie podalgebry Cartana są sprzężone. Dokładniej, jeśli $x \in A$ i ad_x jest operatorem nilpotentnym, to $\exp(\text{ad}_x)$ jest automorfizmem A . Automorfizm który jest produktem automorfizmów postaci $\exp(\text{ad}_x)$ (z nilpotentnym ad_x) nazywamy automorfizmem elementarnym. Automorfizmy elementarne tworzą grupę, jest to dokładnie grupa generowana przez automorfizmy postaci $\exp(\text{ad}_x)$ z nilpotentnym ad_x .

Komentarz: Definicja $\exp(\text{ad}_x)$ zawiera dzielenie, dlatego zakładamy charakterystykę 0. Widać że wystarczyłaby charakterystyka większa od wymiaru algebry, a z dowodu widać że wystarczy charakterystyka większa niż wymiary przestrzeni A_α . Dla klasycznych algebr prostych przestrzenie A_α są jednowymiarowe, więc dla nich wynik zachodzi z dowolnej charakterystyce.

Lemat 1.5 *Niech A będzie algebrą Liego nad ciałem algebraicznie domkniętym K charakterystyki 0. Jeśli C_1 i C_2 są dwoma podalgebrami Cartana w A to istnieje automorfizm elementarny u taki że $u(C_1) = C_2$.*

Dowód: Wiemy że każda podalgebra Cartana C jest postaci T_0 gdzie

$$T_0 = \{a \in A : \exists_k \text{ad}_T^k(a) = 0\}$$

dla pewnego $T \in C$. Element C dla którego $T_0 = C$ nazywamy elementem regularnym. Elementy $T \in C$ które nie są regularne to dokładnie te elementy że rząd ad_T jest mniejszy niż maksymalny możliwy. Rząd można wyliczać przy pomocy minorów. W szczególności zbiór elementów $T \in C$ które nie są regularne jest zbiorem zer pewnego wielomianu (produktu odpowiednich minorów). Przypomnijmy że mamy

$$A = C \oplus \bigoplus_{\lambda \neq 0} A_\lambda.$$

Jeśli $x \in A$ z $\lambda \neq 0$ to ad_x jest nilpotentny. Mianowicie, $\text{ad}_x(V_\beta) \subset V_{\beta+\lambda}$ i $\text{ad}_x^k(V_\beta) \subset V_{\beta+k\lambda}$. Dla dostatecznie dużego k wszystkie przestrzenie $V_{\beta+k\lambda}$ będą zerowe, czyli $\text{ad}_x^k = 0$. Teraz definiujemy odwzorowanie ϕ na $C \times \prod_\lambda V_\lambda$ wzorem

$$\phi(h, x_{\lambda_1}, \dots, x_{\lambda_n}) = \exp(\text{ad}_{x_{\lambda_1}}) \dots \exp(\text{ad}_{x_{\lambda_n}})h$$

Zauważmy że elementy w obrazie ϕ mają postać $u(h)$ gdzie u jest automorfizmem elementarnym zaś $h \in C$. Twierdzimy że pochodna w zerze ϕ jest na. Mianowicie, pochodna cząstkowa względem x_{λ_k} to identyczność, podobnie pochodna cząstkowa względem h to identyczność. A więc na mocy Lematu 3.7 z dodatku obraz zbioru elementów regularnych przez ϕ zawiera zbiór otwarty w topologii Zariskiego. Niech teraz ϕ_1 będzie odwzorowaniem dla C_1 a ϕ_2 odwzorowaniem dla C_2 . Przekrój obrazów zawiera zbiór otwarty w topologii Zariskiego, a więc jest niepusty. A więc istnieją u_i, T_i , $i = 1, 2$ takie że u_i jest automorfizmem elementarnym zaś T_i jest elementem regularnym w C_i i mamy

$$u_1(T_1) = u_2(T_2)$$

czyli

$$u_2^{-1}u_1(T_1) = T_2.$$

Jako że $u_2^{-1}u_1$ jest automorfizmem, to

$$u_2^{-1}u_1(C_1) = u_2^{-1}u_1((T_1)_0) = (T_2)_0 = C_2$$

czyli faktycznie automorfizm elementarny $u_2^{-1}u_1$ przeprowadza C_1 na C_2 .

2 Forma Killinga i kryterium Cartana

Definicja. Niech A będzie skończenie wymiarową algebrą Liego nad ciałem. Formę

$$K(x, y) = \text{Tr}(\text{ad}_x \text{ad}_y)$$

nazywamy formą Killinga A .

Lemat 2.1 *Forma Killinga jest niezmiennicza:*

$$K([z, x], y) + K(x, [z, y]) = 0.$$

Dowód:

$$\begin{aligned} K([z, x], y) + K(x, [z, y]) &= \text{Tr}(\text{ad}_z \text{ad}_x \text{ad}_y - \text{ad}_x \text{ad}_z \text{ad}_y) + \text{Tr}(\text{ad}_x \text{ad}_z \text{ad}_y - \text{ad}_x \text{ad}_y \text{ad}_z) \\ &= \text{Tr}(\text{ad}_z \text{ad}_x \text{ad}_y - \text{ad}_x \text{ad}_y \text{ad}_z) \\ &= \text{Tr}(\text{ad}_z \text{ad}_x \text{ad}_y - \text{ad}_z \text{ad}_x \text{ad}_y) = 0. \end{aligned}$$

□

Lemat 2.2 *Forma Killinga obcięta do ideału to forma Killinga ideału.*

Proof: Dowód zostawiam jako ćwiczenie dla czytelnika.

