1 Konstrukcje uniwersalne

1.1 Moduły Liego

Przypominam że jeśli A jest algebrą Liego nad pierścieniem R zaś M jest modułem nad R to mówimy że M jest modułem Liego jeśli zadane jest działanie A na M które jest dwuliniowe i spełnia

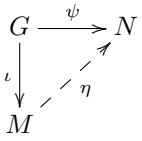
$$xyv - yxv = [x, y]v$$

dla dowolnych $x, y \in A$ i $v \in M$. W literaturze używa się też termin reprezentacja algebry A.

W naturalny sposób definiujemy homomorfizmy, podmoduły, sumę prostą, produkt i iloraz modułów Liego.

Definicja. Powiemy że moduł Liego M nad A jest wolnym modułem Liego generowanym przez zbiór $G \subset M$ jeśli dowolne odwzorowanie ψ z G w moduł Liego N nad A jednoznacznie przedłuża się do homomorfizmu η z M w N.

Można to zilustrować następującym diagramem:



gdzie ι jest włożeniem tożsamościowym G w M, a przerywana strzałka oznacza że wymagamy istnienia i jednozanczności odpowiedniego odwzorowania.

Z definicji wolnego modułu Liego wynika że jest on zdefiniowany jednoznacznie z dokładnością do izomorfizmu. Mianowicie, gdy M_1 i M_2 są dwoma różnymi wolnymi modułami Liego generowanym przez zbiór G, to odwzorowanie indentycznościowe na G przedłuża się do homomorfizmu $\eta : M_1 \to M_2$ i $\lambda : M_2 \to M_1$. Na mocy jednoznaczności przedłużenia kompozycja $\eta \circ \lambda$ która jest homomorfizmem z M_2 w M_2 będącym identycznością na G jest identycznością M_2. Podobnie $\lambda \circ \eta$ jest identycznością M_1. Czyli η i λ są izomorfizmami.

Lemat 1.1 *Wolny moduł Liego istnieje.*

Dowód: Rozpatrujemy zbiór S klas izomorfizmu modułów Liego N nad A mocy ograniczonej przez moc A do potęgi moc G z dodatkowym odwzorowaniem z G w N. Niech

$$\tilde{M} = \otimes_{N \in S} N$$

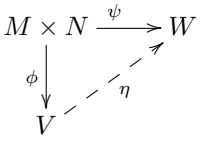
z prodktowym odwzorowaniem z G w $\tilde{M}$. Jako M bierzemy podmoduł Liego w $\tilde{M}$ generowany przez obraz G. Twierdzimy że M jest wolnym modułem Liego generowanym przez G. Mianowicie, jeśli V jest modułem Liego nad A z odwzorowaniem z G w V to rozpatrujemy podmoduł $\tilde{V}$ generowamy przez G. $\tilde{V}$ ma moc ograniczoną przez moc A do potęgi moc G, a więc jest izorficzny z pewnym $N \in S$. Rzutowanie z M na składową daje więc odwzorowanie z $\tilde{M}$ w V. Jako że $\tilde{M}$ jest generowany przez G to odwzorowanie jest wyznaczone jednoznacznie przez wartości na G. □

1.2 Iloczyn tensorowy

Niech R będzie pierścieniem przemiennym, zaś M i N będą R-modułami. Powiemy że moduł V jest iloczynem tensorowym modułów M i N (co oznaczamy pisząc $V = M \otimes N$) jeśli zadana jest operacja dwuliniowa ϕ z $M \times N$ w V mająca następującą własność: jeśli ψ jest operacją dwuliniową z $M \times N$ w pewien R-moduł W to istnieje dokładnie jedna operacja liniowa η z V w W taka że

$$\psi = \eta \circ \phi.$$

Można to zilustrować diagramem



Zamiast $\phi(m, n)$ zwykle piszemy $m \otimes n$.

