Wydział Matematyki i Informatyki
Uniwersytetu im. Adama Mickiewicza

Piotr Rzonsowski

# Arytmetyka Grupy Mordella-Weila na rozmaitości abelowej nad ciałem skończenie generowanym nad $\mathbb{Q}$.

Rozprawa doktorska
napisana pod kierunkiem
Prof. dr hab. Grzegorza Banaszaka

Poznań 2010

# Wstęp

Niniejsza rozprawa jest poświęcona rozwiązaniu dwóch problemów.

Pierwszym problemem jaki będę rozważał w rozprawie jest problem nośnika. Problem jako pierwszy sformułował P. Erdös w następujący sposób:

**Pytanie.** *Załóżmy, że dla pewnych liczb całkowitych $x$, $y$ następujący warunek jest spełniony:*

$$Supp(x^n - 1) = Supp(y^n - 1),$$

*dla wszystkich liczb naturalnych $n$. Czy z tego wynika, że $x = y$.*

Problem ten został rozwiązany przez C. Corrales-Rodrigáñez i R. Schoof w [7].

Następnie problem ten został uogólniony na rozmaitości abelowe nad ciałem liczbowym i był rozwiązany dla szczególnych klas rozmaitości abelowych przez Banaszaka, Gajdę, Krasonia, Khare, Prasada i innych. Jednakże rozwiązany został w pełnej ogólności przez Larsena w [16]. Podał on następujące twierdzenie:

**Twierdzenie 1.** *Niech $F$ będzie ciałem liczbowym, $\mathcal{O}_F$ będzie pierścieniem liczb całkowitych. Niech $A$ będzie rozmaitością abelową, $R := End_F(A)$, $P, Q \in A(F)$. Załóżmy, że dla każdego $n \in \mathbb{Z}$ i dla prawie wszystkich $v \in \mathcal{O}_F$ zachodzi:*

$$nP \equiv 0 \mod v \implies nQ \equiv 0 \mod v$$

*Istnieje wtedy $k \in \mathbb{N}$ i endomorfizm $\varphi \in End_F(A)$ taki, że*

$$\varphi(P) = kQ$$

W swojej rozprawie rozszerzam ten wynik dla abelowych rozmaitości nad ciałem skończenie generowanym nad $\mathbb{Q}$. Co ważne dowód zawarty w tej pracy jest znacząco inny od tego zaproponowanego przez Larsena i znacznie krótszy choć obejmuje również przypadek ciał liczbowych.

Drugi problem dotyczy liniowej zależności punktów na rozmaitości abelowej. Pytanie to sformułował W. Gajda w 2002 r. w następujący sposób:

**Pytanie.** *Czy dla rozmaitości abelowej $A$ i jej podgrupy $\Lambda$ następujące warunki są równoważne:*

- $P \in \Lambda$
- $r_v(P) \in r_v(\Lambda)$, *dla prawie wszystkich* $v \in \mathcal{O}_F$

Problematyka ta była rozważana w przeciągu kilku następnych lat w wielu pracach [2], [3], [4], [11], [36]. Jednakże wszystkie wyniki uzyskiwane w tych pracach były dla rozmaitości abelowych nad ciałem liczbowym. W rozprawie rozszerzam ten problem na ciała skończenie generowane nad $\mathbb{Q}$.

Teraz omówię pokrótce zawartość poszczególnych rozdziałów.

W rozdziale pierwszym na początku przedstawiam podstawowe definicje i własności rozmaitości abelowych. Następnie rozważam zagadnienia związane z schematami abelowymi. W drugiej części przedstawiam twierdzenia związane z l-adyczną reprezentacją rozmaitości abelowej.

W rozdziale 2 badam odwzorowanie redukcji i jego własności, jest to fundamentalny rozdział, który pozwala nam poznać poszczególne własności odwzorowania redukcji. Poczynając od tego, że odwzorowanie to jest iniektywne na częściach l-torsyjnych jak również to, że możemy redukować punkty nietorsyjne na punkty o dowolnym rzędzie.

W rozdziale 3 jest rozważany problem liniowej zależności. Wprowadzamy w nim metodę redukcji rozmaitości abelowej do przypadków rozmaitości prostych a następnie ją ″sklejamy″ i uzyskujemy końcowy rezultat. Metody zawarte w tym rozdziale są uogólnieniem metod zawartych w pracach [1] i [4].

W rozdziale 4 rozwiązujemy problem nośnika na rozmaitości abelowej. Używając metod rozwiniętych w rozdziale 3 uogólniamy wynik z pracy [6], który rozszerzam na ciała skończenie generowane nad $\mathbb{Q}$. Dodatkowo pokazujemy, że twierdzenie z pracy [5] również zachodzi dla tych ciał.

*Podziękowania*

W tym miejscu chciałbym serdecznie podziękować mojemu Nauczycielowi i Promotorowi rozprawy prof. dr. hab. Grzegorzowi Banaszakowi za inspiracje matematyczne, cierpliwość oraz niezliczone godziny rozmów.

Słowa podziękowania kieruję również w stronę moich Rodziców i Żony, za wsparcie w realizacji trudnych celów oraz wszelką pomoc w trudnych sytuacjach.

# Spis treści

Rozdział 1

# Preliminaria

## Oznaczenia

- $K$-ciało skończenie generowane nad $\mathbb{Q}$;
- $A$ rozmaitość abelowa nad ciałem $K$;
- $A[l^k]$ jądro odwzorowania $l^k : A \to A$;
- $A[l^\infty] = \bigcup_k A[l^k]$;
- $T_l(A) := \varprojlim_k A[l^k]$- moduł Tate'a rozmaitości abelowej $A$;
- $K_{l^\infty} = K\left(A[l^\infty]\right)$;
- $G_K = Gal\left(\overline{K}/K\right)$;
- $\mathcal{A}$- schemat abelowy nad schematem $S$;
- $k(s)$ ciało reszt punktu $s \in S$;
- $g_s := Gal(\overline{k(s)}/k(s))$;
- $\mathcal{A}_s := \mathcal{A} \times \operatorname{Spec} k(s)$ oznacza włókno $\mathcal{A}$ nad $s \in S$;
- $\operatorname{End}^0(A) = \operatorname{End}(A) \otimes \mathbb{Q}$;
- $\pi_1(S) := \pi_1^{et}(S)$ fundamentalna grupa étalna schematu $S$;
- $c := |A(K)|_{tor}$;
- $\Omega := cA(K)$;
- $\Lambda$ podgrupa $A(K)$.

## 1.1. Rozmaitości abelowe

Na początku zacznijmy od pojęcia rozmaitości abelowej i kilku jej własności.

**Definicja 1.** ***Rozmaitością grupową*** *nad ciałem $K$ będziemy nazywać rozmaitość algebraiczną $G$ wraz z morfizmami*

$$m : G \times G \to G \qquad \textit{mnożenie};$$

$$i : G \to G \qquad \textit{odwrotność};$$

*i elementem $e \in G(K)$ tworzącymi strukturę grupy na $G(\overline{K})$ z elementem neutralnym $e$. Czyli przemienne są następujące diagramy:*

*i) łączność*

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{Id_G \times m} & G \times G \\ \downarrow{\scriptstyle m \times Id_G} & & {\scriptstyle m}\downarrow \\ G \times G & \xrightarrow{m} & G \end{array}$$

*ii) Element neutralny*

$$\begin{array}{ccc} \{e\} \times G & \xrightarrow{e \times Id_G} & G \times G \\ \downarrow{\scriptstyle \pi_2} & & {\scriptstyle m}\downarrow \\ G & \xrightarrow{=} & G \end{array} \qquad \begin{array}{ccc} G \times \{e\} & \xrightarrow{Id_G \times e} & G \times G \\ \downarrow{\scriptstyle \pi_1} & & {\scriptstyle m}\downarrow \\ G & \xrightarrow{=} & G \end{array}$$

*iii) element odwrotny*

$$\begin{array}{ccc} G & \longrightarrow & \{e\} \\ \downarrow{\scriptstyle (Id_G, i)} & & {\scriptstyle e}\downarrow \\ G \times G & \xrightarrow{m} & G \end{array} \qquad \begin{array}{ccc} G & \longrightarrow & \{e\} \\ \downarrow{\scriptstyle (i, Id_G)} & & {\scriptstyle e}\downarrow \\ G \times G & \xrightarrow{m} & G \end{array}$$

**Definicja 2.** *Zupełną rozmaitość grupową będziemy nazywać* ***rozmaitością abelową****.*

**Twierdzenie 1.1** (Rigidity)**.** *Niech $f : V \times W \to U$ będzie morfizmem rozmaitości algebraicznych nad ciałem $K$. Jeżeli $V$ jest zupełną rozmaitością algebraiczną i*

$$f(V \times \{w_0\}) = \{u_0\} = f(\{v_0\} \times W),$$

*dla pewnych $u_0 \in U$, $v_0 \in V$, $w_0 \in W$. Wtedy $f(V \times W) = \{u_0\}$.*

*Dowód.* [18, Thm 2.1, str 104] □

**Wniosek 1.1.**
- *Każdy morfizm $f : A \to B$ rozmaitości abelowych jest złożeniem homomorfizmu $h : A \to B$ i translacji $t_a : B \to B$, $a = -f(0)$.*
- *Działanie grupowe na rozmaitości abelowej jest wyznaczone jednoznacznie poprzez wybór elementu neutralnego.*
- *Działanie grupowe na rozmaitości abelowej jest przemienne.*

**Twierdzenie 1.2.** *Każda rozmaitość abelowa jest projektywna.*

*Dowód.* [18, Thm 7.1, str 113] □

## 1.2. Izogenie

Teraz podam definicję i podstawowe własności izogenii. Ten rodzaj odwzorowania między rozmaitościami abelowymi będzie odgrywał fundamentalną rolę w dalszej części pracy.

**Definicja 3.** *Niech $f : A \to B$ będzie homomorfizmem rozmaitości abelowych. Jeżeli $f$ będzie odwzorowaniem surjektywnym które ma skończone jądro to będziemy je nazywać **izogenią**.*

*Przez **stopień izogenii** $f$ (ozn $\deg f$) będziemy rozumieć rząd jądra odwzorowania $f$ (jako skończonego schematu grupowego).*

**Lemat 1.1.** *Niech $f : A \to B$ będzie homomorfizmem rozmaitości abelowych, wtedy następujące warunki są równoważne:*

**i)** *$f$ jest izogenią;*

**ii)** *$dimA = dimB$ i $f$ jest suriekcją;*

**iii)** *$dimA = dimB$ i jądro $f$ jest skończonym schematem grupowym;*

**iv)** *$f$ jest skończone, płaskie i surjektywne.*

Niech teraz $n_A$ oznacza odwzorowanie z $A$ do $A$ zadane wzorem $a \mapsto na$, gdzie $na = \underbrace{a + a + \cdots + a}_{n}$.

**Twierdzenie 1.3.** *Niech $A$ będzie rozmaitością abelową wymiaru $g$, $n \in \mathbb{N}$. Wtedy $n_A : A \to A$ jest izogenią stopnia $n^{2g}$ i jest ona étalna wtedy i tylko wtedy, gdy charakterystyka ciała nie dzieli $n$.*

*Dowód.* [18, Thm 8.2, str 115] □

**Uwaga 1.2.1.** *Niech $f : A \to B$ będzie izogenią stopnia $n = \deg f$. Wtedy istnieje izogenia $g : B \to A$ dla której zachodzi równość $n_A = f \circ g$. Izogenie $g$ będziemy nazywać **izogenią dualną**.*

**Uwaga 1.2.2.** *Jeżeli $K$ ciałem i $n$ nie dzieli charakterystyki ciała wtedy jądro $A[n]$ izogenii $n_A : A \to A$ posiada $n^{2g}$ elementów. Ponieważ jest to prawdą dla każdego $n'|n$, więc $A[n]$ jest wolnym $\mathbb{Z}/n\mathbb{Z}$-modułem rangi $2g$. Dlatego możemy zdefiniować* ***moduł Tate'a*** *jako:*

$$T_l(A) = \varprojlim_k A[l^k],$$

*gdzie $A[l^k] = \{P \in A(\overline{K}) \ : \ l^n P = 0\}$*

**Twierdzenie 1.4** (Poincare irreducibility)**.** *Jeżeli $A$ jest rozmaitością abelową, a $Y$ jest podrozmaitością abelową, wtedy istnieje podrozmaitość abelowa $Z$ taka, że $Y \cap Z$ jest zbiorem skończonym oraz $Y + Z = A$. Innymi słowy rozmaitość abelowa $A$ jest izogeniczna z $Y \times Z$.*

*Dowód.* [20, Rozdział 19, Tw 1, Str. 173] □

**Wniosek 1.2.** *Dowolna rozmaitość abelowa $A$ jest izogeniczna z produktem $A_1^{e_1} \times \cdots \times A_s^{e_s}$, gdzie $A_i$ są podrozmaitościami prostymi, które nie są izogeniczne między sobą. Rozmaitości $A_i$ z dokładnością do izogenii oraz stałe $e_i$ są wyznaczone jednoznacznie.*

*Dowód.* [20, Rozdział 19, Wniosek 1, Str 174] □

## 1.3. Pierścień Endomorfizmów

Teraz przejdziemy do omówienia pierścienia endomorfizmów rozmaitości abelowej. Dzięki jego strukturze będziemy w stanie rozwiązać problemy omawiane we wstępie.

**Lemat 1.2.** *Dla dowolnej liczby pierwszej $l \neq char(K)$ odwzorowanie*

$$\mathrm{Hom}(A, B) \to \mathrm{Hom}_{\mathbb{Z}_l}(T_l(A), T_l(B))$$

*jest iniekcją, w szczególności $\mathrm{Hom}(A, B)$ jest beztorsyjny.*

*Dowód.* [18, Lemat 12.3 str 122] □

Przyjmijmy teraz oznaczenie $\mathrm{End}^0(A) := \mathrm{End}(A) \otimes Q$. Jeżeli $A$ jest rozmaitością abelową wymiaru $g$ nad $K$, wtedy dla każdego $\varphi \in \mathrm{End}(A)$ definiujemy jego stopień następująco: jeżeli $\varphi$ jest izogenią to naszym stopniem jest stopień izogenii (zdefiniowany wcześniej), a jeżeli nie to $deg\varphi = 0$. Ponieważ $deg(n\varphi) = n^{2g} deg(\varphi)$ to możemy rozszerzyć definicję na $\mathrm{End}^0(A)$, następująco. Jeżeli $n\varphi \in \mathrm{End}(A)$ to $deg(\varphi) = \frac{1}{n^{2g}} deg(n\varphi)$.