□

Niech A będzie skończenie wymiarową półprostą algebrą Liego nad ciałem algebraicznie domkniętymi F charakterystyki 0 i niech C będzie podalgebrą Cartana w C . Mamy wtedy rozkład

$$A = C \oplus \bigoplus_{\alpha \in \Lambda} A_\alpha$$

gdzie $\Lambda = \{\alpha : \alpha \neq 0, A_\alpha \neq \{0\}\}$.

Lemat 2.3 (Weyl) *Jeśli $e \in A_\alpha$, $f \in A_{-\alpha}$, $h = [e, f]$, $\beta \neq 0$, $A_\beta \neq \{0\}$ to istnieje liczba wymierna $r_{\alpha, \beta}$ zależna od α, β lecz niezależna od wyboru e, f , taka że $\beta(h) = r_{\alpha, \beta} \alpha(h)$.*

Dowód: Niech $V = \bigoplus_{n \in \mathbb{Z}} A_{\beta+n\alpha}$. V jest ad_e, ad_f i ad_h niezmiennicza. Skoro $h = [e, f]$ to $\text{Tr}_V(\text{ad}_h) = 0$. Czyli

$$\sum_{n \in \mathbb{Z}} (\beta(h) + n\alpha(h)) \dim(A_{\beta+n\alpha}) = 0$$

czyli

$$\beta(h) \sum_{n \in \mathbb{Z}} \dim(A_{\beta+n\alpha}) = -\alpha(h) \sum_{n \in \mathbb{Z}} n \dim(A_{\beta+n\alpha})$$

i

$$\beta(h) = -\frac{\sum_{n \in \mathbb{Z}} n \dim(A_{\beta+n\alpha})}{\sum_{n \in \mathbb{Z}} \dim(A_{\beta+n\alpha})} \alpha(h)$$

□

Lemat 2.4 *Jeśli A jest algebrą Liego nad ciałem charakterystyki 0, taką że $A = [A, A]$ to forma Killinga A jest niezerowa.*

Dowód: Bez zmniejszania ogólności można zakładać że ciało podstawowe jest algebraicznie domknięte. Niech C będzie podalgebrą Cartana w A . Mamy

$$A = \bigoplus_{\alpha} A_{\alpha}$$

gdzie $A_0 = C$. Ponieważ dla $\beta \neq -\alpha$ mamy $[A_{\alpha}, A_{\beta}] \subset A_{\alpha+\beta}$ założenie że $[A, A] = A$ implikuje że $C = \text{lin}[A_{\alpha}, A_{-\alpha}]$. W szczególności istnieje $\alpha \neq 0$, $e \in A_{\alpha}$, $f \in A_{-\alpha}$ takie że $h = [e, f] \neq 0$. Z lematu 2.3 wynika teraz że

$$K(h, h) = \sum_{\beta} \beta(h)^2 \dim(A_{\beta}) = \alpha(h)^2 \sum_{\beta} r_{\alpha, \beta}^2 \dim(A_{\beta}).$$

Suma po β powyżej jest sumą liczb nieujemnych, przy tym $r_{\alpha, \alpha} = 1$, $\dim(A_{\alpha}) > 0$, czyli suma jest dodatnia. A więc $K(h, h) = 0$ implikuje że $\alpha(h) = 0$ i konsekwentnie dla dowolnego β takiego że $A_{\beta} \neq 0$ mamy $\beta(h) = 0$. C jest rozpinane przez wektory h jak wyżej, gdyby dla dowolnego takiego h zachodziło $K(h, h) = 0$ to jedynym α takim że $A_{\alpha} \neq \{0\}$ byłoby 0, czyli $A = C$ byłaby nilpotentna. Lecz to przeczyłoby warunkowi $[A, A] = A$. □

Lemat 2.5 *(Kryterium Cartana). Jeśli A jest skończenie wymiarową algebrą Liego nad ciałem charakterystyki 0 to*

- *A jest rozwiązalna wtedy i tylko wtedy gdy A jest ortogonalne do $[A, A]$ względem formy Killinga*
- *A jest półprosta wtedy i tylko wtedy gdy forma Killinga A jest niezdegenerowana*

Dowód: Jeśli A jest rozwiązalna, to po rozszerzeniu ciała do ciała algebraicznie domkniętego, na mocy twierdzenia Liego dla $x \in A$, $y \in [A, A]$ operator

$\text{ad}_x \text{ad}_y$ jest nilpotentny, czyli $K(x, y) = \text{Tr}(\text{ad}_x \text{ad}_y) = 0$. Jeśli A jest ortogonalne do $[A, A]$ względem formy Killinga, ale A nie jest rozwiązalna to definiując $A_0 = A$, $A_{k+1} = [A_k, A_k]$ dla pewnego $k \geq 1$ mielibyśmy $A_k = A_{k+1} = [A_k, A_k]$. A_k są ideałami A , a więc forma Killinga A_k jest obcięciem formy Killinga A do A_k . Czyli forma Killinga A_k byłaby zerowa. Ale na mocy lematu 2.4 jest to niemożliwe, co kończy dowód pierwszej części twierdzenia.