Zauważmy najpierw że z definicji wyżej wynika że jeśli produkt tensorowy istnieje to jest wyznaczony jednoznacznie z dokładnością do izomorfizmu. Mianowicie, jeśli V_1 z $\otimes_1$ oraz V_2 z $\otimes_2$ są dwoma różnymi produktami tensorowymi to na mocy własności definicyjnej istnieją jedyne odwzorowania liniowe η_1 i η_2 takie że

$$m \otimes_2 n = \eta_1(m \otimes_1 n)$$

i

$$m \otimes_1 n = \eta_2(m \otimes_2 n)$$

Wtedy

$$m \otimes_1 n = \eta_2(\eta_1(m \otimes_1 n)).$$

Lecz na mocy definicji istnieje dokładnie jedno odwzorowanie liniowe mające własność wyżej czyli $\eta_2\eta_1$ to identyczność. Podobnie $\eta_1\eta_2$ to identyczność, czyli V_1 jest izomorficzne z V_2.

Lemat 1.2 *Iloczyn tensorowy istnieje.*

Dowód: Podobnie do konstrukcji wolnego modułu Liego możemy zbudować produkt klas izomorfizmu modułów S ograniczonej mocy z odwzorowaniem dwuliniowym z $M \times N$ w S i wziąść podmoduł generowany przez obraz produktowego odwzorowania dwuliniowego. Łatwo sprawdzić że spełnia on własność produktu tensorowego. □

Uwaga: Nieco konkretniejsza konstrukcja $M \otimes N$ używa moduł wolny T nad R generowany przez formalne produkty $m \otimes n$ gdzie $m \in M$, $n \in N$. Następnie T dzielimy przez podmoduł reprezentujący relacje zachodące w iloczynie tensorowym, tzn. $(rm)\otimes n - r(m \otimes n)$, $m \otimes (rn) - r(m \otimes n)$, $(m_1 + m_2) \otimes n - m_1 \otimes n - m_2 \otimes n$, $m \otimes (n_1 + n_2) - m \otimes n_1 - m \otimes n_2$.

Lemat 1.3 *Jeśli M, N, K są R-modułami to $M \otimes N$ jest izomorficzne z $N \otimes M$, $(M \otimes N) \otimes K$ jest izomorficzne z $M \otimes (N \otimes K)$. Jeśli $M = M_1 \oplus M_2$ i $N = N_1 \oplus N_2$ to $M \otimes N$ jest izomorficzne z $(M_1 \otimes N) \oplus (M_2 \otimes N)$ i $M \otimes N$ jest izomorficzne z $(M \otimes N_1) \oplus (M \otimes N_2)$.*

Dowód. Wynika to używając własność definicyjną. □

Lemat 1.4 *Jeśli $M = \oplus_\alpha M_\alpha$ to $M \otimes N$ jest izomorficzny z $\oplus_\alpha (M_\alpha \otimes N)$. Jeśli $N = \oplus_\alpha N_\alpha$ to $M \otimes N$ jest izomorficzny z $\oplus_\alpha (M \otimes N_\alpha)$.*

Lemat 1.5 *$M \otimes R$ jest izomorficzne z M. Podobnie $R \otimes M$ jest izomorficzne z M.*

Podobnie jak poprzednio są to łatwe wnioski z własności definicyjnej.

Lemat 1.6 *Jeśli M jest modułem wolnym z bazą $\{e_\alpha\}$ zaś N jest modułem wolnym z bazą $\{f_\beta\}$ to $M \otimes N$ jest modułem wolnym z bazą $\{e_\alpha \otimes f_\beta\}$*

Dowód: jest to bezpośredni wniosek z poprzednich lematów. □

Wniosek: Jeśli R to ciało to $\dim(M \otimes N) = \dim(M)\dim(N)$.

Przykład: Jeśli $R = \mathbb{Z}$, zaś p i q to względnie pierwsze liczby całkowite dodatnie to $R/(pR) \otimes R/(qR)$ to moduł zerowy. Mianowicie skoro p i q są względnie pierwsze to istnieją liczby całkowite a i b takie że $1 = ap + bq$. Teraz dla $u \otimes v \in R/(pR) \otimes R/(qR)$ mamy

$$u \otimes v = (ap + bq)(u \otimes v) = ap(u \otimes v) + bq(u \otimes v)$$

$$= a(pu \otimes v) + b(u \otimes qv).$$

Lecz $pu = 0$ w $R/(pR)$ i $qv = 0$ w $R/(qR)$ czyli powyższy element to 0. Jako że elementy postaci $u \otimes v$ generują $R/(pR) \otimes R/(qR)$ to produkt tensorowy jest zerowy.