**Lemat 1.3.** *Funkcja $\varphi : \mathrm{End}^0(A) \to \mathbb{Q}$, $\varphi \mapsto deg\,\varphi$ jest jednorodną funkcją wielomianową stopnia $2g$ na $\mathrm{End}^0(A)$.*

*Dowód.* [18, Prop 12.4, str 123] □

**Wniosek 1.3.** *Z powyższego lematu mamy, że dla każdego* $\alpha \in End^0(A)$ *istnieje wielomian* $P_\alpha(X) \in \mathbb{Q}[X]$ *stopnia* $2g$*, taki, że dla każdej liczby wymiernej* $r$ *mamy* $P_\alpha(r) = deg(\alpha - r_A)$*. Wielomian* $P_\alpha(X)$ *nazywamy* ***wielomianem charakterystycznym endomorfizmu*** $\alpha$ *który ma postać*

$$P_\alpha(X) = X^{2g} - tr(\alpha)X^{2g-1} + \cdots + deg\ \alpha.$$

**Lemat 1.4.** *Dla każdej liczby pierwszej* $l \neq charK$*,* $P_\alpha(X)$ *jest wielomianem charakterystycznym* $\alpha$ *działającego na* $T_lA \otimes \mathbb{Q}_l$*. Stąd ślad i stopień* $\alpha$ *jest śladem i wyznacznikiem* $\alpha$ *działającego na* $T_lA \otimes \mathbb{Q}_l$

*Dowód.* [18, Prop 12.9, str 125] □

**Lemat 1.5.** *Niech* $\varphi \in \mathrm{Hom}(A, B)$*, jeżeli* $\varphi$ *jest podzielne przez* $l^n$ *w* $\mathrm{Hom}(T_lA, T_lB)$*, wtedy jest on podzielny przez* $l^n$ *w* $\mathrm{Hom}(A, B)$*.*

*Dowód.* [18, Lem 12.6, str 124] □

**Lemat 1.6.** *Jeżeli* $A$ *jest prostą rozmaitością abelową, wtedy*

$$\mathrm{End}_{\mathbb{Z}_l} A \otimes \mathbb{Z}_l \to \mathrm{End}(T_lA)$$

*jest iniekcją.*

*Dowód.* [18, Lem 12.7, str 124] □

**Twierdzenie 1.5.** *Dla każdych rozmaitości abelowych* $A$ *i* $B$*,* $\mathrm{Hom}(A, B)$ *jest wolnym* $\mathbb{Z}$*-modułem o skończonej randze mniejszej bądź równej* $4dim(A)dim(B)$*. Dla każdej liczby pierwszej* $l \neq char(K)$*, odwzorowanie:*

$$\mathrm{Hom}(A, B) \otimes \mathbb{Z}_l \to \mathrm{Hom}(T_l(A), T_l(B))$$

*jest iniekcją z beztorsyjnym kojądrem.*

*Dowód.* [18, Them 12.5, str 123] □

Z twierdzenia 1.4 i wniosku 1.2 każda rozmaitość abelowa jest izogeniczna z

$$A = \prod_{i=1}^{t} A_i^{e_i}.$$

Z tego powodu dostajemy

$$\mathrm{End}^0(A) = \prod_{i=1}^{t} M_{e_i}(\mathrm{End}^0(A_i)),$$

gdzie $\mathrm{End}^0(A_i) := \mathrm{End}(A_i) \otimes \mathbb{Q}$ jest algebrą z dzieleniem. Zatem dla każdej rozmaitości abelowej $A$ pierścień $\mathrm{End}^0(A)$ jest algebrą półprostą, skończenie wymiarową nad $\mathbb{Q}$. Dlatego w następnym podrozdziale zamierzam opisać pewne własności algebr półprostych i modułów nad nimi, które są zawarte w pracy [4].

## 1.4. Półproste algebry

Niech $D$ będzie algebrą z dzieleniem, a $K_i \subset M_e(D)$ oznacza lewy ideał w $M_e(D)$ który złożony jest z macierzy postaci:

$$\widetilde{\alpha}_i := \begin{bmatrix} 0 & \dots a_{1i} & \dots & 0 \\ 0 & \dots a_{2i} & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & \dots a_{e\,i} & \dots & 0 \end{bmatrix} \in K_i$$

Niech $W$ będzie przestrzenią wektorową nad $D$ i $e \in \mathbb{N}$. Wtedy $W^e := \underbrace{W \times \cdots \times W}_{e-razy}$ jest $M_e(D)$-modułem. Dla $\omega \in W$ oznaczmy :

$$\widetilde{\omega} := \begin{bmatrix} \omega \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

**Lemat 1.7.** *Każdy niezerowy prosty podmoduł $M_e(D)$-modułu $W^e$ jest postaci*

$$K_1\widetilde{\omega} = \{\widetilde{\alpha_1}\widetilde{\omega}, \quad \widetilde{\alpha_1} \in K_1\} = \{ \begin{bmatrix} a_{11}\omega \\ a_{21}\omega \\ \vdots \\ a_{e1}\omega \end{bmatrix}, \quad a_{i1} \in D, \quad 1 \leqslant i \leqslant e\}$$

*dla pewnego $\omega$.*

*Dowód.* [4, str 8] □

Niech $D_i$ będą skończenie generowanymi algebrami z dzieleniem nad $\mathbb{Q}$, dla każdego $1 \leqslant i \leqslant t$. Przyjmijmy następujące oznaczenia:

$$\mathbb{D} := \prod_{i=1}^{t} D_i$$

$$\mathbb{M}_e(\mathbb{D}) = \prod_{i=1}^{t} M_{e_i}(D_i), \qquad e = (e_1, e_2, \dots, e_t).$$

Jeżeli $W_i$ jest przestrzenią wektorową nad $D_i$, dla wszystkich $i = 1, 2, \ldots, t$ to $W := \bigoplus_{i=1}^{t} W_i^{e_i}$ ma strukturę $\mathbb{M}_e(\mathbb{D})$-modułu.

**Wniosek 1.4.** *Każdy prosty niezerowy $\mathbb{M}_e(\mathbb{D})$-podmoduł modułu $W = \bigoplus_{i=1}^{t} W_i^{e_i}$ jest następującej postaci:*

$$K(j)_1\widetilde{\omega(j)} = \{\widetilde{\alpha(j)}_1\widetilde{\omega(j)} : \quad \widetilde{\alpha(j)}_1 \in K(j)_1\} = \{\begin{bmatrix} a_{11}\omega(j) \\ a_{21}\omega(j) \\ \vdots \\ a_{e1}\omega(j) \end{bmatrix}, \quad a_{k1} \in D_j, \quad 1 \leqslant k \leqslant e_j\},$$

*dla pewnego $1 \leqslant j \leqslant t$ i $\omega(j) \in W_j$, gdzie $K(j)_1 \subset M_{e_j}(D_j)$ oznacza ideał w $M_{e_j}(D_j)$ który zawiera pierwszą kolumnę macierzy.*

Niech $D_i$ będzie skończenie wymiarową algebrą z dzieleniem nad $\mathbb{Q}$, dla każdego $1 \leqslant i \leqslant t$. Wtedy homomorfizm śladu: $\mathrm{tr}_i \ : \ M_{e_i}(D_i) \to \mathbb{Q}$, dla $i = 1, 2, \ldots, t$, daje nam homomorfizm śladu: $\mathrm{tr} \ : \ \mathbb{M}_e(\mathbb{D}) \to \mathbb{Q}$, gdzie $\mathrm{tr} := \sum_{i=1}^{t} \mathrm{tr}_i$. Niech $W_i$ będą skończenie generowanymi przestrzeniami wektorowymi nad $D_i$ odpowiednio dla $1 \leqslant i \leqslant t$. Wtedy $W$ jest w naturalny sposób skończenie generowanym $\mathbb{M}_e(\mathbb{D})$-modułem i homomorfizm $tr$ daje nam odwzorowanie między przestrzeniami wektorowymi nad $\mathbb{Q}$:

$$\mathrm{tr} \ : \ \mathrm{Hom}_{\mathbb{M}_e(\mathbb{D})}(W, \mathbb{M}_e(\mathbb{D})) \to \mathrm{Hom}_{\mathbb{Q}}(W, \mathbb{Q}) \tag{1.1}$$

**Lemat 1.8.** *Odwzorowanie śladu zdefiniowane powyżej* (1.1) *jest izomorfizmem.*

*Dowód.* [4, str 9] □

**Uwaga 1.4.1.** *Ponieważ $\mathbb{M}_e(\mathbb{D})$ jest półprostą algebrą, dlatego $W$ jest półprostym modułem, a więc dla każdego $\widetilde{\pi} \in \mathrm{Hom}_{\mathbb{M}_e(\mathbb{D})}(W, \ \mathbb{M}_e(\mathbb{D}))$ istnieje $\mathbb{M}_e(\mathbb{D})$-homomorfizm $\widetilde{s} \ : \ Im \ \widetilde{\pi} \to W$, dla którego zachodzi $\widetilde{\pi} \circ \widetilde{s} = Id$. Dzięki izomorfizmom:*

$$\bigoplus_{i=1}^{t} \mathrm{Hom}_{M_{e_i}(D_i)}(W_i^{e_i}, M_{e_i}(D_i)) \cong \mathrm{Hom}_{\mathbb{M}_e(\mathbb{D})}(W, \mathbb{M}_e(\mathbb{D}))$$

$$\bigoplus_{i=1}^{t} \mathrm{Hom}_{\mathbb{Q}}(W_i^{e_1}, \mathbb{Q}) \cong \mathrm{Hom}_{\mathbb{Q}}(W, \mathbb{Q})$$

*możemy zapisać: $\widetilde{\pi} = \prod_{i=1}^{t} \widetilde{\pi(i)}$, dla pewnych $\widetilde{\pi(i)} \in \mathrm{Hom}_{M_{e_i}(D_i)}(W_i^{e_i}, \ M_{e_i}(D_i))$. Mamy również $Im \ (\widetilde{\pi}) = \prod_{i=1}^{t} Im \ \widetilde{\pi(i)}$, teraz dla każdego $\widetilde{\pi(i)}$ możemy znaleźć $M_{e_i}(D_i)$-homomorfizm $\widetilde{s(i)} \ : \ Im \ \widetilde{\pi(i)} \to W_i^{e_i}$ taki, że $\widetilde{\pi(i)} \circ \widetilde{s(i)} = Id$ i $\widetilde{s} = \bigoplus_{i=1}^{t} \widetilde{s(i)}$, ponieważ $M_{e_i}(D_i)$ jest prostą algebrą.*

**Uwaga 1.4.2.** *Na mocy twierdzenia* [25, twierdzenie 7.3, str 91] *każdy prosty $M_{e_i}(D_i)$-podmoduł $M_{e_i}(D_i)$ jest izomorficzny z $K(i)_1$. Ponieważ mamy $\dim_{D_i} M_{e_i}(D_i) = e_i^2$ oraz $\dim_{D_i} K(i)_1 = e_i$, dlatego $M_{e_i}(D_i)$ jest sumą prostą $e_i$ prostych $M_{e_i}(D_i)$-podmodułów które są w jednej klasie izomorfizmu jako $M_{e_i}(D_i)$-moduły. Stąd każdy $M_{e_i}(D_i)$-podmoduł w $M_{e_i}(D_i)$ jest sumą prostą co najwyżej $e_i$ prostych $M_{e_i}(D_i)$-podmodułów.*

.

## 1.5. Inwolucja Rosati

Teraz podam kilka definicji powiązanych z rozmaitościami abelowymi i pierścieniem endomorfizmów.

**Definicja 4.** *Przez $Pic^0(A)$ będziemy rozumieć grupę klas izomorfizmów odwracalnych snopów na $A$ spełniających jeden z równoważnych warunków* ([18, Rozdział 9, Prop 9.2])*:*

**i)** $A = \{a \in A :$ *obcięcie snopu* $m^*\mathcal{L} \otimes q^*\mathcal{L}^{-1}$ *do* $\{a\} \times A$ *jest snopem trywialnym* $\}$;

**ii)** $t_a^*\mathcal{L} \approx \mathcal{L}$ *na* $A_{\overline{K}}$ *dla wszystkich* $a \in A(\overline{K})$;

**iii)** $m^*\mathcal{L} \approx p^*\mathcal{L} \otimes q^*\mathcal{L}$;

*gdzie $\mathcal{L}$ jest odwracalnym snopem na $A$, $t_a : A \to A$ jest translacją o element $a \in A$, a $p, q : A \times A \to A$ są projekcjami pierwszej, drugiej współrzędnej odpowiednio.*

**Definicja 5.** *Rozmaitość abelową $A^\vee$ nazywamy* ***dualną*** *do $A$, a snop $\mathcal{P}$ snopem* ***Poincaré*** *jeżeli*

**i)** *$\mathcal{P}|_{\{0\} \times A^\vee}$ jest snopem trywialnym leżącym w $Pic^0(A(K(a)))$ dla wszystkich $a \in A^\vee$;*

**ii)** *Dla każdego $K$-schematu $T$ i snopu odwracalnego $\mathcal{L}$ na $A \times T$ takiego, że $\mathcal{L}|_{\{0\} \times T}$ jest trywialny i $\mathcal{L}|_{A \times \{t\}}$ leży w $Pic^0(A(K(t)))$ dla wszystkich $t \in T$, istnieje wtedy jednoznacznie wyznaczony morfizm $f : T \to A^\vee$ taki, że $(1 \times f)^*\mathcal{P} \approx \mathcal{L}$.*

Dla rozmaitości abelowej $A$ i liczby całkowitej $m$ mamy **przekształcenie dwuliniowe Weil'a** ( zobacz np. [18, str 131]):

$$\overline{e}_m : A[m](\overline{K}) \times A^\vee[m](\overline{K}) \to \mu_m.$$

W poniższym lemacie zawarte są podstawowe własności tego przekształcenia.

**Lemat 1.9.** *Niech $\overline{e}_m$ będzie przekształceniem dwuliniowym Weil'a oraz niech $f : A \to B$ będzie homomorfizmem rozmaitości abelowych. Wtedy $\overline{e}_m$ posiada następujące własności:*

**i)** *Niech* $n, m \in \mathbb{Z}$ *i nie dzielą charakterystyki ciała* $K$, $a \in A[mn](\overline{K})$, $a' \in A^{\vee}[mn](\overline{K})$ *wtedy:*

$$\overline{e}_{mn}(a, a')^n = \overline{e}_m(na, na');$$

**ii)** $\overline{e}_m(a, f^{\vee}(b)) = \overline{e}_m(f(a), b), \qquad a \in A[m],\ b \in B^{\vee}[m]$

**iii)** $e_l(a, f^{\vee}b) = e_l(f(a), b) \qquad a \in T_lA,\ b \in T_lB;$

**iv)** $\overline{e}_m$ *jest niezdegenerowanym przekształceniem liniowym.*

*gdzie* $f^{\vee} : B^{\vee} \to A^{\vee}$ *jest odwzorowaniem dualnym.*

**Definicja 6.** *Oznaczmy homomorfizm* $\varphi_{\mathcal{L}} : A(k) \to PicA$, $a \mapsto t_a^*\mathcal{L} \otimes \mathcal{L}^{-1}$. *Izogenię* $\lambda : A \to A^{\vee}$ *taką, że* $\lambda_{\overline{k}} = \varphi_{\mathcal{L}}$ *dla pewnego szerokiego odwracalnego snopa na* $A_{\mathcal{L}}$, *będziemy nazywać* ***polaryzacją*** *rozmaitości* $A$.

**Definicja 7.** *Ustalmy polaryzację* $\lambda$ *na* $A$. ***Inwolucją Rosati*** *na* $\mathrm{End}^0 A$ *związaną z polaryzacją* $\lambda$ *nazywamy odwzorowanie:*

$$\dagger \ : \ \mathrm{End}^0(A) \to \mathrm{End}^0(A);$$

$$\alpha \mapsto \alpha^{\dagger} = \lambda^{-1} \circ \alpha^{\vee} \circ \lambda$$

## 1.6. Schematy abelowe

**Definicja 8.** *Niech* $S$ *będzie schematem. Schemat grupowy* $\pi : \mathcal{A} \to S$ *nad* $S$ *nazywamy* ***schematem abelowym***, *jeżeli* $\pi$ *jest właściwy, gładki i włókna* $\pi$ *są spójne.*

**Twierdzenie 1.6** (Rigidity)**.** *Niech* $S$ *będzie spójnym schematem,* $\pi : \mathcal{V} \to S$ *będzie właściwym płaskim odwzorowaniem którego włókna są rozmaitościami algebraicznymi. Niech* $\pi' : \mathcal{V}' \to S$ *będzie drugim* $S$*-schematem, a* $f : \mathcal{V} \to \mathcal{V}'$ *będzie morfizmem* $S$*-schematów. Jeżeli dla jakiegoś punktu* $s \in S$ *obraz* $\mathcal{V}_s$ *w* $\mathcal{V}'_s$ *jest pojedynczym punktem, wtedy istnieje odwzorowanie* $s' : S \to \mathcal{V}'$ *takie, że* $f = s'\pi$.