Jeśli $I \subset A$ jest nietrywialnym ideałem rozwiązalnym to rozważając $I_0 = I$, $I_{k+1} = [I_k, I_k]$ widzimy że A zawierałaby nietrywialny ideał abelowy (takim ideałem jest I_k z maksymalnym k takim że $I_k \neq \{0\}$). Jeśli I jest ideałem abelowym, $x \in A$, $y \in I$ to I jest podprzestrzenią niezmienniczą dla ad_x i dla ad_y czyli I jest niezmiennicze dla $\text{ad}_x \text{ad}_y$. Na I mamy $\text{ad}_y = 0$ czyli $\text{Tr}_I(\text{ad}_x \text{ad}_y) = 0$. Skoro $\text{ad}_y(A) \subset I$ to na przestrzeni ilorazowej A/I operator ad_y indukuje operator zerowy i

$$K(x, y) = \text{Tr}(\text{ad}_x \text{ad}_y) = \text{Tr}_I(\text{ad}_x \text{ad}_y) + \text{Tr}_{A/I}(\bar{\text{ad}}_x \bar{\text{ad}}_y) = 0$$

gdzie $\bar{\text{ad}}_x$ i $\bar{\text{ad}}_y = 0$ są operatorami na A/I indukowanymi przez ad_x i ad_y . A więc gdyby A nie była półprosta to forma Killinga K byłaby zdegenerowana.

Pozostaje pokazać że algebra półprosta ma niezdegenerowaną formę Killinga. Nie wprost, gdyby A była półprosta, zaś K byłaby zdegenerowana to $I = \{x \in A : \forall y \in A K(x, y) = 0\}$ byłby ideałem A z zerową formą Killinga. Na mocy pierwszej części I byłby ideałem rozwiązalnym, co przeczyłoby półprostocie. Czyli $I = \{0\}$ i K jest niezdegenerowana. $\square$

Lemat 2.6 Niech A będzie skończeniem wymiarową półprostą algebrą Liego nad ciałem charakterystyki 0 i niech $\text{Der}(A)$ będzie algebrą Liego różniczkowań A . Wtedy odwzorowanie $x \mapsto \text{ad}_x$ zadaje izomorfizm A z $\text{Der}(A)$

Dowód: Jądem odwzorowania $x \mapsto \text{ad}_x$ jest centrum A , skoro A jest półprosta to centrum jest trywialne i A jest izomorficzne ze swoim obrazem $\tilde{A}$ w $\text{Der}(A)$. $\tilde{A}$ jest ideałem w $\text{Der}(A)$:

$$\begin{aligned} [d, \text{ad}_x](z) &= d([x, z]) - [x, d(z)] = [d(x), z] + [x, d(z)] - [x, d(z)] \\ &= [d(x), z] = \text{ad}_{d(x)}(z). \end{aligned}$$

A więc forma Killinga algebry $\text{Der}(A)$ na $\tilde{A}$ jest identyczna z formą Killinga $\tilde{A}$ czyli jest niezdegenerowana. Niech $I = \{d \in \text{Der}(A) : \forall x \in \tilde{A} K(d, x) = 0\}$. Mamy wtedy $\text{Der}(A) = \tilde{A} \oplus I$. Mianowicie, dla $d \in \text{Der}(A)$ i $x \in \tilde{A}$ definiujemy $\beta_d(x) = K(d, x)$. Skoro K jest niezdegenerowana na $\tilde{A}$ to istnieje $y \in \tilde{A}$ taki że $\beta_d(x) = K(y, x)$. Teraz dla dowolnego $x \in \tilde{A}$ mamy $K(d - y, x) = 0$, czyli $d - y \in I$, co pokazuje że $d \in \tilde{A} + I$. Jako że d jest dowolne to $\text{Der}(A) = \tilde{A} + I$. Jeśli $x \in I \cap \tilde{A}$ to x leży jądrze K obciętego do $\tilde{A}$, co dzięki temu że K jest niezdegenerowana na $\tilde{A}$ oznacza że $x = 0$, czyli suma $\tilde{A} + I$ jest sumą prostą.

Forma Killinga jest niezmiennicza, a więc I jest ideałem: dla $d \in I$, $x \in \tilde{A}$, $z \in \text{Der}(A)$ mamy $[z, x] \in \tilde{A}$ i

$$K([z, d], x) = -K(d, [z, x]) = 0$$

czyli $[z, d] \in I$. Teraz dla $d \in I$ i $x \in \tilde{A}$ mamy $[d, x] \in \tilde{A} \cap I = \{0\}$. Lecz, jak to obliczyliśmy wyżej $[d, \text{ad}_x] = \text{ad}_{d(x)}$, czyli $d = 0$, co oznacza że $I = \{0\}$ i

$$\text{Der}(A) = \tilde{A}.$$

□

Definicja: Mówimy że operator S na przestrzeni wektorowej V jest półprosty jeśli V ma bazę złożoną z wektorów własnych S .

Lemat 2.7 *Jeśli V jest skończenie wymiarową przestrzenią wektorową nad ciałem algebraicznie domkniętym zaś A jest operatorem liniowym na V , to istnieją operatory S i N takie że $A = S + N$, S jest półprosty, N jest nilpotentny i S komutuje z każdym operatorem komutującym z A .*

Dowód: Jeśli A ma tylko jedną wartość własną a to $S = aI$ i $N = A - S$ daje żądany rozkład. Mianowicie, skoro A ma tylko jedną wartość własną to wielomian minimalny A to $(X - a)^k$ dla pewnego k , czyli $N^k = (A - aI)^k = 0$ i N jest nilpotentny. Oczywiście S jest półprosty i komutuje z każdym operatorem a więc tym bardziej z każdym operatorem komutującym z A .