Lemat 1.7 *Jeśli dla $i = 1, 2$ M_i, N_i są R-modułami, zaś $\phi_i : M_i \to N_i$ są homomorfizmami to istnieje dokładnie jeden homomorfizm $\phi : (M_1 \otimes M_2) \to (N_1 \otimes N_2)$ taki że*

$$\phi(m_1 \otimes m_2) = \phi_1(m_1) \otimes \phi_2(m_2)$$

Dowód: $\phi_1(m_1) \otimes \phi_2(m_2)$ jest odwzorowaniem dwuliniowym z $M_1 \times M_2$ w $N_1 \otimes N_2$ a więc ϕ istnieje i jest jednoznaczne z własności definicyjnej iloczynu tensorowego $M_1 \otimes M_2$. □

W dalszym ciągu odwzorowanie ϕ wyżej będziemy oznaczać przez $\phi_1 \otimes \phi_2$.

1.3 Rozszerzanie skalarów

Istotną konstrukcją jest rozszerzanie skalarów. Mianowicie dla pierścienia S "rozszerzającego" R i algebry Liego A nad R piszemy

$$A_S = S \otimes_R A$$

A_S ma strukturę S modułu, więc jest algebrą Liego nad S.

Uwaga: słowo "rozszerzającego" napisaliśmy w cudzysłowach, bo konstrukcja wymaga tylko by mieć homomorfizm z R w S, wtedy S jest R modułem i produkt tensorowy da nam R-moduł. Homomorfizm jest potrzebny by mnożenie przez elemeny S zgadzało się z mnożenim przez elementy R. Ważnym przykładem jest $S = \mathbb{Z}_p$ (ciało reszt modulo p) i $R = \mathbb{Z}$. Ogólniej, dla każdego pierścienia (z jedynką) S mamy naturalny homomorfizm z $\mathbb{Z}$ w S, co pozwala budować algebry nad dowolnymi pierścieniami z algebr nad $\mathbb{Z}$.

Jeśli A i B są algebrami Liego nad R, zaś $h : A \to B$ jest homomorfizmem, to $h_S = \mathrm{id}_S \otimes_R h$ jest homomorfizmem algebr Liego. Przy tym $(g \circ h)_S = g_S \circ h_S$.

Zauważmy że algebrę A_S można też traktować jako algebrę Liego nad R. Elementy postaci $1 \otimes a$ dla $a \in A$ tworzą podalgebrę nad R będącą homomorficznym obrazem A.

Lemat 1.8 *Jeśli I jest podalgebrą w A to I_S obraz I_S w A_S jest podalgebrą w A_S. Jeśli I jest ideałem to obraz I_S jest ideałem w A_S.*

Lemat 1.9 *Zakładamy że S jest modułem wolnym nad R (np. R jest ciałem). Jeśli I jest podalgebrą w A to I_S wkłada się różnowartościowo w A_S. Pondto algebra A jest rozwiązalna (nilpotentna) wtedy i tylko wtedy gdy A_S jest rozwiązalna (nilpotentna).*

Dowód: Gdy S jest modułem wolnym nad R z bazą e_i to jako R moduł

$$S = \oplus_i e_i R$$

czyli

$$S \otimes A = \oplus_i (e_i R \otimes A)$$

i dowolny podmoduł A wkłada się różnowartościowo w $S \otimes A$.

Gdy

$$A_0 = A,$$

$$A_{i+1} = [A_i, A_i]$$

jest ciągiem podalgebr z definicji rozwiązalności, to

$$(A_S)_i = (A_i)_S$$

czyli $A_k = \{0\}$ implikuje $(A_S)_k = 0$. Jeśli S jest modułem wolnym nad R to A_k wkłada się różnowartościowo w $(A_S)_k$, czyli $(A_S)_k = \{0\}$ implikuje $A_k = \{0\}$. Identyczny argument działa w przypadku nilpotentności. □

1.4 Algebra tensorowa

Niech M będzie R-modułem. Oznaczmy przez

$$M^{\otimes k} = M \otimes M \otimes \cdots \otimes M$$

k-krotny produkt tensorowy M z sobą. Mówimy wtedy o potędze tensorowej. Przyjmujemy że $M^{\otimes 0} = R$.