*Dowód.* [21, 6.1] □

**Wniosek 1.5. i)** *Każdy morfizm schematów abelowych który przekształca element neutralny w element neutralny jest homomorfizmem;*

**ii)** *Struktura grupowa na schemacie abelowym jest wyznaczona jednoznacznie przez wybór elementu neutralnego;*

**iii)** *Schemat abelowy jest grupą przemienną;*

*Dowód.* [18, Cor 20.2, str 146] □

**Lemat 1.10.** *Niech $\mathcal{A}$ będzie schematem abelowym o wymiarze $g$ nad $S$ i $n_{\mathcal{A}}$ będzie mnożeniem przez $n$ na $\mathcal{A}$. Wtedy $n_{\mathcal{A}}$ jest płaskie, surjektywne i skończone, a jądro $\mathcal{A}[n]$ jest skończonym płaskim schematem grupowym nad $S$ o rzędzie $n^{2g}$. Co więcej $n_{\mathcal{A}}$(a zatem też jądro) jest étalne nad $S$ wtedy i tylko wtedy, gdy $n$ nie dzieli się przez charakterystykę żadnego z ciał reszt $S$.*

*Dowód.* [18, Prop. 20.7, str 147] □

**Uwaga 1.6.1.** *Niech $S$ będzie całkowitym schematem noetherowskim, a $A$ będzie rozmaitością abelową nad ciałem funkcji wymiernych $K$ schematu $S$. Niech $\mathcal{A}$ będzie domknięciem $A$ w $\mathbb{P}^n_U$, Wtedy istnieje podzbiór otwarty $U \subset S$ taki, że $\mathcal{A}$ rozszerza się na nim do projektywnego schematu abelowego $A_U \subset \mathbb{P}^n_U$.*

**Uwaga 1.6.2.** *Jeżeli $K$ jest skończenie generowanym ciałem nad $\mathbb{Q}$ to istnieje pierścień $R \subset K$, skończenego typu nad $\mathbb{Z}$ taki, że $K = Fr(R)$. Niech $S = \operatorname{Spec} R$. Rozpatrzymy morfizm schematów $S \to \operatorname{Spec} \mathbb{Z}$. Z definicji gładkości* [18, uwaga po definicji 3, str 36] *wynika, że istnieje otwarty podzbiór $U \subset S$ taki, że morfizm $U \to \operatorname{Spec} \mathbb{Z}$ jest gładki.*

Rozważmy diagram

$$\begin{array}{ccc} L & \longleftarrow & R' \\ \uparrow & & \uparrow \\ K & \longleftarrow & R \end{array}$$

gdzie $R'$ będzie całkowitym domknięciem $R$ w skończonym rozszerzeniu $L/K$. Niech $\mathcal{A}' := \mathcal{A} \otimes_S S'$ gdzie $S' = \operatorname{Spec} R'$. Wtedy $\mathcal{A}'$ jest abelowym schematem projektywnym nad $S'$, ponieważ gładkość i właściwość morfizmu schematów zachowuje się ze względu na zmianę bazy (gładkość [6, Cor 4.8 str 102], właściwość [13, Uwaga pod definicją 3 na str 34]).

**Lemat 1.11** (Raynaud)**.** *Niech $S$ będzie noetherowskim całkowitym schematem oraz $G$ i $H$ będą dwoma abelowymi schematami nad $S$. Załóżmy, że nad gęstym otwartym podschematem $U$ schematu $S$ istnieje homomorfizm $\psi_U : H_U \to G_U$. Wtedy $\psi$ rozszerza się (jednoznacznie) do homomorfizmu $\psi : H \to G$ nad $S$.*

*Dowód.* [10, Prop 2.7, str 9] □

**Uwaga 1.6.3.** *Niech $\mathcal{A}/S$, $\mathcal{B}/S$ będą dwoma projektywnymi schematami abelowymi z włóknami generycznymi $A/K$, $B/K$ odpowiednio. Wtedy z 1.11 mamy*

$$\operatorname{Hom}_K(A, B) = \operatorname{Hom}_S(\mathcal{A}, \mathcal{B}), \tag{1.2}$$

*ponieważ* $\mathrm{Hom}_K(A, B)$ *jest skończenie generowaną grupą abelową i każdy homomorfizm* $\varphi \in \mathrm{Hom}_K(A, B)$ *rozszerza się do elementu z* $\mathrm{Hom}_U(\mathcal{A}|_U, \mathcal{B}|_U)$ *to z lematu 1.11 i z twierdzenia Grothendiecka (zobacz* [6, Rozdział 1, podrozdział 1.2, lemat 5]*) mamy*

$$\varinjlim_U \mathrm{Hom}_U(\mathcal{A}|_U, \mathcal{B}|_U) = \mathrm{Hom}_K(A, B).$$

*To daje równość* (1.2)*. W szczególności mamy*

$$\mathrm{End}_K(A) = \mathrm{End}_S(\mathcal{A}).$$

Rozważmy teraz rozmaitość abelową $A$ nad ciałem $K$, która jest włóknem generycznym schematu abelowego $\mathcal{A}/S$. Istnieje izogenia $\varphi : A \to A_1^{e_t} \times \cdots \times A_t^{e_t}$ określona nad pewnym skończonym rozszerzeniem $L/K$, gdzie $A_i$ są prostymi parami nieizogenicznymi rozmaitościami abelowymi określonymi nad $L$. Weźmy całkowite domknięcie $R$ w $L$, które oznaczamy $R'$. Wtedy, dostajemy schemat abelowy $\mathcal{A}' := \mathcal{A} \times_S S'$ nad $S'$, którego włókno generyczne jest równe $A \otimes_K L$. Istnieje $U_L \subset S'$ zbiór otwarty taki, że $\mathcal{A}_i/U_L$ są schematami abelowymi z włóknami generycznymi $A_i/L$ oraz morfizm $\varphi$ rozszerza się do morfizmu schematów abelowych

$$\varphi' : \mathcal{A}'_{U_L} \to \prod_{i=1}^{t} \mathcal{A}_i^{e_i}$$

tak, że $\varphi' \otimes_{U_L} L = \varphi$.

**Uwaga 1.6.4.** *Jeżeli* $A/K$ *jest rozmaitością abelową nad ciałem skończenie generowanym o charakterystyce 0 to z powyższych uwag wynika, że istnieje gładki i normalny schemat* $S = \mathrm{Spec}\, R$*, taki, że* $Fr(R) = K$ *i istnieje schemat abelowy* $\mathcal{A}/S$*, którego generycznym włóknem jest* $A/K$*. W szczególności jeżeli* $\varphi : A \to \prod_{i=1}^{t} A_i^{e_i}$ *jest izogenią rozmaitości abelowych nad* $K$ *to rozszerza się ona do morfizmu schemtów abelowych* $\varphi'$ *jak wyżej dla pewnego afinicznego normalnego* $U_L$*, którego ciałem funkcyjnym jest* $L$ *oraz takiego, że* $U_L \to \mathrm{Spec}\, \mathbb{Z}$ *jest gładkie.*

## 1.7. Reprezentacje $l$-adyczne dla rozmaitości abelowej nad ciałami skończenie generowanymi

**Twierdzenie 1.7** (Mordell-Weil,Lang-Néron)**.** *Niech* $A$ *będzie rozmaitością abelową nad ciałem skończenie generowanym* $K$ *(o dowolnej charakterystyce), wtedy* $A(K)$ *jest skończenie generowaną grupą abelową.*

*Dowód.* Zobacz [15, p. 27.3] $\square$

**Twierdzenie 1.8** (Chebotarev). *Niech $A/K$ będzie rozmaitością abelową nad ciałem charakterystyki zero. Zbiór $\{\mathrm{Fr}_v \ : \ v$ punkt domknięty w $\pi_1(S)\}$ jest gęsty w $\pi_1(S)$.*

*Dowód.* Zobacz [9, str. 206-207]. □

**Twierdzenie 1.9** (Faltings, Zarhin). *Dla dowolnej rozmaitości abelowej i liczby pierwszej $l$ mamy*

1. $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_l \xrightarrow{\sim} \mathrm{End}_{G_K}(T_l(A))$ *jest izomorfizmem;*
2. $V_l(A)$ *jest półprostym* $\mathbb{Q}_l[G_{l^\infty}]$*-modułem.*

*Dowód.* Dla przypadku, gdzie $K$ jest ciałem skończenie generowanym nad $\mathbb{Q}$, dowód znajduje się w [9, twierdzenie 1, str. 204], a w przypadku, gdy $K$ jest ciałem skończenie generowanym nad ciałem charakterystyki dodatniej [38, Wnioski 1 i 2, str. 240]. □

**Twierdzenie 1.10** (Zarhin). *Dla dowolnej rozmaitości abelowej $A/K$, char $K$ względnie pierwsza z $l$, mamy:*

1. $\mathrm{End}_K(A) \otimes \mathbb{Z}/l \xrightarrow{\sim} \mathrm{End}_{G_K}(A[l])$ *jest izomorfizmem, dla każdej liczby pierwszej $l$;*
2. $A[l]$ *jest półprostym* $\mathbb{Z}/l[G_l]$ *modułem, dla $l \gg 0$.*

*Dowód.* [33, Prop. 3.4] □

**Twierdzenie 1.11** (Serre). *Niech $A/K$, char $K = 0$, będzie rozmaitością abelową:*

$$\rho \quad : \quad G_K \to \mathrm{GL}_n(T_l(A))$$

*będzie $l$-adyczną reprezentacją stowarzyszoną z $A$. Wtedy indeks*

$$e_l := \left[\mathbb{Z}^\times \mathrm{Id}_{T_l(A)} \quad : \quad \rho_l(G_K) \cap \mathrm{Id}_{T_l(A)}\right]$$

*jest ograniczony niezależnie od $l$.*

*Dowód.*
Przedstawimy tu dwa dowody, pierwszy należy do J.P. Serre'a.

Dowód będzie przeprowadzony przez indukcję względem $n = \mathrm{tr.deg}\, K$. Jeżeli $n > 0$, wtedy możemy rozważać $K$ jako ciało funkcyjne nad gładką krzywą nad ciałem $K_0$, którego stopień przestępny jest równy $n-1$. Wtedy rozmaitość $A/K$ definiuje abelowy schemat grupowy $\widetilde{\mathcal{A}}$ nad otwartym gęstym podzbiorem $U$ krzywej $C$. Wybierzmy domknięty punkt $P$ z $U$ i niech $v$ będzie waluacją dyskretną ciała $K$ odpowiadającą punktowi $P$. Wiemy, że jego ciało reszt $k_v$ jest skończonym rozszerzeniem ciała $K_0$. Jeżeli $m$ jest większe od zera, to rozszerzenie ciał $K(A[m])/K$ jest nierozgałęzione w $v$. Mamy teraz grupę Galois odpowiadającą temu rozszerzeniu $G\,(K(A[m])/K)$, której grupa dekompozycji $v$ jest izomorficzna z $G\left(k_v(\widetilde{\mathcal{A}})[m]/k_v\right)$, gdzie $\widetilde{\mathcal{A}_v}$ oznacza włókno $\widetilde{A}$ w $v$. Biorąc teraz granicę odwrotną po $m$ dostajemy, że obraz $G\,(\bar{K}/K) \to \prod_l \mathrm{GL}(T_l(A))$ zawiera obraz $G\,(\bar{k_v}/k_v) \to \prod_l \mathrm{GL}\left(T_l(\widetilde{\mathcal{A}_v})\right)$, gdzie $\mathrm{GL}\,(T_l(A)) \cong \mathrm{GL}\left(T_l(\widetilde{\mathcal{A}_v})\right) \cong \mathrm{GL}_{2g}(\mathbb{Z}_l)$. Teraz na mocy indukcji obraz $G\,(\bar{k}_v/k_v) \to \prod_l \mathrm{GL}\left(T_l(\widetilde{\mathcal{A}_v})\right)$ zawiera $e$-tą potęgę homotetii, dla pewnego $e > 0$, stąd $G\,(\bar{K}/K) \to \prod_l \mathrm{GL}\,(T_l(A))$ zawiera również $e$-tą potęgę homotetii.

Dowód 2 (G. Banaszak)
Krok 1.
Istnieje gładki, geometrycznie nierozkładalny schemat $S$ nad $L$ (domkniecie algebraiczne $\mathbb{Q}$ w $K$) z punktem generycznym $\eta = spec\ K$ takim, że $A$ jest włóknem generycznym schematu abelowego $\mathcal{A}$. Co więcej istnieje domknięty punkt $P \in S(L)$ [9, str 212], a więc dostajemy $A = \mathcal{A} \times_S \operatorname{Spec} K$, oznaczmy $\mathcal{A}_P := \mathcal{A} \times_S P$.
Krok 2.
Naturalne odwzorowanie $G_K \to \pi_1(S)$ jest suriekcją, a grupa rozkładu $D_P \subset \pi_1(S)$ jest izomorficzna z $G_L$ . Ponadto $G_K$ działa na $T_l(A)$ poprzez $\pi_1(S)$ [9, str 212].
Krok 3.
Z [31] wiemy, że indeks

$$e_l = \left[\mathbb{Z}^\times \operatorname{Id}_{T_l(\mathcal{A}_P)} : \rho_{L,l}(D_P) \cap \mathbb{Z}^\times \operatorname{Id}_{T_l((A)_P)}\right]$$

jest ograniczony dla zmieniających się $l$, gdzie

$$\rho_{L,l} : G_L \to GL(T_l(\mathcal{A}_P)).$$

Krok 4.
Z twierdzenia [19, Rozdział VI, podrozdział 4 wniosek 4.2] zastosowanego do snopa stałego $\mathbb{Z}/l^k$ na $\mathcal{A}$, dla każdego $k \geqslant 1$ mamy naturalny izomorfizm $T_l(A) \cong T_l(\mathcal{A}_P)$ jako $\mathbb{Z}_l[D_P]$- modułów taki, że $D_P$ działa na $T_l(A)$ jako podgrupa $\pi_1(S)$. Stąd $\widetilde{e_l} \leqslant e_l$. □

**Wniosek 1.6** (Bogomolov)**.** *Niech $A/K$, gdzie char $K = 0$, będzie rozmaitością abelową, a $l$ liczbą pierwszą. Niech $\rho_l : G_K \to \mathrm{GL}\,(T_l(A))$ będzie reprezentacją stowarzyszoną z $A$, wtedy $\rho(G_K) \cap \mathbb{Z}_l^\times \operatorname{Id}_{T_l(A)}$ jest zbiorem otwartym w $\mathbb{Z}_l^\times \operatorname{Id}_{T_l(A)}$.*

*Dowód.* Dowód wynika z twierdzenia (1.11). □

**Uwaga 1.7.1.** *Jeżeli w twierdzeniu 1.11 i wniosku 1.6 nie założymy, że charaktery-*

*styka ciała jest równa zero, to twierdzenia te nie są prawdziwe. Przykłady rozmaitości dla których to twierdzenie jest fałszywe podał Zarhin w artykule* [39].