Jeśli A ma wartości własne $a_1, \dots, a_n$ to niech $V_i = \{v \in V : (A - a_i I)^{\dim(V)} v = 0\}$. Jeśli B komutuje z A to dla $v \in V_i$ mamy $(A - a_i I)^{\dim(V)} Bv = B(A - a_i I)^{\dim(V)} v = 0$, czyli $Bv \in V_i$. Innymi słowy, podprzestrzenie V_i są niezmiennicze dla B . Lecz $V = \oplus V_i$ czyli jeśli zbudujemy rozkład na każdym z V_i z osobna to będzie miał żądane własności: skoro V_i są niezmiennicze dla B to S komutując z B na każdym z V_i z osobna będzie komutował z B . Oczywiście S będąc sumą prostą operatorów półprostych jest półprosty, N będąc sumą prostą operatorów nilpotentnych jest nilpotentny. □

Lemat 2.8 *Niech A będzie skończenie wymiarową półprostą algebrą Liego nad ciałem algebraicznie domkniętym charakterystyki 0 i niech C będzie podalgebrą Cartana w A . Niech $A = \oplus_{\alpha} A_{\alpha}$ gdzie $A_0 = C$. Dla $\alpha \neq -\beta$ przestrzenie A_{α} i A_{β} są ortogonalne względem formy Killinga. Forma Killinga A obcięta do C jest niezdegenerowana. Ponadto forma Killinga zadaje dualność między A_{α} a $A_{-\alpha}$.*

Dowód: Wiemy że $[A_{\alpha}, A_{\gamma}] \subset A_{\alpha+\gamma}$, a więc dla $x \in A_{\alpha}$, $y \in A_{\beta}$ mamy $\text{ad}_x \text{ad}_y (A_{\gamma}) \subset A_{\alpha+\beta+\gamma}$ i $(\text{ad}_x \text{ad}_y)^k (A_{\gamma}) \subset A_{k(\alpha+\beta)+\gamma}$. Jeśli $\alpha \neq -\beta$ dla dowolnego γ takiego że $A_{\gamma} \neq \{0\}$ i dużych k mamy $A_{k(\alpha+\beta)+\gamma} = \{0\}$, czyli $\text{ad}_x \text{ad}_y$ jest nilpotentny, czyli $K(x, y) = \text{Tr}(\text{ad}_x \text{ad}_y) = 0$. Skoro forma Killinga jest niezdegenerowana zaś dla $\alpha \neq -\beta$ A_{α} jest ortogonalne do A_{β} to $A_{-\alpha}$ musi być dualne do A_{α} . W szczególności dla $\alpha = 0$ oznacza to że forma Killinga obcięta do C jest niezdegenerowana. □

3 Dodatek o topologii Zariskiego

Głównym celem dodatku jest dowód Lematu 3.7. Można by podać inne dowody, ten używa tylko podstawowy materiał z algebry i przynajmniej teoretycznie jest konstruktywny, tzn. można by jawnie wyliczyć odpowiednie wielomiany definiujące zbiory których istnienie dowodzimy. Alternatywny dowód można podać

zauważając że Lemat 3.5 jest szczególnym przypadkiem twierdzenia o eliminacji kwantyfikatorów dla teorii ciał algebraicznie domkniętych, zaś to twierdzenie ma relatywnie prosty dowód metodami teorii modeli.

Definicja. Niech W będzie skończenie wymiarową przestrzenią wektorową nad ciałem. Powiemy że zbiór $F \subset W$ jest domknięty w topologii Zariskiego (albo krócej domknięty) jeśli jest zbiorem zer pewnego układu wielomianów.

Zauważmy że jeśli pewien zbiór wielomianów G zeruje się na F to również ideał pierścienia wielomianów generowany przez G zeruje się na F . Zgodnie z twierdzeniem Hilberta o bazie ideały w pierścieniu wielomianów ustalonej skończonej liczny zmiennych są skończenie generowalne, więc zbiór domknięty w topologii Zariskiego jest zbiorem zer skończonego układu wielomianów. Dany zbiór może być zbiorem zer wielu różnych ideałów. Największy ideał dostaniemy biorąc wszystkie wielomiany zerujące się na F , ten ideał oznaczamy niekiedy przez $I(F)$.

Zauważmy też że dowolny przekrój zbiorów domkniętych w topologii Zariskiego oraz skończona suma zbiorów domkniętych w topologii Zariskiego jest domknięta w topologii Zariskiego. Mianowicie, przekrój zbiorów zer ideałów I_α jest równy zbiorowi zer $\bigcup_\alpha I_\alpha$. Dla sumy korzystamy z tego że zbiór domknięty jest zbiorem zer skończonego układu wielomianów. Jeśli F jest zbiorem zer $p_1, \dots, p_k$, zaś G jest zbiorem zer $q_1, \dots, q_l$, to $F \cup G$ jest zbiorem zer $\{p_i q_j : i = 1, \dots, k, j = 1, \dots, l\}$. Pokazuje to że suma dwu zbiorów domkniętych jest domknięta. Ponadto zbiór pusty jest domknięty jako zbiór zer wielomianu stale równego 1 i całe W jest domknięte jako zbiór zer wielomianu zerowego. A więc zbiory domknięte dają nam topologię na W którą nazywamy topologią Zariskiego. Jak zwykle w topologii mówimy że zbiór jest otwarty jeśli jego dopełnienie jest domknięte.

Definicja. Powiemy że zbiór F domknięty w topologii Zariskiego jest nierozkładalny jeśli nie da się go przedstawić jako sumy dwu zbiorów domkniętych w topologii Zariskiego F_1, F_2 , takich że $F_i \neq F$.