Niech

$$T(M) = \oplus_{k=0}^{\infty} M^{\otimes k}$$

Z definicji $T(M)$ jest R modułem. Na $T(M)$ możemy wprowadzić mnożenie definiując mnożenie z $M^{\otimes k} \times M^{\otimes l}$ w $M^{\otimes k+l}$ wzorem

$$(m_1 \otimes \dots m_k) \cdot (n_1 \otimes \dots n_l) = m_1 \otimes \dots m_k \otimes n_1 \otimes \dots n_l.$$

To mnożenie rozszerzamy dwuliniowo do mnożenia na $T(M)$. Łatwo sprawdzić że to mnożenie jest łączne. A więc $T(M)$ jest pierścieniem (zwykle nieprzemiennym) i algebrą łączną nad R.

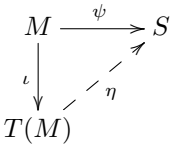
Lemat 1.10 *Dowolny homomorfizm ψ modułów z M w algebrę łączną S nad R jednoznacznie rozszerza się do homomorfizmu η algebr z $T(M)$ w S.*

Dowód: Bierzemy

$$\eta(m_1 \otimes \dots m_k) = \phi(m_1) \dots \phi(m_k)$$

Na k krotnym producie M jest to odwzorowanie k liniowe, więc ma jednoznaczne przedułużenie na $M^{\otimes k}$, co przez liniowość daje η na całym $T(M)$. Widać że jest to jedyna możliwa definicja, co daje jednoznaczność η. Z definicji jest to homomorfizm R-modułów. Łatwo sprawdzić że iloczym tensorów prostych przechodzi na iloczyn, co oznacza że η jest homomorfizmem pierścieni. □

Można to zilustrować następującym diagramem:

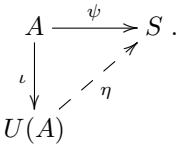


gdzie ι jest włożeniem tożsamościowym M w $T(M)$.

1.5 Uniwersalna algebra obwiednia

Niech A będzie algebrą Liego. Powiemy że algebra łączna $U(A)$ z odwzorowaniem $\iota : A \to U(A)$ które jest homomorfizmem algebr Liego z A w $U(A)$ potraktowane jako algebra Liego z komutatorem jako nawiasem Liego, jest uniwersalną algebrą obwiednią dla A jeśli dla dowolnego homomorfizmu ψ z A w algebrę łączną S traktowaną jako algebra Liego z komutatorem jako nawiasem Liego istnieje homomorfizm algebr łącznych η z $U(A)$ w S taki że $\psi = \eta \circ \iota$. Jak poprzednio, bezpośrednio z definicji wynika że $U(A)$ o ile istnieje to jest wyznaczone jednoznacznie z dokładnością do izomorfizmu.

Można to zilustrować diagramem



Lemat 1.11 *Uniwersalna algebra obwiednia $U(A)$ istnieje.*

Dowód: Działa ogólna konstrukcja przez podobiekt produktu. □

Uwaga: Mamy $U(A) = T(A)/I$ gdzie I to ideał w $T(A)$ generowany przez elementy postaci $x \otimes y - y \otimes x - [x, y]$. To daje nieco bardziej konkretną konstrukcję $U(A)$.

Lemat 1.12 *Mamy naturalną 1-1 odpowiedniość między modułami Liego nad A i modułami nad $U(A)$. Przy tym wolnym modułom Liego nad A odpowiadają moduły wolne nad $U(A)$.*

Uwaga: powyższy lemat oznacza że opisanie struktury wolnych modułów Liego jest równoważne opisaniu struktury $U(A)$.

Lemat 1.13 *Jeśli A jest modułem wolnym nad R z liniowo uporządkowaną bazą E, zaś G jest zbiorem to istnieje moduł Liego M generowany przez G który jest modułem wolnym nad R z bazą*

$$e_1 e_2 \dots e_k g$$

gdzie $e_1, e_2, \dots e_k$ przebiega wszystkie ciągi skończone elementów E takie że $e_1 \leq e_2 \leq \dots \leq e_k$ zaś g przebiega elementy G.