**Twierdzenie 1.12** (Serre II)**.** *Dla dowolnej rozmaitości abelowej nad $K$ i dowolnej liczby pierwszej $l \neq \operatorname{char} K$:*

1. $H^n\left(G_{l^\infty}\ ;\ V_l(A)\right) = 0$;

2. $H^n\left(G_{l^\infty}\ ;\ T_l(A)\right)$ *jest skończoną grupą abelową.*

*Dowód.* [31, wniosek i uwaga 2 str 734] □

**Twierdzenie 1.13.** *Niech $A$ będzie rozmaitością abelową nad $K$. Wtedy:*

1. $H^n\left(G_{k'}\ ;\ A[l^k]\right) = 0$ *dla* $l \gg 0$ *i* $k' \geqslant k \geqslant 1$;

2. $H^n\left(G_{l^\infty}\ ;\ T_l(A)\right) = 0$ *dla* $l \gg 0$.

*Dowód.* Z twierdzenia (1.11) istnieje stała $e \in \mathbb{N}$ taka, że $e \geqslant e_l$ dla wszystkich $l$. Weźmy teraz $l \gg 0$ tak, żeby zachodziło $l > c + 1$. Ponieważ $\mathbb{Z}_l^\times \cong (\mathbb{Z}/l)^\times \times (1 + l\mathbb{Z}_l)$, więc istnieje $h := c\operatorname{Id}_{T_l(A)} \in (\mathbb{Z}/l)^\times \operatorname{Id}_{T_l(A)} \subset \mathbb{Z}_l^\times \operatorname{Id}_{T_l(A)}$, gdzie $c \not\equiv 1 \mod l$. Niech $\Delta$ będzie podgrupą $G_{l^\infty}$ generowaną przez $c\mathbb{Z}_l^\times \operatorname{Id}_{T_l(A)}$. Zauważmy, że $|\Delta| \;\Big|\; l-1$. Możemy zauważyć, że $\Delta$ odwzorowuje się izomorficznie na swój obraz za pomocą odwzorowania $G_{l^\infty} \to G_{l^k} \quad \forall_{k \geqslant 1}$, ponadto $\Delta \subset Z\left(G_{l^\infty}\right)$ i $\Delta \subset Z\left(G_{l^k}\right)$, dla wszystkich $k \geqslant 1$. Rozważmy teraz ciąg spektralny:

$$E_2^{i,j} = H^i\Big(G_{l^{k'}}/\Delta\ ;\ H^j(\Delta\ ;\ A[l^k])\Big) \Rightarrow H^{i+j}(G_{l^{k'}}\ ;\ A[l^k])$$

Zauważmy, że $H^j\left(\Delta\ ;\ A[l^k]\right) = 0$, dla wszystkich $j \geqslant\!\geqslant 1$, ponieważ $|\Delta|\Big|l-1$. Co więcej z definicji $\Delta$ mamy: $H^0\left(\Delta\ :\ A[l^k]\right) = A[l^k]^\Delta = 0$. Stąd dostajemy, że $H^n\left(\Delta\ :\ A[l^k]\right) = 0$, dla wszystkich $n \geqslant 0$, $l > e + 1$ i dla wszystkich $k' \geqslant k \geqslant 0$. Stąd $H^n\left(G_{l^\infty}\ :\ T_l(A)\right) = \varprojlim_k \varinjlim_{k'} H^n\left(G_{l^{k'}}\ :\ A[l^k]\right) = 0$, dla $l > e + 1$. □

# Rozdział 2

# Twierdzenia o redukcji

## 2.1. Odwzorowanie redukcji

Niech $\mathcal{A}/S$ będzie schematem abelowym $l$ będzie liczbą pierwszą, względnie pierwszą z charakterystyką ciał reszt schematu $S$. Wtedy odwzorowanie mnożenia przez $l^k$ na $\mathcal{A}/S$ jest odwzorowaniem étalnym ([19, Prop. 20.7]), stąd pull back poprzez sekcję elementu neutralnego (unit section $e : S \to A$) jest schematem skończonym, który jest étalny nad $S$. W szczególności jądro odwzorowania $l^k$ jest skończonym schematem nad $S$.

Niech $S = \operatorname{Spec} R$, $K = Fr(R)$ i niech $R$ będzie całkowicie domknięty w $K$. Rozważmy teraz wszystkie skończone rozszerzenia $L/K$, $L \subset \overline{K}_s$ takie, że normalizacja $R'$ pierścienia $R$ w $L$ daje nierozgałęzione rozszerzenie schematów $S'/S$, w każdym punkcie $S$, gdzie $S' = \operatorname{Spec} R'$. Jeżeli $K^{ur}$ oznacza sumę wszystkich takich ciał $L$ zawartych w $\overline{K}_s$, wtedy z [19, Examp 5.2 (b)] $\pi_1(S) := \pi_1(S, \eta) = G(K^{ur}/K)$. W tym przypadku $R^{ur}$ definiujemy jako sumę pierścieni $R'$ w $\overline{K}_s$ i schemat $S^{ur} = \operatorname{Spec} R^{ur}$ będziemy nazywać nakryciem uniwersalnym $S$.

Przypomnijmy, że każda rozmaitość abelowa $A/K$ jest rozmaitością projektywną. Jeżeli $K = K(S)$ jest ciałem funkcyjnym całkowitego noetherowskiego schematu $S$, wtedy możemy wziąć domknięcie Zariskiego rozmaitości $A$ w $\mathbb{P}^n/S$, żeby otrzymać schemat projektywny $\mathcal{A}/S$. Nad pewnym otwartym podzbiorze $U \subset S$ schemat $\mathcal{A}/U$ stanie się projektywnym schematem abelowym ( [18, Rem. 20.9] ).

Dla dowolnego schematu abelowego $\mathcal{A}/S$, możemy zawsze znormalizować schemat $S$ do $S'$ i zmienić bazę przez $S' \to S$ tak, żeby dostać schemat abelowy $\bar{\mathcal{A}} := \mathcal{A} \times_S S'$ nad normalnym schematem bazowym $S'$.

Jeżeli $M$ oznacza dowolną grupę abelową to $Div(M) := Div(M)$ oznacza maksymalną podgrupę podzielną. Przypomnijmy, że $g_s = Gal(\overline{k(s)}/k(s))$.

**Twierdzenie 2.1** (G. Banaszak)**.**
*Niech $\mathcal{A}/S$ będzie schematem abelowym nad całkowitym, normalnym schematem bazowym $S$ i $A/K$ będzie włóknem generycznym. Niech $s \in S$ będzie ustalonym punktem schematu $S$ (nie koniecznie domkniętym), $l$ będzie liczbą pierwszą względnie pierwszą z charakterystyką $K$ i $k(s)$. Załóżmy ponadto, że naturalne przekształcenie $\mathcal{A}(S) \twoheadrightarrow A(K)$ jest suriekcją oraz grupa $H^0\left(g_s, \mathcal{A}[l^\infty]\right)$ jest skończona. Wtedy:*

(1) *$l$-adyczne uzupełnienie na przekształceniu $\mathcal{A}(S) \twoheadrightarrow A(K)$ daje izomorfizm*

$$\varprojlim_k \mathcal{A}(S)/l^k \quad \stackrel{\sim}{\to} \quad \varprojlim A(K)/l^k,$$

(2) *odwzorowanie redukcji*

$$r_s \ : \ \mathcal{A}(S)_l \to \mathcal{A}_s(k(s))_l$$

*jest monomorfizmem.*

*Dowód.* Ponieważ skończony schemat grupowy $\mathcal{A}[l^k]$ jest étalny nad $S$, dla wszystkich $k \geqslant 1$, a więc działanie $G_K$ na $A[l^k]$ faktoryzuje się przez działanie $\pi_1(S) = G\left(K^{ur}/K\right)$ ponieważ $\mathcal{A}[l^k] \cong A[l^k]$ jako $G(K^{ur}/K)$-moduły. Jeżeli $l$ jest względnie pierwsze z charakterystyką $k(s)$, wtedy mamy izomorfizm grup skończonych $\mathcal{A}_s[l^k] \cong \left(\mathbb{Z}/l^k\right)^{2g}$, dla każdego $s$ dla którego $char\ k(s) \neq l$. W szczególności dla każdego $s$, którego $char\ k(s) \neq l$ mamy izomorfizm $g_s$-modułów $\mathcal{A}_s[l^k] \cong A[l^k]$. Wynika to z twierdzenia [19, Chap. VI, sec 4, Cor 4.2] zastosowanego dla snopu stałego $\mathbb{Z}/l^k$ na $\mathcal{A}$, dla $k \geqslant 1$. Z [18, rozdział 2 podrozdział 1] i z tego, że grupowy abelowy schemat może być traktowany jako étalny snop dostajemy, że $\mathcal{A}(S^{ur})^{\pi_1(S)} = \mathcal{A}(S)$. Biorąc długi ciąg dokładny kohomologii dla grupy $\pi_1(S)$ zastosowanego do krótkiego ciągu dokładnego:

$$0 \to \mathcal{A}[l^k] \to \mathcal{A}(S^{ur}) \xrightarrow{l^k} \mathcal{A}(S^{ur}) \to 0$$

uzyskujemy monomorfizm $\mathcal{A}(S)/l^k \hookrightarrow H^1(\pi_1(S); \mathcal{A}[l^k])$. W podobny sposób pokazujemy, że $A(K)/l^k \hookrightarrow H^1(G_K; A[l^k])$ i $\mathcal{A}_s(k(s))/l^k \hookrightarrow H^1(g_s; T_l(\mathcal{A}))$ są monomorfizmami. Dla każdego $s \in S$ mamy $Div = 0$ w $H^0\left(g_s, \mathcal{A}_s[l^\infty]\right)$ z założenia skończoności. Stąd dolna, prawa, pozioma strzałka w diagramie przemiennym:

$$\begin{tikzcd}
A(K)_l \arrow[d] & \mathcal{A}(S)_l \arrow[l, "r_\eta"'] \arrow[r, "r_s"] \arrow[d] & \mathcal{A}_s(k(s))_l \arrow[d] \\
\varprojlim_k A(K)/l^k \arrow[d] & \varprojlim_k \mathcal{A}(S)/l^k \arrow[l, "r_\eta"'] \arrow[r, "r_s"] \arrow[d] & \varprojlim_k \mathcal{A}_s(k(s))/l^k \arrow[d] \\
H^1(G_K,\, T_l(A))_l \arrow[d, "="] & H^1(\pi_1(S),\, T_l(\mathcal{A}))_l \arrow[l, "r_\eta"'] \arrow[r, "r_s"] \arrow[d, "="] & H^1(g_s,\, T_l(\mathcal{A}_s))_l \arrow[d, "="] \\
H^0(G_K,\, A[l^\infty])/Div \arrow[r, equal] & H^0(\pi_1(S),\, \mathcal{A}[l^\infty])/Div \arrow[r, "r_s"] & H^0(g_s,\, \mathcal{A}_s[l^\infty])/Div
\end{tikzcd}$$

jest monomorfizmem, a środkowe pionowe strzałki są monomorfizmami z zastosowania długich ciągów dokładnych w kohomologii. Z twierdzenia [35, Prop 2.3 p. 261] dolne pionowe strzałki są równościami. Górne pionowe strzałki są monomorfizmami bo skończoność grupy $H^0(g_s, \mathcal{A}_s[l^\infty])$ pociąga skończoność grup $H^0(\pi_1(S), \mathcal{A}[l^\infty])$, $H^0(G_K, A[l^\infty])$. Stąd prawa górna pozioma strzałka jest monomorfizmem i druga od góry lewa pozioma strzałka jest monomorfizmem i z założenia epimorfizmem a zatem jest izomorfizmem. □

**Wniosek 2.1.** *Niech $\mathcal{A}/S$ będzie schematem abelowym nad całkowitym, normalnym afinicznym schematem $S = \operatorname{Spec} R$, gdzie $R$ jest skończenie generowaną $\mathbb{Z}$-algebrą lub $\mathbb{F}_p$-algebrą. Niech $A/K$ będzie włóknem generycznym. Niech $v \in S$ będzie punktem domkniętym i niech $k_v := k(v)$. Załóżmy ponadto, że naturalne przekształcenie $\mathcal{A}(S) \twoheadrightarrow A(K)$ jest suriekcją. Niech $l$ będzie liczbą pierwszą względnie pierwszą z charakterystyką ciała reszt punktu $v$ i punktu generycznego $\eta \in S$. Wtedy:*

(1) *$l$-adyczne uzupełnienie na przekształceniu $\mathcal{A}(S) \twoheadrightarrow A(K)$ daje izomorfizm*

$$\varprojlim_k \mathcal{A}(S)/l^k \quad \xrightarrow{\sim} \quad A(K) \otimes \mathbb{Z}_l$$

(2) *odwzorowanie redukcji*

$$r_s \;:\; A(K)_l \to \mathcal{A}_s(k(s))_l$$

*jest monomorfizmem.*

*Dowód.* Z twierdzenia [18, Rozdział VI, podrozdział 4, wniosek 4.2] zastosowanego do snopa stałego $\mathbb{Z}/l^k$ na $\mathcal{A}$ dostajemy, że dla każdego $k \geqslant 1$ mamy naturalny izomorfizm $g_v := G(\overline{k}_v/k_v)$-modułów $H^1(A, \mathbb{Z}/l^k) \cong H^1(\mathcal{A}_v, \mathbb{Z}/l^k)$, dla każdego $k$. Biorąc granicę odwrotną po $k$ dostajemy izomorfizm $\mathbb{Z}_l$ i $g_v$-modułów $T_l(A) \cong T_l(\mathcal{A}_v)$. Tensorując z $\mathbb{Q}_l/\mathbb{Z}_l$ dostajemy izomorfizm $g_v$-modułów $A[l^\infty] \cong \mathcal{A}_v[l^\infty]$. Grupa $g_v$

działa na tych modułach poprzez $G(k_v(\mathcal{A}_v[l^\infty])/k_v)$. Ponieważ $k_v$ jest ciałem skończonym, wiemy z hipotezy Weila, udowodnionej przez Deligne'a, że $H^0(g_v, \mathcal{A}_v[l^\infty])$ jest skończona. Stąd $H^0(G_K, A[l^\infty])$ i $H^0(\pi_1(S), \mathcal{A}[l^\infty])$ również są skończone. Ponieważ $A(K)$ jest skończenie generowana (twierdzenie 1.7) to wtedy $\varprojlim_k A(K)/l^k \cong A(K) \otimes \mathbb{Z}_l$ i lewa dolna pozioma strzałka z dowodu twierdzenia 2.1 pokazuje, że $A(K)_l = \mathcal{A}(S)_l$. Dlatego wniosek wynika z twierdzenia 2.1. $\square$

Z założenia wniosku 2.1 wynika, że $k_v$ jest ciałem skończonym, a zatem $\mathcal{A}_v(k_v)$ jest grupą skończoną. Stąd $\varprojlim \mathcal{A}_v(k_v)/l^k \cong \mathcal{A}_v(k_v)_l$ i drugie od góry poziome strzałki w diagramie z dowodu twierdzenia 2.1 prowadzą do naturalnego przekształcenia redukcji:

$$r_v : A(K) \otimes \mathbb{Z}_l \to \mathcal{A}_v(k_v)_l. \tag{2.1}$$

Ponieważ mamy naturalny homomorfizm $A(K) \to A(K) \otimes \mathbb{Z}_l$ to dostajemy przekształcenie redukcji:

$$r_v : A(K) \to \mathcal{A}_v(k_v)_l \tag{2.2}$$

Zauważmy, że jądro przekształcenia $A(K) \to A(K) \otimes \mathbb{Z}_l$ jest grupa skończona $A(K)_{tor}/A(K)_l$ o rzędzie względnie pierwszym z $l$.