Zauważmy że jeśli zbiór nierozkładalny F jest zawarty w skończonej sumie zbiorów domkniętych w topologii Zariskiego F_i to istnieje i takie że $F \subset F_i$. Mianowicie, zastępując F_i przez $F \cap F_i$ można zakładać że suma F_i jest równa F . Dla dwu składników wynik teraz dostajemy z definicji nierozkładalności, zaś dla większej ilości składników używamy indukcję.

Lemat 3.1 *Jeśli zbiór F jest nierozkładalny to ideał $I(F)$ wszystkich wielomianów zerujących się na F jest pierwszy.*

Dowód: Niech p_1 i p_2 będą wielomianami takimi że $p_1 p_2 \in I(F)$, czyli dla każdego $w \in W$ mamy $p_1 p_2(w) = 0$. Dla $i = 1, 2$ niech $F_i = \{w : p_i(w) = 0\}$. Jeśli $w \in F$ to albo $p_1(w) = 0$ i wtedy $w \in F_1$, albo $p_2(w) = 0$ i wtedy $w \in F_2$. A więc $F \subset F_1 \cup F_2$. Jako że F jest nierozkładalny oznacza to że $F \subset F_1$ lub $F \subset F_2$. Jeśli $F \subset F_1$ to p_1 jest zerem na F , czyli $p_1 \in I(F)$. Podobnie, jeśli $F \subset F_2$ to $p_2 \in I(F)$. Jako że p_1, p_2 były dowolne oznacza to że $I(F)$ jest ideałem pierwszym. $\square$

Lemat 3.2 *Jeśli F jest domknięty w topologii Zariskiego to jest on skończoną sumą zbiorów nierozkładalnych.*

Dowód: Przypuśćmy że zbioru F nie da się przedstawić jako skończonej sumy zbiorów nierozkładalnych. Wtedy F można by przedstawić jako sumę mniejszych zbiorów z których co najmniej jeden nie byłby skończoną sumą zbiorów nierozkładalnych. Indukcyjnie otrzymalibyśmy nieskończony ciąg zbiorów domkniętych F_i takich że $F = F_1$, $F_{i+1} \subset F_i$ i $F_i \neq F_{i+1}$. Niech $I_i = I(F_i)$ będą odpowiadającymi im ideałami. Mamy $I_i \subset I_{i+1}$ i skoro $F_i \neq F_{i+1}$ to $I_i \neq I_{i+1}$. Ale pierścień wielomianów jest noetherowski, czyli nie istnieje nieskończony wstępujący ciąg ideałów, co daje sprzeczność która kończy dowód. $\square$

Lemat 3.3 *Niech W będzie skończenie wymiarową przestrzenią wektorową nad ciałem algebraicznie domkniętym K . Jeśli $T, V \subset W \times K$ są zbiorami domkniętymi w topologii Zariskiego, takimi że T jest nierozkładalny i $T - V \neq \emptyset$, zaś S jest rzutem $T - V$ na W to istnieją podzbiory $F, G \subset W$ domknięte w topologii Zariskiego, takie że $S \subset F$, $F - G \subset S$ i domknięcie Zariskiego $F - G$ to F . Przy tym F jest nierozkładalny.*

Dowód: Niech π oznacza operator rzutowania na W . Jako F bierzemy domknięcie $\pi(T - V)$ w topologii Zariskiego. Zauważmy że $\pi(T) \subset F$. Mianowicie $T \subset \pi^{-1}(F) \cup V$. Jako że T jest nierozkładalny to zawiera się w jednym ze składników sumy. Ale $T \subset V$ jest wykluczone przez założenie $T - V \neq \emptyset$, czyli $T \subset \pi^{-1}(F)$ co oznacza że $\pi(T) \subset F$. F jest nierozkładalny. Mianowicie przypuśćmy że $F = F_1 \cup F_2$ z domkniętymi F_i . Wtedy mamy $T = T_1 \cup T_2$ gdzie $T_i = \pi^{-1}(F_i) \cap T$. T jest nierozkładalny, czyli T jest równe jednemu ze składników, powiedzmy T_1 . Wtedy $\pi(T) = \pi(T_1) \subset F_1$, czyli $F = F_1$ co oznacza że F faktycznie jest nierozkładalny. Zauważmy że jeśli G jest zbiorem domkniętym takim że $F - G \neq \emptyset$, to domknięcie $F - G$ w topologii Zariskiego jest równe F . Mianowicie, oznaczając domknięcie przez H mamy $F \subset H \cup G$. Jako że F jest nierozkładalny i nie jest podzbiorem G to F jest podzbiorem H , czyli $F = H$.

A więc pozostaje znaleźć zbiór domknięty G taki że $F - G \subset \pi(T - V)$. Wielomiany zadające T i V możemy traktować jako elementy pierścienia $K[W, x]$ wielomianów od x i zmiennych z W . Podobnie wielomiany zadające F są elementami pierścienia $K[W]$ wielomianów od zmiennych z W który możemy traktować jako podpierścień $K[W, x]$. Niech I będzie zbiorem elementów $K[W, x]$ zerujących się na T zaś M będzie zbiorem elementów $K[W]$ zerujących się na F . Elementy M potraktowane jako elementy $K[W, x]$ zerują się na T (bo $\pi(T) \subset F$), a więc $M \subset I$. Zauważmy że jest możliwe $I = K[W, x]M$. Ten przypadek jest łatwy, wtedy $T = F \times K$. Z założenia istnieje wielomian p taki że p zeruje się na V ale istnieje $(w, k) \in T$ takie że $p(w, k) \neq 0$. Jeśli p nie zależy od x to jako G można wziąć zbiór zer p . Jeśli p zależy od k to przy ustalonym $w \in F$ ma tylko skończenie wiele zer, czyli istnieje $k \in K$ takie że $p(w, k) \neq 0$, co oznacza że $\pi(T - V) = \pi(T) = F$. A więc w dalszym ciągu możemy zakładać że $I \neq K[W, x]M$.