Dowód: W ramach sformułowania lematu podaliśmy bazę M, co jednoznacznie wyznacza strukturę M jako modułu nad R (w tym miejscu traktujemy $e_1 e_2 \dots e_k g$ jako symbole, ale dalej działanie zdefiniujemy tak że będzie to efekt działania na g). Trzeba jeszcze zadać działanie A na M (i sprawdzić że M faktycznie jest modułem Liego). Działanie wystarczy zdefiniować na elementach bazy A i M. Dla elementów bazy M wielkość k nazywamy rzędem elementu. Definicję robimy indukcyjnie z względu na rząd k. Przy tym dodatkowo pokażemy że dla $e_1 \leq e_2 \leq \dots \leq e_k$ i dowolnej permutacji α zbioru $\{1, \dots, k\}$ mamy

$$e_{\alpha(1)} e_{\alpha(2)} \dots e_{\alpha(k)} g = e_1 e_2 \dots e_k g$$

modulo elementy rzędu mniejszego niż k.

Dla $k = 0$ nie mamy wyboru, po prostu bierzemy

$$eg.$$

Zakładając że jest zdefiniowane działanie A na elementach bazy M aż do $k-1$ chcemy zdefininiować

$$h \cdot e_1 e_2 \dots e_k g.$$

Jeśli $h \leq e_1$ to bierzemy

$$h e_1 e_2 \dots e_k g$$

(jest to element bazowy). W przeciwnym razie, bierzemy

$$[h, e_1] e_2 \dots e_k g + e_1 \cdot (h \cdot e_2 \dots e_k g).$$

Pierwszy składnik to mnożenie elementu z mniejszym rzędem przez element A, co już było zdefiniowane. Podobnie, produkt z nawiasach w drugim składniku ma mniejszy rząd, więc ten produkt jest dobrze zdefiniowany, przy tym jest to

$$e_{l_1} \dots e_{l_k} g$$

gdzie $e_{l_1}, \ldots, e_{l_k}$ jest uporządkowaną permutacją $h, e_2, \ldots, e_k$ plus człony niższego rzędu. A więc $e_1 \leq e_{l_1}$, czyli produkt z e_1 sprowadza się do już zdefiniowanych przypadków.

Zauważmy teraz że nasza definicja ma własność podaną wyżej: produkt $e_1 \ldots e_k g$ daje nam produkt uporządkowanch elementów bazy plus człony niższego rzędu.

Jako że działanie definiowaliśmy na bazach to jest ono automatycznie dwuliniowe. A więc pozostaje sprawdzić zachowanie komutatora. Rozważmy elementy f i h z bazy A oraz element

$$w = e_1 e_2 \ldots e_k g$$

z bazy M. Bez utraty ogólności możemy zakładać że $f < h$ (przypadek $f = h$ jest trywialny, zaś $f > h$ sprowadza się do powyższego).

Musimy rozpatrzeć dwa przypadki: $f \leq e_1$ (lub $k = 0$) i $e_1 < f$. Piszemy $w = e_1 w_1$ gdzie w_1 jest zdefininiowane przez tą równość. Jeśli $f \leq e_1$ to fw jest elementem bazy. Podobnie gdy $w = g$ (to znaczy $k = 0$). Czyli

$$hfw = f(hw) + [h, f]w.$$

A więc

$$fhw - hfw = fhw - fhw - [h, f]w = [f, h]w$$

co daje tożsamość dla komutatora w tym przypadku.

W przeciwnym przypadku rozpatrujemy

$$[f, h]e_1 w_1 = [[f, h], e_1]w_1 + e_1[f, h]w_1$$

gdzie równość wynika z założenia indukcyjnego. Zauważmy że mamy równości

$$[e_1, f]hw_1 = e_1 fhw_1 - fe_1 hw_1,$$

$$[e_1, h]fw_1 = e_1 hfw_1 - he_1 fw_1.$$

Mianowicie, z własności działania hw_1 to suma elementu rzędu k gdzie piewszy czynnik jest większy lub równy e_1 i elementów niższego rzędu. Dla elementów niższego rzędu równość mamy z założenia indukcyjnego. Dla członu rzędu k pierwszy czynnik większy lub równy e_1 oznacza że jesteśmy w już udowodnionym przypadku. Podobnie pokazujemy drugą równość.