Od tej pory w każdej sytuacji kiedy pracujemy z odwzorowaniami redukcji 2.1 lub 2.2 w domyśle zawsze mamy schemat abelowy $\mathcal{A}$ nad $S$ taki, że $\mathcal{A}$ spełnia założenia wniosku 2.1 ponadto $S \to \operatorname{Spec} \mathbb{Z}$ jest gładkim morfizmem, $S$ jest normalnym schematem, którego ciało funkcyjne jest równe $K$. W sformułowaniach twierdzeń w tej pracy $r_v$ będzie rozumiane jak zwykle jako następujące przekształcenie redukcji:

$$r_v : \mathcal{A}(S) \to \mathcal{A}_v(k_v).$$

Tensorując to przekształcenie redukcji przez $\mathbb{Z}_l$ dostajemy następujące odwzorowanie redukcji które będzie używane w dowodach tych twierdzeń i ich wniosków:

$$r_v : A(K) \otimes \mathbb{Z}_l \to A_v(k_v)_l.$$

Niech $A_i$ dla $i = 1, \ldots, t$, będą rozmaitościami abelowymi nad $K$ takimi, że $\operatorname{Hom}_{\overline{K}}(A_i, A_j) = 0$ dla wszystkich $j \neq i$. Niech $P_{i1}, \ldots, P_{ir_i} \in A_i(K)$ będą liniowo niezależnymi punktami nad pierścieniem $\mathcal{R}_i = \operatorname{End}_K(A_i)$, dla wszystkich $1 \leqslant i \leqslant t$.

Kolejne dwa lematy są oparte na metodach rozwiniętych w pracach [2] i [4], dlatego przypomnijmy oznaczenia: $K_{l^\infty} := K(A[l^\infty])$, $G_{l^\infty} := Gal(K_{l^\infty}/K)$, $H_{l^\infty} := Gal(\bar{K}/K_{l^\infty})$, $H_{l^k} := Gal(\bar{K}/K_{l^k})$, dla wszystkich $k \geqslant 1$. Teraz zdefiniujmy dla wszystkich $1 \leqslant i \leqslant t$ i $1 \leqslant j \leqslant r_j$ odwzorowanie:

$$\phi_{ij} \ : \ H_{l^\infty} \to T_l(A_i),$$

oznaczający granicę odwrotną odwzorowań Kummerowskich po $k$:

$$\phi_{ij}^{(k)} \ : \ H_{l^k} \to A_i[l^k],$$
$$\phi_{ij}^{(k)}(\sigma) := \sigma\left(\frac{1}{l^k}P_{ij}\right) - \frac{1}{l^k}P_{ij}$$

**Lemat 2.1.** *Jeżeli* $\alpha_{11}, \dots, \alpha_{1r_1} \in \mathcal{R}_1 \otimes_{\mathbb{Z}} \mathbb{Z}_l, \ \dots, \ \alpha_{t1}, \dots, \alpha_{tr_t} \in \mathcal{R}_t \otimes_{\mathbb{Z}} \mathbb{Z}_l$ *spełniają równanie* $\sum_{i=1}^{t} \sum_{j=1}^{r_t} \alpha_{ij}\phi_{ij} = 0$, *wtedy* $\alpha_{ij} = 0$ *w* $\mathcal{R}_i$, *dla wszystkich* $1 \leqslant i \leqslant t$, $1 \leqslant j \leqslant r_i$.

*Dowód.* Niech $\Psi$ będzie złożeniem odwzorowań:

$$A(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l \hookrightarrow H^1(G_K; T_l(A)) \longrightarrow H^1\left(H_{l^\infty}; T_l(A)\right) \ = \ Hom\left(H_{l^\infty}; T_l(A)\right).$$

Zauważmy, że $\Psi(P_{ij} \otimes 1) = \phi_{ij}$. Z twierdzenia 1.12 grupa $H^1(G_{l^\infty}; T_l(A))$ jest grupą skończoną, a więc $\ker \Psi \subset (A(K) \otimes \mathbb{Z}_l)_{tor}$. Niech $c := |A(K)_{tor}|$, ponieważ $\Psi$ jest $\mathcal{R} \otimes_{\mathbb{Z}} \mathbb{Z}_l$-homomorfizmem, mamy:

$$0 = \sum_{i=1}^{t} \sum_{j=1}^{r_t} \alpha_{ij}\phi_{ij} = \Psi\left(\sum_{i=1}^{t} \sum_{j=1}^{r_t} \alpha_{ij}(\phi_{ij} \otimes 1)\right).$$

Stąd $\sum_{i=1}^{t} \sum_{j=1}^{r_t} \alpha_{ij}(\phi_{ij} \otimes 1) \in (A(K \otimes_{\mathbb{Z}} \mathbb{Z}_l)_{tor}$. A więc

$$c\sum_{i=1}^{t} \sum_{j=1}^{r_t} \alpha_{ij}(\phi_{ij} \otimes 1) = 0$$

w $A(K) \otimes \mathbb{Z}_l$. Ponieważ $P_{i1} \otimes 1, \dots, P_{ir_i} \otimes 1$ są liniowo niezależne nad $\mathcal{R}_i \otimes Z_l$ w $A_i(K) \otimes \mathbb{Z}_l$ dostajemy $c\alpha_{ij} = 0$ a zatem:

$$\alpha_{i1} = \dots = \alpha_{ir_i} = 0,$$

dla wszystkich $1 \leqslant i \leqslant t$ ponieważ $\mathcal{R}_i$ jest wolnym $\mathbb{Z}$-modułem. □

Zdefiniujmy teraz następne odwzorowanie:

$$\Phi_i^k \ : \ H_{l^k} \to A_i[l^k]^{r_i}$$

$$\Phi_i^k(\sigma) := \left(\phi_{i1}^{(k)}(\sigma), \dots, \phi_{ir_i}^{(k)}(\sigma)\right)$$

i teraz z tego odwzorowania stwórzmy kolejne:

$$\Phi^k \ : \ \bigoplus_{i=1}^{t} A_i[l^k]^{r_i}$$

$$\Phi^k := \bigoplus_{i=1}^{t} \Phi_i^k.$$

oraz odwzorowanie w moduł Tate'a:

$$\Phi_i \ : \ H_{l^\infty} \to T_l(A_i)^{r_i}$$

$$\Phi_i(\sigma) := (\phi_{i1}(\sigma), \ldots, \phi_{ir_i}(\sigma)),$$

$$\Phi \ : \ H_{l^\infty} \to \bigoplus_{i=1}^{t} T_l(A_i)^{r_i}$$

$$\Phi := \bigoplus_{i=1}^{t} \Phi_i.$$

**Lemat 2.2.** *Obraz odwzorowania $\Phi$ jest zbiorem otwartym w $\bigoplus_{i=1}^t T_l(A_i)^{r_i}$.*

*Dowód.* Przyjmijmy oznaczenia $T := \bigoplus_{i=1}^t T_l(A_i)^{r_i}$, $W := T \otimes_{\mathbb{Z}_l} \mathbb{Q}_l = \bigoplus_{i=1}^t V_{il}^{r_i}$, gdzie $V_{il} := T_l(A_i) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$. Przez $\Phi \otimes 1$ oznaczmy złożenie $\Phi$ z zanurzeniem $T \hookrightarrow W$ oraz $M := \mathrm{Im}(\Phi \otimes 1) \subset W$. Wiemy, że $M$, $W$ są $\mathbb{Q}_l[G_{l^\infty}]$-modułami. Wystarczy pokazać, że $\mathrm{Im}\Phi$ jest skończonego indeksu w $T$. Dlatego wystarczy pokazać, że $\Phi \otimes 1$ jest "na". Zauważmy, że $V_{il}$ jest półprostym $\mathbb{Q}_l[G_{l^\infty}]$-modułem, dla każdego $1 \leqslant i \leqslant t$ bo na mocy twierdzenia 1.9

$$V_l = \bigoplus_{i=1}^{t} V_{il}$$

i $V_l$ jest półprostym $\mathbb{Q}_l[G_{l^\infty}]$-modułem. Zauważmy, że $G_{l^\infty}$ działa na $V_{il}$ poprzez $Gal\,(K(A_i[l^\infty])/K)$. Jeżeli $\Phi \otimes 1$ nie byłoby odwzorowaniem "na" to istniałby rozkład $W$ na $\mathbb{Q}_l[G_{l^\infty}]$-moduły $M \oplus M_1$, gdzie $M_1$ jest nietrywialnym modułem.

Niech $\pi_{M_1} : W \to W$ będzie projekcją na $M_1$, a $\pi_i : W \to V_{il}$ będzie projekcją, która odwzorowuje $M_1$ nietrywialnie. Oznaczmy $\widetilde{\pi} := \pi \circ \pi_{M_1}$.

Mamy $\mathrm{Hom}_{G_{l^\infty}}(V_{il}; V_{i'l}) \cong \mathrm{Hom}_K(A_i; A_{i'}) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l = 0$, dla wszystkich $i \neq i'$. Stąd dostajemy:

$$\widetilde{\pi}(v_{ij}) = \sum_{j=1}^{r_i} \beta_{ij} v_{ij},$$

dla pewnych $\beta ij \in \mathcal{R}_i \otimes \mathbb{Q}_l$. Ponieważ $\pi$ jest nietrywialne na $M_1$ więc musi istnieć przynajmniej jedno niezerowe $\beta_{ij}$. Jednak z drugiej strony:

$$\widetilde{\pi}_i\left(\Phi(h)\otimes 1\right)=\sum_{j=1}^{r_i}\beta_{ij}\left(\phi_{ij}(h)\otimes 1\right)=0,$$

dla wszystkich $h\in H_{l^\infty}$. Ponieważ $\beta_{ij}\in\mathcal{R}_i\otimes\mathbb{Q}_l$ możemy przemnożyć ostatnią równość przez odpowiednią potęgę $l$ i dostać:

$$0=\sum_{j=1}^{r_i}\alpha_{ij}\left(\phi_{ij}(h)\otimes 1\right),$$

dla pewnych $\alpha_{ij}\in\mathcal{R}_i\otimes\mathbb{Z}_l$. Ponieważ następujące odwzorowania $\mathcal{R}_i\otimes\mathbb{Z}_l\hookrightarrow\mathcal{R}_i\otimes\mathbb{Q}_l$, $\mathrm{Hom}(H_{l^\infty},T_l)\hookrightarrow\mathrm{Hom}(H_{l^\infty},V_l)$ są zanurzeniami(imbeddings) $\mathcal{R}\otimes\mathbb{Z}_l$-modułów, dostajemy $\sum_{i=1}^{r_i}\alpha_{ij}\phi_{ij}=0$. Teraz z lematu 2.1 dostajemy, że $\alpha_{i1}=\cdots=\alpha_{ir_i}=0$ i stąd $\beta_{i1}=\cdots=\beta_{ir_i}=0$ ponieważ $\mathcal{R}$ jest beztorsyjny. Jednakże to jest sprzeczne z założeniem, że $M_1\neq 0$ czyli $M_1=0$. □

**Twierdzenie 2.2.** *Niech $A=\prod_{i=1}^{t}A_i$ będzie rozmaitością abelową nad ciałem skończenie generowanym $K$, gdzie $\mathrm{Hom}_{\overline{K}}(A_i,A_j)=0$ dla wszystkich $i\neq j$. Niech $Q_{ij}\in A_i(K)$, dla $1\leqslant j\leqslant r_i$ będą liniowo niezależnymi punktami nad $\mathcal{R}_i$, dla wszystkich $1\leqslant i\leqslant t$. Wtedy dla każdego podzbióru otwartego $U\subset S$, istnieje nieskończnie wiele punktów domkniętych $v\in U$ takich, że $r_v(Q_{ij})=0$ dla wszystkich $1\leqslant j\leqslant r_i$ i $1\leqslant i\leqslant t$.*

*Dowód.* Krok 1

Z lematu 2.2 istnieje stała $m\in\mathbb{N}$ taka, że

$$l^m\bigoplus_{i=1}^{t}T_l(A_i)^{ri}\subset\Phi(H_{l^\infty})\subset\bigoplus_{i=1}^{t}T_l(A_i)^{r_i}.$$

Niech $\Gamma$ będzie $\mathcal{R}$-podmodułem $A(K)$ generowanym przez wszystkie punkty $Q_{ij}$, to znaczy

$$\Gamma:=\{P\in A(K)\ :\ P=\sum_{i=1}^{t}\sum_{j=1}^{r_i}\alpha_{ij}Q_{ij}\ ,\alpha_{ij}\in\mathcal{R}_i\}.$$

Teraz dla $k\geqslant m$ rozważmy następujący diagram przemienny:

$$
\begin{tikzcd}
G(K_{l^\infty}(\frac{1}{l^\infty}\Gamma)/K_{l^\infty}) \arrow[r, "\overline{\Phi}"] \arrow[d] & \bigoplus_{i=1}^{t} T_l(A_i)^{r_i}/l^m \bigoplus_{i=1}^{t} T_l(A_i)^{r_i} \arrow[d] \\
G\left(K_{l^{k+1}}(\frac{1}{l^{k+1}}\Gamma)/K_{l^{k+1}}\right) \arrow[r, "\overline{\Phi^{k+1}}"] \arrow[d] & \bigoplus_{i=1}^{t} \left(A_i[l^{k+1}]\right)^{r_i}/l^m \bigoplus_{i=1}^{t} \left(A_i[l^{k+1}]\right)^{r_i} \arrow[d, "="] \\
G\left(K_{l^k}(\frac{1}{l^k}\Gamma)/K_{l^k}\right) \arrow[r, "\overline{\Phi^k}"] & \bigoplus_{i=1}^{t} \left(A_i[l^k]\right)^{r_i}/l^m \bigoplus_{i=1}^{t} \left(A_i[l^k]\right)^{r_i}
\end{tikzcd}
$$

Odwzorowania $\overline{\Phi}$ i $\overline{\Phi^k}$, dla $k \geqslant 1$ są indukowane przez odwzorowanie Kummer'a. Dla $k \gg 0$ obrazy odwzorowań $\overline{\Phi^k}$ i $\overline{\Phi^{k+1}}$ są izomorficzne, a więc dolna lewa pionowa strzałka w diagramie jest odwzorowaniem ″na″, ponieważ odwzorowanie $\overline{\Phi^k}$ jest iniektywne dla $k \geqslant 1$. Rozważmy wieżę ciał:

$$
\begin{tikzcd}[column sep=small]
 & K_{l^{k+1}}\left(\frac{1}{l^{k+1}}\Gamma\right) \arrow[d, dash] & \\
 & K_{l^{k+1}}\left(\frac{1}{l^k}\Gamma\right) \arrow[dl, dash] \arrow[dr, dash] & \\
K_{l^k}\left(\frac{1}{l^k}\Gamma\right) \arrow[dr, dash] & & K_{l^{k+1}} \arrow[dl, dash] \\
 & K_{l^k} \arrow[d, dash] & \\
 & K &
\end{tikzcd}
$$

Wtedy z powyższego argumentu dostajemy:

$$K_{l^k}(\frac{1}{l^k}\Gamma) \ \cap \ K_{l^{k+1}} \quad = \quad K_{l^k} \quad \text{for} \quad k \gg 0 \tag{2.3}$$

Krok 2 Niech $U_0 := \operatorname{Spec} R_0 \subset S$ będzie afinicznym zbiorem otwartym , gdzie $R_0$ jest lokalizacją $R$. Niech $R_1$ (odpowiednio $R_2$) będzie całkowitym domknięciem $R_0$ w $K_{l^{k+1}(\frac{1}{l^k}\Gamma)}$ (odpowiednio w $K_{l^k(\frac{1}{l^k}\Gamma)}$). Niech $U_1 := \operatorname{Spec} R_1$ i $U_2 := \operatorname{Spec} R_2$.