Pierścień $K[F]$ funkcji regularnych na F to $K[W]/M$. Jako że F jest nierozkładalny to (Lemat 3.1) M jest ideałem pierwszym i $K[W]/M$ nie ma dzielników zera. A więc pierścień K_F ułamków $K[F]$ jest ciałem. Teraz rozpatrujemy pierścień $K_F[x]$ wielomianów jednej zmiennej x o współczynnikach w ciele K_F . Zauważmy że elementy $K[W]$ naturalnie odwzorowują się w K_F . To się przedłuża do homomorfizmu $j : K[W, x] \rightarrow K_F[x]$. Zauważmy że $K_F[x] = j(K[W, x])K_F$

(pokazujemy to sprowadzając współczynniki elementu $K_F[x]$ do wspólnego mianownika który daje element K_F).

Zbiór $J = j(I)K_F$ jest ideałem w $K_F[x]$. J jest niezerowy, bo $j^{-1}(\{0\}) = K[W, x]M \neq I$. Wiadomo że $K_F[x]$ jest pierścieniem ideałów głównych, czyli istnieje niezerowy wielomian $g \in K_F[x]$ taki że g generuje J . Jako że $K_F[x] = j(K[W, x])K_F$ to g można wybrać postaci $j(h)$ dla pewnego $h \in I$. Twierdzimy że g jest nierozkładalny. Mianowicie rozkład $g = g_1g_2$ w $K_F[x]$ po sprowadzeniu do wspólnego mianownika prowadziłby do równości $sj(h) = sj(h_1)j(h_2)$ w $K[F][x]$ dla pewnych $r, s \in K[F] - \{0\}$ i $h_1, h_2 \in K[W, x]$, co prowadziłoby do równości

$$th - uh_1h_2 = p$$

gdzie p jest elementem $K[W, x]$ takim że $j(p) = 0$ zaś obrazy t i u w $K[F]$ to odpowiednio r i s . W szczególności $r, u \notin M$ zaś wszystkie współczynniki p traktowanego jako wielomian od x o współczynnikach z $K[W]$ należą do M . A więc p zeruje się na $F \times K$, czyli również na T . A więc na T mamy równość

$$th - uh_1h_2 = 0$$

czyli $uh_1h_2 \in I$. Jako że T jest nierozkładalny, to I jest ideałem pierwszym, czyli jeden z czynników należy do I . Gdyby któreś $h_i \in I$ to g nie był by generatorem J , co daje sprzeczność. Gdyby $u \in I$, to u zerowałoby się na $\pi(T)$, czyli $u \in M$ co też daje sprzeczność. A więc przypuszczenie że g jest rozkładalny daje sprzeczność, czyli g jest nierozkładalny.

Teraz twierdzimy że jeśli $q \in K[W, x]$ i $g|j(q)$ w $K_F[x]$ to $q \in I$. Mianowicie wtedy w $K[F][x]$ mamy równość postaci

$$rj(q) = sj(h)j(q_2)$$

z $r, s \in K[F] - \{0\}$ i $q_2 \in K[W, x]$, co prowadzi do równości postaci

$$tq - uhq_2 = p$$

z p zerującym się na $F \times K$ (a więc i na T), czyli na $F \times K$ mamy równość

$$tq - uhq_2 = 0$$

czyli $tq \in I$. Jako poprzednio $t \in I$ jest niemożliwe, więc skoro I jest pierwszy to $q \in I$.

Zauważmy że gdyby $J = K_F[x]$, czyli g miałby stopień 0, to $I = K[W, x]$. Ale zakładamy że T jest niepusty, więc $I \neq K[W, x]$, czyli g ma stopień dodatni.

Jeśli $q \in I$, to istnieje $f \in K[W] - M$ takie że jeśli $(w, k) \in F \times K$ są takie że $f(w) \neq 0$ i $h(w, k) = 0$ to $q(w, k) = 0$. Mianowicie, to skoro g generuje J to g dzieli $j(q)$ w $K_F[x]$ czyli jak wyżej na $F \times K$ mamy równość

$$tq - uhq_2 = 0$$

czyli

$$t(w)q(w, k) = u(w)h(w, k)q_2(w, k).$$

Jeśli $h(w, k) = 0$ to prawa strona jest zerem, czyli $t(w)q(w, k) = 0$. Jeśli ponadto $t(w) \neq 0$ to $q(w, k) = 0$. A więc wystarczy wziąć $f = t$.

Zauważmy że można wybrać f wspólne dla wszystkich elementów I . Mianowicie, I ma skończony zbiór generatorów $q_1, \dots, q_n$. Wybieramy f_i dla q_i . Wtedy $f = f_1 \dots f_n$ działa dla wszystkich q_i . Jeśli generatory I zerują się na (k, w) to wszystkie elementy I zerują się na (k, w) . Podsumowując, istnieje $f \in K[W] - M$ takie że jeśli (w, k) spełnia $f(w) \neq 0$ i $h(w, k) = 0$ to $(w, k) \in T$. Mianowicie, wtedy dla dowolnego $q \in I$ mamy $q(w, k) = 0$. Jako że T jest zbiorem zer I oznacza to że $(w, k) \in T$.