Na mocy tożsamości Jakobiego

$$[[f, h], e_1] = -[e_1, [f, h]] = -[[e_1, f], h] - [f, [e_1, h]]$$

$$= [h, [e_1, f]] - [f, [e_1, h]].$$

A więc z założenia inducyjnego

$$[[f, h], e_1]w_1 = [h, [e_1, f]]w_1 - [f, [e_1, h]]w_1$$

$$= h[e_1, f]w_1 - [e_1, f]hw_1 - f[e_1, h]w_1 + [e_1, h]fw_1.$$

Człony $[e_1, f]w_1$ i $[e_1, h]w_1$ rozpisujemy z założenia indukcyjnego, pozostałe dwa z wcześniej uzasadnionych równości otrzymując

$$[[f, h], e_1]w_1$$

$$= he_1fw_1 - hfe_1w_1 - e_1fhw_1 + fe_1hw_1 - fe_1hw_1 + fhe_1w_1 + e_1hfw_1 - he_1fw_1$$
$$= fhe_1w_1 - hfe_1w_1 - e_1fhw_1 + e_1hfw_1$$

Razem

$$[f,h]e_1w_1 = [[f,h],e_1]w_1 + e_1[f,h]w_1$$
$$= fhe_1w_1 - hfe_1w_1 - e_1fhw_1 + e_1hfw_1 + e_1fhw_1 - e_1hfw_1$$
$$= ghe_1w_1 - hge_1w_1$$

gdzie rozpisaliśmy $[f,h]w_1$ z założenia indukcyjnego. A więc również w obecnym przypadku otrzymaliśmy równość dla komutatora

$$[f,h]w = fhw - hfw.$$

□

Lemat 1.14 *Moduł M z poprzedniego lematu jest wolnym modułem Liego.*

Dowód: Zauważmy najpierw że elementy postaci

$$e_1e_2\dots e_kg$$

z $e_1 \le e_2 \le \dots \le e_k$, $e_i \in E$ generują wolny moduł Liego W. Mianowicie, jest oczywiste że dowolne (nieuporządkowane) podukty jak wyżej generują W. Ale oznaczając przez W_k podmoduł nad R generowany przez produkty długości mniejszej lub równej k widać że $W_{k-1} \subset W_k$ i że modulo W_{k-1} możemy zmieniać kolejność czynnków. Czyli również uporządkowane produkty generują W_k. Jako że W jest sumą W_k daje wynik o generowaniu.

Rozważny teraz odwzorowanie z wolnego modułu Liego w moduł M które jest tożsamością na G. Generatory W podane wyżej przechodzą na elementy linowo niezależne w M. A więc generatory wyżej muszą być liniowo niezależne w W, czyli są bazą i W jest modułem wolnym nad R. Ale to oznacza że homomorfizm z W w M przeprowadza bazę na bazę, czyli jest izomorfizmem. A więc M jest wolnym modułem Liego. □

Lemat 1.15 *(twierdzenie Poincarego-Birkhoffa-Witta) Niech A będzie algebrą Liego która jest modułem wolnym nad R z liniowo uporządkowaną bazą E. Wtedy $U(A)$ jest modułem wolnym nad R, włożenie ι z A w $U(A)$ jest różnowartościowe i elementy*

$$e_1e_2\dots e_k$$

stanowią bazę $U(A)$. Powyżej $e_i \in i(E)$, $e_1 \le e_2 \le \dots \le e_k$ zaś na $\iota(E)$ rozpatrujemy porządek przetransportowany przez ι z E.

Dowód: Wolny moduł Liego M nad A z jednym generatorem jest naturalnie izomorficzny z modułem wolnym nad $U(A)$ z jednym generatorem który z kolei jest izomorficzny z $U(A)$. Przy tym element

$$e_1e_2\dots e_kg \in M$$

odpowiada

$$\iota(e_1)\iota(e_2)\dots\iota(e_k) \in U(A).$$

A więc skoro mamy izomorfizm to produkty $\iota(e_1)\dots\iota(e_k)$ są bazą $U(A)$. W szczególności ι jest różnowartościowe. $\square$