Zauważmy, że $U_0$ możemy wybrać w taki sposób, że $\mathcal{A}(U_1) \twoheadrightarrow A(K_{l^{k+1}(\frac{1}{l^k}\Gamma)})$ oraz $\mathcal{A}(U_2) \twoheadrightarrow A(K_{l^k(\frac{1}{l^k}\Gamma)})$. Zauważmy, że $\mathcal{A}(U_0) \twoheadrightarrow A(K)$.

Niech $h \in G\left(K_{l^\infty}/K_{l^k}\right)$ będzie automorfizmem działającym na $T_l A$ jako homotetia $1 + l^k u$, dla pewnego $u \in \mathbb{Z}_l^\times$. Taka homotetia istnieje, dla $k \gg 0$ z twierdzenia Bogomolov'a 1.6. Niech $h'$ oznacza projekcję $h$ do $G\left(K_{l^{k+1}}/K_{l^k}\right)$. Z równości (2.3) możemy wybrać $\sigma \in G\left(K_{l^{k+1}}\left(\frac{1}{l^k}\Gamma\right)/K\right)$ taką, że $\sigma|_{K_{l^k}(\frac{1}{l^k}\Gamma)} = \mathrm{id}$ i $\sigma|_{K_{l^{k+1}}} = h'$. Z twierdzenia Chebotarev'a 1.8 istnieje nieskończona rodzina punktów domkniętych $v$ w $U_0$ takich, że dla każdego $v \in U_0$ istnieje $\omega_1$ w $U_1$ nad $v$, dla którego Frobenius w $K_{l^{k+1}}\left(\frac{1}{l^k}\Gamma\right)/K$ jest równy $\sigma$.

Niech $l^{c_{ij}}$ będzie rzędem elementu $r_v(Q_{ij})$ w grupie $\mathcal{A}_{iv}(k_v)_l$, dla pewnej stałej $c_{ij} \geqslant 0$, a $\omega_2$ będzie punktem domkniętym w $U_2$ leżącym pod $\omega_1$. Rozważmy teraz następujący diagram:

$$\begin{array}{ccc}
A_i(K) & \xrightarrow{r_v} & \mathcal{A}_{i\,v}(k_v)_l \\
\downarrow & & \downarrow{=} \\
A_i\left(K_{l^k}(\frac{1}{l^k}\Gamma)\right) & \xrightarrow{r_{w_2}} & \mathcal{A}_{i,\,v}(k_{w_2})_l \\
\downarrow & & \downarrow \\
A_i\left(K_{l^{k+1}}(\frac{1}{l^k}\Gamma)\right) & \xrightarrow{r_{w_1}} & \mathcal{A}_{i\,v}(k_{w_1})_l
\end{array} \tag{2.4}$$

Zauważmy, że wszystkie pionowe strzałki są iniektywne. Niech

$$R_{ij} := \frac{1}{l^k} Q_{ij} \in A\left(K_{l^k}\left(\frac{1}{l^k}\Gamma\right)\right) \subset A\left(K_{l^{k+1}}\left(\frac{1}{l^k}\Gamma\right)\right).$$

Element $r_{\omega_1}(R_{ij})$ ma rząd $l^{k+c_{ij}}$ w grupie $\mathcal{A}_{i\omega_1}(k_{\omega_1})_l$, ponieważ $l^{k+c_{ij}} r_{\omega_1}(R_{ij}) = l^{c_{ij}} r_\omega(Q_{ij}) = 0$. Z wyboru $v$, dostajemy $k_v = k_{\omega_2}$, stąd element $r_{\omega_1}(R_{ij})$ pochodzi od elementu z $\mathcal{A}_{iv}(k_v)_l$. Jeżeli $c_{ij} \geqslant 1$, wtedy:

$$h'\left(l^{c_{ij}-1} r_{\omega_1}(R_{ij})\right) = (1 + l^k u) l^{c_{ij}-1} r_{\omega_1}(R_{ij}),$$

ponieważ $l^{c_{ij}-1} r_{\omega_1}(R_{ij}) \in \mathcal{A}_{i\omega_1}(k_v)[l^{k+1}]$.

Z drugiej strony, z wyboru $v$, Frobenius w $\omega_1$ działa na $l^{c_{ij}-1} r_{\omega_1}(R_{ij})$ poprzez $h$, a więc $h\left(l^{c_{ij}-1} r_{\omega_1}(R_i j)\right) = l^{c_{ij}-1} r_{\omega_1}(R_{ij})$, ponieważ $r_{\omega_1}(R_{ij}) \in \mathcal{A}_{iv}(k_v)_l$. Stąd $l^{c_{ij}-1} u r_{\omega_1}(Q_{ij}) = 0$, ale to jest sprzeczne z tym, że rząd $r_{\omega_1}(Q_{ij})$ jest równy $l^{c_{ij}}$, zatem dostajemy $c_{ij} = 0$. □

**Wniosek 2.2.** *Niech $A = \prod_{i=1}^t A_i$ będzie rozmaitością abelową nad ciałem skończenie generowany $K$, gdzie $\mathrm{Hom}_{\overline{K}}(A_i, A_j) = 0$ dla wszystkich $i \neq j$ oraz niech $l$ będzie liczbą pierwszą. Niech $m \in \mathbb{N} \cup \{0\}$. Niech $P_{ij} \in A_i(K)$ będzie rodziną punktów li-*

*niowo niezależnych nad* $R_i$, $T_{ij} \in A_i[l^m]$ *będzie dowolnym elementem torsyjnym dla wszystkich* $1 \leqslant j \leqslant r_i$, $1 \leqslant i \leqslant t$. *Oznaczmy przez* $R'$ *całkowite domknięcie* $R$ *w* $K(A[l^m])$. *Niech* $\omega'$ *oznacza punkt domknięty w* $U'$ *nad* $v$, *gdzie* $U' := \gamma^{-1}(U)$ *i* $\gamma$ *jest naturalnym odwzorowaniem* $\gamma : \operatorname{Spec} R' \to \operatorname{Spec} R$. *Wtedy istnieje nieskończona rodzina punktów domkniętych* $v \in U$, *dla których zachodzi:*

$$r_{\omega'}(T_{ij}) = r_v(P_{ij}) \ \ w \ A_{iv}(k_v)_l,$$

*dla wszystkich* $1 \leqslant j \leqslant r_i$, $1 \leqslant i \leqslant t$, *gdzie* $r_{\omega'} \ : \ A_i\left(K(A_i[l^m])\right) \to A_{i\omega'}(k_{\omega'})_l$ *jest odwzorowaniem redukcji.*

# Rozdział 3

# Liniowa zależność punktów

## 3.1. Liniowa zależność

**Lemat 3.1.** *Niech $A$ będzie rozmaitością abelową nad $K$ taką, że $A = A_1 \times \ldots \times A_t$ i $Q_1, \ldots, Q_r \in A(K)$. Zapiszmy $Q_i = \left[Q_i^j\right]_{1 \leqslant j \leqslant t}$. Jeżeli $Q_1, \ldots, Q_r \in A(K)$ są liniowo niezależne nad $\mathrm{End}_K(A)$, wtedy $Q_1^j, \ldots, Q_r^j$ są liniowo niezależne nad $\mathrm{End}_K A_j$, dla wszystkich $1 \leqslant j \leqslant t$.*

*Dowód.*
Załóżmy, że istnieje $j$ takie, że $\sum_{i=1}^r \alpha_i^j Q_i^j = 0$ i $\alpha_i^j \neq 0$ dla pewnego $i$. Wtedy:

$$\sum_{i=1}^{r} \begin{bmatrix} 0 & \cdots & & 0 \\ \vdots & \ddots & & \vdots \\ \vdots & \alpha_i^j & & \vdots \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & & 0 \end{bmatrix} \begin{bmatrix} Q_i^1 \\ \vdots \\ Q_i^j \\ \vdots \\ Q_i^t \end{bmatrix} = \sum_{i=1}^{r} \begin{bmatrix} 0 \\ \vdots \\ \alpha_i^j Q_i^j \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

ale to przeczy założeniu, że $Q_i$ są liniowo niezależne nad $\mathrm{End}_K(A)$. $\square$

**Lemat 3.2.** *Niech $A$ będzie rozmaitością abelową nad $K$ taką, że $A = A_1 \times \ldots \times A_t$ i $\mathrm{Hom}(A_i, A_j) = \{0\}$, dla wszystkich $j \neq i$. Niech $Q_1 \ldots, Q_r \in A(K)$. Wtedy następujące warunki są równoważne:*

1. *$Q_1, \ldots, Q_r \in A(K)$ są liniowo niezależne nad $\mathrm{End}_K(A)$;*
2. *jeżeli $Q_i = \left[Q_i^j\right]_{1 \leqslant j \leqslant t}$, wtedy:*

$$\forall_{1 \leqslant j \leqslant t} Q_1^j, \ldots, Q_r^j \textit{ są liniowo niezależne nad } \mathrm{End}_K(A_j).$$

*Dowód.*
(1)$\Rightarrow$(2) Udowodnione w lemacie (3.1)

(2)$\Rightarrow$(1)
Załóżmy, że istnieje $\alpha_i \neq 0$, dla pewnego $i$ oraz $\sum_{i=1}^{r} \alpha_i Q_i = 0$. Wtedy z założenia, że $\mathrm{Hom}(A_i, A_j) = \{0\}$, dla wszystkich $j \neq i$, mamy $\mathrm{End}(A) = \prod_{i=1}^{t} \mathrm{End}(A_i)$. Zatem możemy zapisać równanie macierzowe:

$$\sum_{i=1}^{r} \begin{bmatrix} \alpha_i^1 & & \cdots & & 0 \\ \vdots & \ddots & & & \vdots \\ \vdots & & \alpha_i^j & & \vdots \\ \vdots & & & \ddots & \vdots \\ 0 & & \cdots & & \alpha_i^t \end{bmatrix} \begin{bmatrix} Q_i^1 \\ \vdots \\ Q_i^j \\ \vdots \\ Q_i^t \end{bmatrix} = \begin{bmatrix} \sum_{i=1}^{r} \alpha_i^1 Q_i^1 \\ \vdots \\ \sum_{i=1}^{r} \alpha_i^j Q_i^j \\ \vdots \\ \sum_{i=1}^{r} \alpha_i^t Q_i^t \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Stąd, dla pewnego $1 \leqslant j \leqslant t$ istnieje $\alpha_i^j \neq 0$ takie, że $\sum_{i=1}^{r} \alpha_i^j Q_i^j = 0$, co jest sprzeczne z (2). Zatem $Q_1, \ldots, Q_r$ są liniowo niezależne nad $\mathrm{End}_K(A)$. $\square$

Od tej pory do końca pracy zakładamy, że $R \subset K$, $Fr(R) = K$, schemat $S = \mathrm{Spec}\, R$ jest normalnym schematem i $\mathrm{Spec}\, S \to \mathrm{Spec}\, \mathbb{Z}$ jest gładkim morfizmem.

**Lemat 3.3.** *Niech $A$ będzie prostą rozmaitością abelową nad $K$, $P, P_1, \ldots, P_r \in A(K)$ będą beztorsyjnymi punktami z $A(K)$. Niech $P_1, \ldots, P_r$ będą punktami liniowo niezależnymi nad $R := \mathrm{End}_K(A)$ i niech $\Lambda$ będzie $\mathbb{Z}$-podmodułem generowanym przez $P_1, \ldots, P_r$. Niech $U$ będzie dowolnym otwartym niepustym zbiorem w $S$. Jeżeli*

$$r_v(P) \in r_v(\Lambda), \tag{3.1}$$

*dla każdego domkniętego punktu $v \in U$, wtedy $aP \in \sum_{i=1}^{r} \mathcal{R} P_i$, dla pewnej liczby $a \in \mathbb{Z} \setminus \{0\}$.*

*Dowód.*
Na początku pokażę, że punkty $P, P_1, \ldots, P_r$ nie mogą być liniowo niezależne nad $\mathcal{R}$. Załóżmy, że te punkty są jednak liniowo niezależne nad $\mathcal{R}$. Wtedy dla pewnej liczby pierwszej $l$, z twierdzenia 2.2 istnieje element $v \in U$ taki, że $r_v(P)$ ma duży rząd i $r_v(P_i) = 0$ w $A_v(k_v)_l$, dla wszystkich $0 \leqslant i \leqslant r$. Ale to przeczy założeniu (3.1).

Stąd wiemy, że te punkty są liniowo zależne nad $\mathcal{R}$, czyli istnieją elementy $\alpha, \alpha_1, \ldots, \alpha_r \in \mathcal{R}$ i $\alpha \neq 0$ takie, że

$$\alpha P = \alpha_1 P_1 + \cdots \alpha_r P_r$$

Ponieważ $A$ jest rozmaitością prostą, więc istnieje izogenia dualna $\widehat{\alpha}$ taka, że

$\widehat{\alpha}\alpha = a$, dla pewnego $a \in \mathbb{N}$. Wtedy mamy:

$$\widehat{\alpha}\alpha P = \sum_{i=1}^{r} \widehat{\alpha}\alpha_i P_i$$

Stąd $aP \in \sum_{i=1}^{r} \mathcal{R} P_i$. □

**Lemat 3.4.** *Niech $A = A_1 \times \cdots \times A_s$ będzie rozmaitością abelową nad ciałem $K$, gdzie $A_i$ są podrozmaitościami prostymi zawartymi w $A$. Niech $P, P_1, \ldots, P_r \in A(K)$ będą beztorsyjne oraz $P_1, \ldots, P_r$ będą punktami liniowo niezależnymi nad pierścieniem $\mathcal{R} := \mathrm{End}_K(A)$ i niech $\Lambda$ będzie $\mathbb{Z}$-podmodułem generowanym przez $P_1, \ldots, P_r$. Jeżeli*

$$r_v(P) \in r_v(\Lambda), \tag{3.2}$$

*dla każdego domkniętego punktu $v \in U$, wtedy $aP \in \sum_{i=1}^{r} \mathcal{R} P_i$ dla pewnej liczby $a \in \mathbb{Z} \setminus \{0\}$.*

*Dowód.*
W taki sam sposób jak w dowodzie lematu 3.3 możemy pokazać, że punkty $P, P_1, \ldots, P_r$ nie są liniowo niezależne nad $\mathcal{R}$. Mianowicie zapiszmy punkty $P, P_1, \ldots, P_r$ następująco:

$$P = \begin{bmatrix} P^1 \\ \vdots \\ P^t \end{bmatrix}, \qquad P_i = \begin{bmatrix} P_i^1 \\ \vdots \\ P_i^t \end{bmatrix}.$$

Z lematu 3.1 wiemy, że punkty $\{P_i^j\}_{1 \leqslant i \leqslant r}$ są liniowo niezależne nad pierścieniem $\mathcal{R}_j := \mathrm{End}(A_j)$, dla wszystkich $1 \leqslant j \leqslant t$. Z założenia (3.2) dostajemy $r_v(P^j) = \sum_{i=1}^{r} \alpha_i r_v(P_i^j)$, dla wszystkich $1 \leqslant j \leqslant s$.