Niech teraz N będzie ideałem elementów $K[W, x]$ zerujących się na V i niech $q_1, \dots, q_n$ będą generatorami N . Gdyby g dzielił wszystkie $j(q_i)$ to mielibyśmy $q_i \in I$, czyli $T \subset V$ co jest niemożliwe z założenia. A więc istnieje i takie że g nie dzieli q_i . Wybieramy jedno takie i i dla uproszczenia oznaczeń dalej zamiast q_i będziemy pisać q .

Jako że g jest nierozkładalny i nie dzieli $j(q)$ to ideał generowany przez q i $j(q)$ w $K_F[x]$ to całe $K_F[x]$, czyli ten ideał zawiera 1. A więc istnieją $v, w \in K_F[x]$ takie że

$$vj(q) + wg = 1.$$

Używając własność $K_F[x] = j(K[W, x]K_F)$ i sprowadzając lewą stronę do wspólnego mianownika widzimy że istnieją $a, b \in K[W, x]$ i $r, s, p \in K[F] - \{0\}$ takie że

$$rj(a)j(q) + sj(b)j(h) = p$$

Jak poprzednio, daje to równość

$$taq + ubh = v$$

na $F \times K$ z $t, u, v \in K[W]$ które nie są tożsamościowo równe zero na F .

Niech $z \in K[W]$ będzie współczynnikiem przy najwyższej potędze x w h (który możemy potraktować jako element $K[W]$). h możemy wybrać tak by z nie należał do M . Mianowicie, wybieramy h minimalnego stopnia względem x ale tak by dostać to samo $j(h)$. Gdyby $z \in M$ to $j(zz^k) = 0$ i można by zastąpić h przez wielomian niższego stopnia względem x .

Niech teraz G będzie zbiorem zer fvz . Z założeń wyżej $f, v, z \notin M$, czyli jako że M jest pierwszy $fvz \notin M$, czyli fvz nie zeruje się tożsamościowo na F , czyli $F - G \neq \emptyset$. Niech teraz $w \in F - G$. $w \notin G$ oznacza że $fvz(w) \neq 0$ i w szczególności $z(w) \neq 0$. A więc przy ustalonym w wielomian $h(w, x)$ jest wielomianem jednej zmiennej x dodatniego stopnia. Jako że K jest algebraicznie domknięte to istnieje $k \in K$ takie że $h(w, k) = 0$. Mamy $fvz(w) \neq 0$ i $h(w, k) = 0$, w szczególności $f(w) \neq 0$, czyli jak pokazaliśmy poprzednio $(w, k) \in T$. Jako że $h(w, k) = 0$, to w równości wyżej człon ubh znika w (w, k) , czyli jako że $v(w) \neq 0$ to

$$t(w)a(w, k)q(w, k) = v(w) \neq 0$$

czyli $q(w, k) \neq 0$, czyli $(w, k) \notin V$. A więc dla dowolnego $w \in F - G$ znaleźliśmy k takie że $(w, k) \in T - V$, czyli $w \in \pi(T - V)$, czyli $F - G \subset \pi(T - V)$. $\square$

Lemat 3.4 *Niech W będzie skończenie wymiarową przestrzenią wektorową nad ciałem algebraicznie domkniętym K . Jeśli $U \subset K \times W$ jest niepustą różnicą zbiorów domkniętych w topologii Zariskiego, zaś S jest rzutem U na W to istnieją podzbiory $F, G \subset W$ domknięte w topologii Zariskiego, takie że $S \subset F$, $F - G \subset S$ i domknięcie Zariskiego $F - G$ to F .*

Dowód: Niech $U = T - V$ gdzie T i V są domknięte. Na mocy Lematu 3.2 T jest skończoną sumą zbiorów nierozkładalnych T_i :

$$T = \bigcup_i T_i.$$

Niech π oznacza operator rzutowania na W . Do par T_i, V stosujemy Lemat 3.3 otrzymując nierozkładalne F_i i domknięte G_i . Zastępując G_i przez $G_i \cap F_i$ możemy zakładać że $G_i \subset F_i$. Bierzemy

$$F = \bigcup_i F_i,$$

$$G = \bigcup_i G_i.$$

Na mocy Lematu 3.3 $\pi(T_i - V) \subset F_i \subset F$, czyli również $\pi(T - V) \subset F$. Podobnie $F_i - G_i \subset \pi(T_i - V) \subset \pi(T - V)$, czyli $F - G \subset \pi(T - V)$. Niech H będzie domknięciem $F - G$ w topologii Zariskiego. Ustalmy i takie że zbiór F_i nie jest zawarty w żadnym F_j dla $j \neq i$. F_i jest zawarty w $H \cup G = F \cup G$. Jako że F_i jest nierozkładalny to jest zawarty w jednym ze składników sumy. $F_i \subset G$ oznaczałoby że istnieje j takie że $F_i \subset G_j$, czyli skoro $G_j \subset F_j$ to $F_i \subset F_j$. Ale i było wybrane tak że F_i nie jest podzbiorem F_j , więc ten przypadek jest niemożliwy. Czyli $F_i \subset H$. W sumie F_i bez zmiany sumy możemy pominąć składniki zawarte w innych składnikach, więc cała suma F_i jest zawarta w H , czyli $H = F$, czyli domknięcie $F - G$ to F . $\square$