Z lematu 3.3 dla wszystkich $1 \leqslant j \leqslant s$ istnieją endomorfizmy $\alpha_i^j \in \mathrm{End}_K(A_j)$ i stałe $a_j \in \mathbb{N}$ takie, że $a_j P = \sum_{i=1}^{r} \alpha_i^j P_i^j$. Przyjmując teraz $a = \mathrm{NWW}\,(a_j \;\;:\; 1 \leqslant j \leqslant t)$ dostajemy $aP^j = \sum_{i=1}^{r} \beta_i^j P_i^j$, dla pewnych $\beta_i^j \in \mathcal{R}_j$. Stąd dostajemy równanie

$$a \begin{bmatrix} P^1 \\ \vdots \\ P^t \end{bmatrix} = \sum_{i=1}^{r} \begin{bmatrix} \beta_1^i & & \cdots & & 0 \\ 0 & \ddots & & & \vdots \\ \vdots & & \beta_k^j & & \vdots \\ \vdots & & & \ddots & \vdots \\ 0 & & \cdots & & \beta_i^t \end{bmatrix} \begin{bmatrix} P_i^1 \\ \vdots \\ P_i^t \end{bmatrix},$$

co kończy dowód. □

**Twierdzenie 3.1.** *Niech $A$ będzie rozmaitością abelową nad ciałem $K$, $P, P_1, \ldots, P_r \in A(K)$ będą punktami beztorsyjnymi z $A(K)$. Niech $P_1, \ldots, P_r$ będą punktami linio-*

*wo niezależnymi nad* $\mathcal{R} := \mathrm{End}_K(A)$ *i* $\Lambda$ *będzie* $\mathbb{Z}$*-podmodułem generowanym przez* $P_1, \ldots, P_r$*. Niech* $U$ *będzie dowolnym otwartym niepustym podzbiorem w* $S$*. Jeżeli*

$$r_v(P) \in r_v(\Lambda), \tag{3.3}$$

*dla każdego domkniętego punktu* $v \in U$*, wtedy* $aP \in \sum_{i=1}^{r} \mathcal{R}P_i$*, dla pewnej liczby* $a \in \mathbb{Z} \setminus \{0\}$*.*

*Dowód.*
Z twierdzenia (1.4) i jego wniosku wiemy, że istnieje skończone rozszerzenie $L/K$ takie, że izogenia $\varphi : A \to A_1^{e_1} \times \cdots \times A_s^{e_s}$ jest zdefiniowana nad $L$. Oznaczmy $B = A_1^{e_1} \times \cdots \times A_s^{e_s}$, gdzie $B$ jest włóknem generycznym schematu abelowego $\mathcal{B}/S' = \prod_{i=1}^{t} \mathcal{A}_i^{e_i}$ oraz $A_i$ są włóknami generycznymi $\mathcal{A}_i$, które są prostymi podrozmaitościami abelowymi, które nie są parami izogeniczne. Możemy pracować nad $L$, ponieważ $A(K) \subset A(L)$ i $\mathcal{A}_v(k_v) \subset \mathcal{A}_w(k_w)$, dla wszystkich $w|v$ z $U_L$, gdzie $U_L \subset S'$ jest takim zbiorem otwartym, że $\mathcal{A}_i(U_l) \twoheadrightarrow A_i(L)$, dla każdego $i$ oraz $U_L \to \mathrm{Spec}\,\mathbb{Z}$ jest gładki. Z warunku (3.3) dostajemy

$$r_w(P) \in r_w(\Lambda), \tag{3.4}$$

dla wszystkich domkniętych punktów $w \in U_L$. Punkty $\varphi(P), \varphi(P_1), \ldots, \varphi(P_r)$ są beztorsyjne w $B(L)$ oraz punkty $\varphi(P_1), \ldots, \varphi(P_r)$ są liniowo niezależne nad $\mathcal{R}'_L = \mathrm{End}_L(B)$. Z lematu 3.4 dostajemy:

$$a\varphi(P) = \sum_{i=1}^{r} \mathcal{R}'_L \varphi(P_i),$$

dla pewnej stałej $a \in \mathbb{N}$.

Istnieje izogenia dualna $\widehat{\varphi} : B \to A$ nad $L$ taka, że $\widehat{\varphi} \circ \varphi = a' \in \mathbb{N}$. Stąd dostajemy $a'aP \in \mathcal{R}_L P_i + T$, gdzie $T \in A(L)_{tor}$. Z twierdzenia (2.2) istnieje nieskończenie wiele $w \in U_L$ takich, że $r_w(P_i) = 0$ w $A_w(k_w)$, dla wszystkich $1 \leqslant i \leqslant r$, czyli z warunku (3.4) dostajemy, że $r_w(T) = 0$, dla nieskończenie wielu $w$. Ale odwzorowanie $r_w$ jest iniektywne (twierdzenie 2.1) na punktach torsyjnych więc mamy $T = 0$. Oznaczmy $b = a'a$, czyli teraz nasza równość przyjmuje postać $bP = \sum_{i=1}^{r} \beta_i P_i$, gdzie $\beta_i \in \mathcal{R}_L := \mathrm{End}_L(A)$, ponieważ zakładaliśmy, że $L/K$ jest rozszerzeniem Galois. Dla $P, P_1, \ldots, P_r \in A(K)$ mamy $b|G\left(L/K\right)|P = \sum_{i=1}^{r} \mathrm{Tr}_{L/K}(\beta_i)P_i$, ale $\mathrm{Tr}(\beta_i) \in \mathcal{R}$, dla wszystkich $1 \leqslant i \leqslant r$. $\square$

**Twierdzenie 3.2.** *Niech* $A$ *będzie rozmaitością abelową nad ciałem* $K$*,* $P, P_1, \ldots, P_r$ *będą nietorsyjnymi punktami w* $A(K)$*. Niech* $P_1, \ldots, P_r$ *będą liniowo niezależne nad* $\mathcal{R}_K := \mathrm{End}_K(A)$*, a* $\Lambda$ *będzie* $\mathbb{Z}$*-podmodułem generowanym przez* $P_1, \ldots, P_r$*. Załóż-*

*my, że*

$$r_v(P) \in r_v(\Lambda), \tag{3.5}$$

*dla każdego domkniętego punktu $v \in U \subset S$, wtedy $P \in \Lambda$.*

*Dowód.*
Z twierdzenia (3.1) mamy:

$$aP = \sum_{i=1}^{r} \alpha_i P_i \tag{3.6}$$

gdzie $\alpha_i \in \mathcal{R} := \mathrm{End}_K(A)$.

Na początku załóżmy, że $\alpha_i \in \mathbb{Z}$, dla wszystkich $i = 1, \ldots, r$. Pokażemy, że $P \in \sum_{i=1}^{r} \mathbb{Z}P_i$. Niech $l^k$ będzie największą potęgą liczby pierwszej $l$, która dzieli $a$. Niech $U \subset S$ będzie ustalonym zbiorem otwartym. Twierdzenie 2.2 pokazuje, że dla każdego $i$ istnieje nieskończona rodzina punktów domkniętych $v \in U$ takich, że zachodzi

$$r_v(P_1) = \cdots = r_v(P_{i-1}) = r_v(P_{i+1}) = \cdots = r_v(P_r) = 0$$

i $r_v(P_i)$ ma rząd równy $l^k$ w $\mathcal{A}_v(k_v)_l$. Z równości (3.6) dostajemy $ar_v(P) = \alpha_i P_i$. Z warunku (3.5) mamy $r_v(P) = \beta_i r_v(P_i)$, dla $\beta_i \in \mathbb{Z}$. Stąd

$$(\alpha_i - a\beta_i) r_v(P_i) = 0$$

w $\mathcal{A}_v(k_v)_l$, czyli $l^k$ dzieli $\alpha_i$, dla wszystkich $i = 1, \ldots, r$. Teraz z równania (3.5) dostajemy:

$$\frac{a}{l^k} P = \sum_{i=1}^{r} \frac{\alpha_i}{l^k} P_i + T, \tag{3.7}$$

dla pewnego punktu $T \in A(K)[l^k]$. Ponownie dzięki twierdzeniu 2.2 istnieje nieskończenie wiele punktów domkniętych $v \in U$ takich, że $r_v(P_i) = 0$ w $A_v(k_v)_l$, dla wszystkich $i = 1, \ldots, r$ oraz wiemy, że $r_v(P) \in \sum_{i=1}^{r} \mathbb{Z} r_v(P_i)$, dla wszystkich $v \in U_K$. Więc z równości (3.7) dostajemy, że $r_v(T) = 0$ dla nieskończenie wielu $v$, ale to przeczy iniektywności odwzorowania $r_v$ chyba, że $T = 0$, dlatego w końcu dostajemy:

$$\frac{a}{l^k} P = \sum_{i=1}^{r} \frac{\alpha_i}{l^k} P_i$$

Powtarzając powyższy argument, dla wszystkich dzielników pierwszych $a$ dostajemy tezę.

Załóżmy teraz, że $\alpha_i \notin \mathbb{Z}$, dla pewnego $1 \leqslant i \leqslant r$. Dla dowolnej liczby pierwszej $l$ zbadajmy działanie $\alpha_i$ na $T_l(A)$. Z [18, Proposition 12.9] dostajemy

$P_{\alpha_i}(n) = deg(\alpha_i - n)$, dla wszystkich $n \in \mathbb{Z}$, gdzie $P_{\alpha_i}(t)$ jest wielomianem charakterystycznym automorfizmu $\alpha_i$ na $T_l(A)$, a $deg : \mathrm{End}(A) \to \mathbb{Z}$ jest funkcją stopnia. Stąd $P_{\alpha_i}(t) \in \mathbb{Z}[t]$, $P_{\alpha_i}(t)$ jest wielomianem unormowanym i niezależnym od wyboru $l$. Niech $E$ będzie ciałem rozkładu wielomianu $P_{\alpha_i}(t)$. Dla każdej liczby pierwszej $l$, która rozkłada się całkowicie w $E$, pierścień $\mathcal{O}_E$ możemy traktować jako podpierścień pierścienia $\mathbb{Z}_l$.

Jeżeli $P_{\alpha_i}(t)$ posiada co najmniej 2 różne pierwiastki, wtedy możemy znaleźć wektor $u \in T_l(A)$, który nie jest wektorem własnym $\alpha_i$. Wystarczy wziąć sumę dwóch wektorów własnych odpowiadających różnym wartościom własnym. Jeżeli $P_{\alpha_i}(t)$ posiada tylko jeden pierwiastek $\lambda \in \mathcal{O}_E$, wtedy $P_{\alpha_i}(t) = (x - \lambda)^{2g}$, a więc $2g\lambda \in \mathbb{Z}$, czyli $\lambda \in \mathcal{O}_E \cap \mathbb{Q} = \mathbb{Z}$. Z twierdzenia 1.9 dostajemy $\alpha_i \neq \lambda\,\mathrm{Id}_{T_l(A)}$, a więc wielomian minimalny automorfizmu $\alpha_i$ na $T_l(A)$ ma postać $(t-\lambda)^k$, dla $1 < k < 2g$.

Również w tym wypadku możemy znaleźć wektor $u \in T_l(A)$, który nie jest wektorem własnym automorfizmu $\alpha_i$. Przemnażając przez odpowiednią stałą (jeżeli to potrzebne), możemy założyć, że $u \notin lT_l(A)$. Stąd dla $m \in \mathbb{N}$ i $m$ dostatecznie dużego dostajemy, że warstwa $u + l^m T_l(A)$ nie jest wektorem własnym $\alpha_i$ na $T_l(A)/l^m T_l(A)$.

Jeżeli $\alpha_i u \equiv c_m u \mod l^m T_l(A)$, dla $c_m \in \mathbb{Z}/l^m$, $m \in \mathbb{N}$, wtedy $c_m \equiv c_{m+1} \mod l^m$, dla wszystkich $m \in \mathbb{N}$. Ale to przeczy założeniu, że $u$ nie jest wektorem własnym $\alpha_i$ na $T_l(A)$.

Niech $T \in A[l^m]$ będzie obrazem warstwy $u + l^m T_l(A)$ względem izomorfizmu $\mathcal{R}$ modułów $T_l(A)/l^m T_l(A) \cong A[l^m]$. Oznaczmy $L := K\,(A[l^m])$ i niech $R'$ będzie całkowitym domknięciem $R$ w $L$ i $U'$ będzie przeciwobrazem $U$ przy przekształceniu $\operatorname{Spec} R' \to \operatorname{Spec} R$. Z twierdzenia 2.2 możemy wybrać punkt domknięty $\omega$ z $U'$ taki, że $r_\omega(P_j) = 0$ dla $j \neq i$ i $r_\omega(P_i) = r_\omega(T)$ w $A_\omega(k_\omega)_l$. Stąd dostajemy $ar_\omega(P) = \alpha_i r_\omega(T)$. Z równości 3.5 istnieje stała $d \in \mathbb{Z}$ taka, że

$$ar_\omega(P) = adr_\omega(P_i) = adr_\omega(T),$$

z tego, że $r_\omega$ jest iniektywne na punktach torsyjnych dostajemy:

$$\alpha_i T = adT \text{ w } A[l^m].$$

Ale to przeczy temu, że $T$ nie jest wektorem własnym $\alpha_i$ działającego na $A[l^m]$. Stąd musimy mieć, że $\alpha_i \in \mathbb{Z}$, dla wszystkich $1 \leqslant i \leqslant r$, co kończy dowód. □

## 3.2. Problem liniowej zależności dla dowolnej podgrupy $\Lambda \subset A(K)$.

W tym rozdziale uogólnimy twierdzenie A z pracy [4], dowód tego twierdzenia jest identyczny jak dowód w [4] jednakże, ponieważ praca [4] jeszcze się nie ukazała, dlatego zamieszczam go tutaj w całości.

Z twierdzenia 1.4 wiemy, że każdą rozmaitość $A$ jest izogeniczna z $A_1^{e_1} \times \cdots \times A_t^{e_t}$, gdzie $A_i$ są prostymi podrozmaitościami. W taki sam sposób jak było to zrobione w pracy [4], dowód uogólnienia twierdzenia A można przeprowadzić w przypadku gdy $A = A_1^{e_1} \times \cdots \times A_t^{e_t}$. Ustalmy teraz oznaczenia:

- $c := |A(K)|_{tor}$;
- $\Omega := cA(K)$;
- $\Lambda$ podgrupa $A(K)$;
- $\mathcal{R} := \mathrm{End}_K(A)$;
- $\mathcal{R}_i := \mathrm{End}_K(A_i)$;
- $D_i := \mathcal{R}_i \otimes_{\mathbb{Z}} \mathbb{Q}$;

Przy powyższych oznaczeniach mamy $\mathcal{R} = \prod_{i=1}^t M_{e_i}(\mathcal{R}_i)$. Niech teraz $E/\mathbb{Q}$ będzie skończonym rozszerzeniem takim, że $D_i \otimes E \cong M_{d_i}(E)$, dla każdego $1 \leqslant i \leqslant t$.

Zauważmy, że warunek $r_v(P) \in r_v(\Lambda)$ pociąga $r_v(cP) \in r_v(c\Lambda)$, co więcej $cP \in c\Lambda + A(A)_{tor}$ zachodzi wtedy i tylko wtedy gdy $P \in \Lambda + A(T)_{tor}$

Niech punkty $P_1, \ldots, P_s$ będące $\mathbb{Z}$-bazą dla $\Omega$, będą takimi, że

$$\Lambda = \mathbb{Z}d_1P_1 + \cdots + \mathbb{Z}d_rP_r + \cdots \mathbb{Z}d_sP_s, \tag{3.8}$$

gdzie $d_i \in \mathbb{Z} \setminus \{0\}$ i $d_i = 0$, dla $i > r$.