Lemat 3.5 *Niech V i W będą skończenie wymiarowymi przestrzeniami wektorowymi nad ciałem algebraicznie domkniętym K . Jeśli $U \subset V \oplus W$ jest niepustą różnicą zbiorów domkniętych w topologii Zariskiego, zaś S jest rzutem U na W to istnieją podzbiory $F, G \subset W$ domknięte w topologii Zariskiego, takie że $S \subset F$, $F - G \subset S$ i domknięcie Zariskiego $F - G$ to F .*

Dowód: Indukcja ze względu na $\dim(V)$. Jeśli $\dim(V) = 1$ to wynik otrzymujemy z Lematu 3.4. Jeśli $\dim(V) > 1$ to piszemy $V = Kv \oplus V_1$ gdzie $V_1 \subset V$ jest podprzestrzenią wymiaru $\dim(V) - 1$ zaś $v \in V - V_1$. Niech $W_1 = V_1 \oplus W$, niech π_1 będzie rzutem z $K \times W_1$ na W_1 i niech $S_1 = \pi_1(U)$. Na mocy Lematu 3.4 istnieją zbiory $F_1, G_1 \subset W_1$ domknięte w topologii Zariskiego, takie że $S_1 \subset F_1$, $F_1 - G_1 \subset S_1$ i domknięcie Zariskiego $F_1 - G_1$ to F_1 .

Biorąc $U_1 = F_1 - G_1$ widzimy że U_1 jest niepustą różnicą zbiorów domkniętych. Niech π_2 będzie rzutem z W_1 na W i niech $S_2 = \pi_2(U_1)$. Stosując założenie indukcyjne otrzymujemy zbiory F, G takie że $S_2 \subset F$ i $F - G \subset S_2$ oraz domknięcie Zariskiego $F - G$ to F . Oczywiście $S_2 \subset S$ więc $F - G \subset S$. Zauważmy że przeciwobraz $\pi_2^{-1}(F)$ jest zbiorem domkniętym i zawiera $U_1 = F_1 - G_1$, więc zawiera też domknięcie $F_1 - G_1$ czyli F_1 . Lecz $\pi_1(U) = S_1 \subset F_1$, czyli $\pi_1(S) \subset \pi_2^{-1}(F)$ czyli $S = \pi_2 \pi_1(U) \subset F$. $\square$

Lemat 3.6 *Niech $\phi : V \rightarrow W$ będzie odwzorowaniem wielomianowym skończenie wymiarowych przestrzeni wektorowych nad ciałem K takim że istnieje punkt*

$v \in V$ że pochodna ϕ w v jest na. Niech p będzie wielomianem na W takim że $p \circ W = 0$. Wtedy $p = 0$.

Dowód: Przesuwając w V i W można zakładać że $v = 0$ i że $\phi(0) = 0$. Zapisujemy p jako sumę wielomianów jednorodnych

$$p = \sum_{i=k}^l p_i$$

gdzie p_i ma stopień i i $p_k \neq 0$. Podobnie

$$\phi = \sum_{i=1}^m \phi_i$$

gdzie ϕ_i jest stopnia i . Jako że $\phi(0) = 0$ to w wyrażeniu na ϕ nie ma członu stopnia 0. Zauważmy że

$$p \circ \phi = p_k \circ \phi_1 + r$$

gdzie wszystkie człony r mają wyższy stopień niż k . Dzięki temu że ϕ_1 jest na $p_k \circ \phi_1 \neq 0$. Jako że $p_k \circ \phi_1$ jest stopnia k to nie może się uprościć z r . A więc $p \neq 0$ implikuje $p \circ \phi \neq 0$. $\square$

Lemat 3.7 Niech $\phi : V \rightarrow W$ będzie odwzorowaniem wielomianowym skończenie wymiarowych przestrzeni wektorowych nad ciałem algebraicznie domkniętym K takim że istnieje punkt $v \in V$ że pochodna ϕ w v jest na. Jeśli U jest zbiorem który zawiera niepusty zbiór otwarty w topologii Zariskiego to $\phi(U)$ zawiera niepusty zbiór otwarty w topologii Zariskiego.

Dowód: Niech $D \subset V \times W$ będzie wykresem ϕ :

$$D = \{(v, w) : \phi(v) = w\}$$

Niech Z będzie niepusty zbiór otwartym zawartym w U . Z definicji D jest zbiorem domkniętym. Niech $H = Z \times W$. Oczywiście H jest niepustym zbiorem otwartym w $V \times W$, czyli $D \cap H$ jest różnicą zbiorów domkniętych. Jako że ϕ jest zdefiniowane na całym V a Z jest niepusty to również $D \cap H$ jest niepusty. Oczywiście $S = \phi(Z)$ jest rzutem $D \cap H$ na W , a więc na mocy Lematu 3.5 istnieją zbiory domknięte F i G takie że $S \subset F$, $F - G \subset S$ i F jest domknięciem $F - G$. Pozostaje pokazać że $F = W$ (wtedy $F - G$ jest niepustym zbiorem otwartym). Niech p będzie wielomianem zerującym się na F . Wtedy $p \circ \phi$ zeruje się na W , czyli jako że K jest nieskończone to $p \circ \phi = 0$. A więc na mocy Lematu 3.6 również $p = 0$. Ale to oznacza że jedyny wielomian zerujący się na F to wielomian zerowy, czyli faktycznie $F = W$. $\square$