**Twierdzenie 3.3.** *Niech $A/K$ będzie rozmaitością abelową zdefiniowaną nad ciałem skończenie generowanym nad $\mathbb{Q}$. Załóżmy, że $A$ jest izogeniczne z $A_1^{e_1} \times \cdots \times A_t^{e_t}$, gdzie $A_i$ są rozmaitościami prostymi, które nie są parami izogeniczne i $\dim_{\mathrm{End}_{K'}(A)^0} H_1(A_i(\mathbb{C}); \mathbb{Q}) \geqslant e_i$, dla każdego $1 \geqslant i \geqslant t$, a $K'$ jest skończonym rozszerzeniem $K$, gdzie izogenia jest zdefiniowana. Niech $P \in A(K)$ i $\Lambda$ będzie podgrupą $A(K)$. Jeżeli $r_v(P) \in r_v(\Lambda)$ dla wszystkich domkniętych punktów $v \in U$, wtedy $P \in \Lambda + A(K)_{tor}$.*

*Dowód.*

Wystarczy przeprowadzić dowód dla $\Omega$ i $\Lambda \subset \Omega$, na podstawie wstępnych uwag.

Załóżmy, że $P \notin \Lambda$, stąd dostajemy, że $P \otimes 1 \notin \Lambda \otimes \mathcal{O}_\lambda$, dla pewnego $\lambda | l$ i pewnej liczby pierwszej $l$. Ponieważ mamy

$$P = \sum_{j=1}^{s} n_j Pj,$$

więc istnieje $n_j \neq 0$, możemy tę równość również rozważać w $\Omega \otimes \mathcal{O}_\lambda$. Ponieważ $P \notin \Omega \otimes \mathcal{O}_\lambda$, więc istnieje $1 \leqslant j_0 \leqslant s$ takie, że $\lambda^{m_1} || n_{j_0}$ i $\lambda^{m_2} | d_{j_0}$, dla liczb naturalnych $m_1 < m_2$. Rozważmy teraz odwzorowanie $\mathbb{Z}$-modułów:

$$\pi \ : \ \Omega \to \mathbb{Z},$$

$$\pi(R) := \mu_{j_0},$$

gdzie $R = \sum_{i=1}^{s} \mu_i P_i, \quad \mu_i \in \mathbb{Z}$, dla wszystkich $1 \leqslant i \leqslant s$. Przez $\pi$ będziemy również oznaczać odwzorowanie $\pi \ : \ \Omega \otimes \mathbb{Q} \to \mathbb{Q}$. Z lematu 1.8 istnieje odwzorowanie $\widetilde{\pi} \in \mathrm{Hom}\,(\Omega \otimes_{\mathbb{Z}} \mathbb{Q},\ \mathbb{M}_e(\mathbb{D}))$ takie, że $tr(\widetilde{\pi}) = tr\pi$. Dzięki uwadze 1.4.1 istnieje $\widetilde{s} \in \mathrm{Hom}_{\mathbb{M}_e(\mathbb{D})}\,(Im\widetilde{\pi},\ \Omega \otimes \mathbb{Q})$ takie, że $\widetilde{\pi} \circ \widetilde{s} = Id$, co więcej, dla każdego $i$ istnieje $\widetilde{\pi(i)} \in \mathrm{Hom}_{M_{e_i}(D_i)}\,(\Omega_i^{e_i} \otimes_{\mathbb{Z}} \mathbb{Q},\ M_{e_i}(D_i))$ i $\widetilde{s} \in \mathrm{Hom}_{M_{e_i}(D_i)}\left(Im\widetilde{\pi(i)},\ \Omega_i^{e_i} \otimes_{\mathbb{Z}} \mathbb{Q}\right)$ takie, że $\widetilde{\pi(i)} \circ \widetilde{s(i)} = Id$ i $\widetilde{\pi} = \prod_{i=1}^{t} \widetilde{\pi(i)}$, $\widetilde{s} = \prod_{i=1}^{t} \widetilde{s(i)}$ oraz $\ker \widetilde{\pi} = \prod_{i=1}^{t} \ker \widetilde{\pi(i)}$ i mamy $\Omega_i^{e_i} \otimes_{\mathbb{Z}} \mathbb{Q} = Im\widetilde{s(i)} \oplus \ker \widetilde{\pi(i)}$, $\Omega \otimes_{\mathbb{Z}} \mathbb{Q} = Im\widetilde{s} \oplus \ker \widetilde{\pi}$. Z lematu 1.7 możemy przedstawić $Im\, \widetilde{s(i)}$ i ker $\widetilde{\pi(i)}$ jako sumę prostą prostych $M_{e_i}(D_i)$-podmodułów:

$$Im\, \widetilde{s(i)} = \bigoplus_{k=1}^{k_i} K(i)_1 \widetilde{\omega_k(i)},$$

$$\ker\, \widetilde{\pi(i)} = \bigoplus_{k=k_i+1}^{u_i} K(i)_1 \widetilde{\omega_k(i)}.$$

Zauważmy, że $k_i \leqslant e_i$ dla wszystkich $1 \leqslant i \leqslant t$ i elementy $\omega_1(i), \dots, \omega_{k_i}(i), \dots, \omega_{u_i}(i)$ tworzą bazę w przestrzeni wektorowej $\Omega_i \otimes_{\mathbb{Z}} \mathbb{Q}$ nad $D_i$. Możemy przyjąć bez straty ogólności, że $\omega_{k_i+1}(i), \dots, \omega_{u_i}(i) \in \Omega_i$.

Tensorujmy teraz odwzorowanie $\pi$ przez $\mathcal{O}_E$ i oznaczmy wynik jako $\pi' : \Omega \otimes_{\mathbb{Z}} \mathcal{O}_E \to \mathcal{O}_E$. W podobny sposób tensorujmy $\widetilde{\pi(i)}$ i $\widetilde{s(i)}$ przez $E$ i dostajemy odwzorowania $\widetilde{\pi(i)}' : \Omega_i^{e_i} \otimes_{\mathbb{Q}} E \to M_{e_i}(D_i) \otimes_{\mathbb{Q}} E$ oraz $\widetilde{s(i)}' : Im\widetilde{\pi(i)}' \to \Omega_i^{e_i} \otimes_{\mathbb{Z}} E$. Zauważmy, że dla każdego $1 \leqslant i \leqslant t$ przestrzeń wektorowa $\Omega_i \otimes_{\mathbb{Q}} E$ jest wolnym $D_i \otimes_{\mathbb{Z}} E \cong M_{e_i}(E)$-modułem. Przypomnijmy, że $\mathcal{R} \subset \mathbb{M}_e(\mathbb{D})$, $\mathcal{R} \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{M}_e(\mathbb{D})$ i $\Omega$ jest skończenie generowanym $\mathcal{R}$-modułem. Stąd istnieje liczba naturalna $M_0$ taka, że następujące homomorfizmy są dobrze określone:

$$M_0\widetilde{\pi}' \ : \ \omega \otimes_{\mathbb{Z}} \mathcal{O}_E \to \mathcal{R} \otimes_{\mathbb{Z}} \mathcal{O}_E,$$

$$\widetilde{s}' \ : \ M_0\widetilde{\pi}'\,(\omega \otimes_{\mathbb{Z}} \mathcal{O}_E) \to \Omega \otimes_{\mathbb{Z}} \mathcal{O}_E.$$

Ograniczmy teraz homomorfizm śladu do $\mathcal{R} \otimes_{\mathbb{Z}} \mathcal{O}_E \subset D \otimes_{\mathbb{Z}} E$, żeby dostać odwzorowanie liniowe nad $\mathcal{O}_E$, $tr \ : \ \mathcal{R} \otimes_{\mathbb{Z}} \mathcal{O}_E \to E$. Mamy też $trM_0\widetilde{\pi} = M_o\widetilde{\pi}$ i $M_0\widetilde{\pi}' \circ \widetilde{s}' = M_0 Id_{M_0\widetilde{\pi}'(\Omega \otimes_{\mathbb{Z}} \mathcal{O}_K)}$. Rozważmy $K(i)_1 \subset M_{e_i}\,(\mathcal{R}_i \otimes_{\mathbb{Z}} \mathcal{O}_E)$ i zdefiniujmy

$M_{e_i}\,(\mathcal{R}_i \otimes_{\mathbb{Z}} \mathcal{O}_E)$-moduł:

$$\widetilde{\Gamma(i)} := \sum_{i=1}^{k_i} K(i)_1 M_0 \widetilde{\omega_k(i)} + \sum_{i=k_i+1}^{u_i} K(i)_1 \widetilde{\omega_k(i)} \subset \Omega_i^{e_i} \otimes_{\mathbb{Z}} \mathcal{O}_E$$

i $\mathcal{R} \otimes_{\mathbb{Z}} \mathcal{O}_E$-moduł $\widetilde{\Gamma} := \bigoplus \widetilde{\Gamma(i)} \subset \Omega \otimes_{\mathbb{Z}} \mathcal{O}_E$.

Przyjmijmy oznaczenia $M_2 := \left[\Omega \otimes_{\mathbb{Z}} \mathcal{O}_E \,:\, \widetilde{\Gamma}\right]$ i $M_3 := \left[\widetilde{\Gamma} \,:\, M_2\Omega \otimes_{\mathbb{Z}} \mathcal{O}_\lambda\right]$. Z wyboru punktu $P_{j_0}$ dostajemy $\pi(P) \notin \pi'\,(\Gamma \otimes_{\mathbb{Z}} \mathcal{O}_\lambda) + \lambda^m \pi'\,(\Omega \otimes_{\mathbb{Z}} \mathcal{O}_\lambda)$, dla $m > m_2$. Stąd

$$M_0\widetilde{\pi}(P) \notin M_0\widetilde{\pi}\,(\Gamma \otimes_{\mathbb{Z}} \mathcal{O}_\lambda) + M_0\lambda^m\widetilde{\pi}\,(\Gamma \otimes_{\mathbb{Z}} \mathcal{O}_\lambda)\,, \tag{3.9}$$

ponieważ $trM_0\widetilde{\pi} = M_0\pi$. Określamy $K(i)_{1,\lambda} := K(i)_1 \otimes_{\mathcal{O}_K} \mathcal{O}_\lambda \subset M_{e_i}(\mathcal{R}_{i\lambda})$. Niech $Q \in \Gamma$ będzie ustalonym punktem. Możemy wtedy zapisać

$$M_2P = \sum_{i=1}^{t}\sum_{k=1}^{k_1} \widetilde{\alpha_k(i)_1} M_0 \widetilde{\omega_k(i)} + \sum_{i=1}^{t}\sum_{k=k_i+1}^{u_i} \widetilde{\alpha_k(i)}_1 \widetilde{\omega_k(i)},$$

$$M_2Q = \sum_{i=1}^{t}\sum_{k=1}^{k_1} \widetilde{\beta_k(i)_1} M_0 \widetilde{\omega_k(i)} + \sum_{i=1}^{t}\sum_{k=k_i+1}^{u_i} \widetilde{\beta_k(i)}_1 \widetilde{\omega_k(i)},$$

dla pewnych $\widetilde{\alpha_k(i)_1}, \widetilde{\beta_k(i)_1}$ gdzie $1 \leqslant k \leqslant u_i$ i $1 \leqslant i \leqslant t$. Wtedy:

$$M_0\widetilde{\pi}\,(M_2(P-Q)) = M_0^2 \prod_{i=1}^{t}\sum_{k=1}^{k_i} \left(\widetilde{\alpha_k(i)_1} - \widetilde{\beta_k(i)_1}\right) \widetilde{\pi}(\widetilde{\omega_k(i)}). \tag{3.10}$$

Skoro $\widetilde{\pi} = \prod_{i=1}^t \widetilde{\pi(i)}$ odwzorowuje moduł $\Omega \otimes_{\mathbb{Z}} \mathbb{Q} = \bigoplus_{i=1}^t \Omega_i^{e_i} \otimes_{\mathbb{Z}} \mathbb{Q}$ w pierścień $\mathbb{M}_e(\mathbb{D}) = \prod_{i=1}^t M_{e_i}(D_i)$, zastępujemy więc $\sum_{i=1}^t$ przez $\prod_{i=1}^t$. Teraz z wzorów 3.9 i 3.10 dostajemy

$$M_0^2 \prod_{i=1}^{t}\sum_{k=1}^{k_i} \left(\widetilde{\alpha_k(i)_1} - \widetilde{\beta_k(i)_1}\right) \widetilde{\pi}(\widetilde{\omega_k(i)}) \notin \lambda^m M_0\widetilde{\pi}\,(M_2\Omega \otimes_{\mathbb{Z}} \mathcal{O}_\lambda)$$

W ten sposób:

$$M_0^2 \prod_{i=1}^{t}\sum_{k=1}^{k_i} \left(\widetilde{\alpha_k(i)_1} - \widetilde{\beta_k(i)_1}\right) \widetilde{\pi}(\widetilde{\omega_k(i)}) \notin \lambda^m M_0\widetilde{\pi}\left(M_3\widetilde{\Lambda}\right), \tag{3.11}$$

stąd dla pewnego $1 \leqslant i \leqslant t$ i $1 \leqslant k \leqslant k_i$ dostajemy

$$\widetilde{\alpha_k(i)_1} - \widetilde{\beta_k(i)_1} \notin \lambda^m M_3 K(i)_{1,\lambda}. \tag{3.12}$$

Niech $e \in \mathbb{N}$ będzie indeksem rozgałęzienia $\lambda$ nad $l$. Zauważmy, że dla każdej liczby $n \in \mathbb{N}$ mamy następujący izomorfizm $A_i[\lambda^{en}] \cong \mathcal{L}_i \otimes_{\mathbb{Z}} \mathcal{O}_\lambda$, ponieważ $l\mathcal{O}_K = \prod_{\lambda|l} \lambda^e$, $A_i[l^n] \cong \mathcal{L}_i \otimes_{\mathbb{Z}} \mathbb{Z}_l / l^n \mathcal{L}_i \otimes_{\mathbb{Z}} \mathbb{Z}_l$ i $A_i[l^n] = \bigoplus_{\lambda|l} A_i[\lambda^{ne}]$.

Przypomnijmy, że dla każdego $1 \leqslant 1 \leqslant t$ wybieraliśmy kratę $\mathcal{L}'_i \subset \mathcal{L}_i$, taką by była ona wolnym $\mathcal{R}_i$-modułem. Niech $M_4 := max_{1 \leqslant i \leqslant t} [\mathcal{L}_i : \mathcal{L}'_i]$. Zapiszmy $\mathcal{L} := \bigoplus_{i=1}^t \mathcal{L}_i$. Z Snake Lemma jądro następującego odwzorowania jest skończone i anihilowane przez $\lambda^{em_4}$

$$z(n, \lambda) \quad : \quad \mathcal{L}' \otimes_{\mathbb{Z}} \mathcal{O}_\lambda / \lambda^{en} \mathcal{L}' \otimes_{\mathbb{Z}} \mathcal{O}_\lambda \to \mathcal{L} \otimes_{\mathbb{Z}} \mathcal{O}_\lambda / \lambda^{en} \mathcal{L} \otimes_{\mathbb{Z}} \mathcal{O}_\lambda, \tag{3.13}$$

gdzie $l^{m_4} || M_4$. Niech $m_0$ i $m_3$ będą liczbami naturalnymi o następujących własnościach: $l^{m_0} || M_0$ i $l^{m_3} || M_3$. Teraz $\eta_1(i), \ldots, \eta_{p_i}(i)$ będzie bazą $\mathcal{L}'_i$ nad $\mathcal{R}_i$. Z założenia mamy $p_i \geqslant e_i$, dlatego $\mathcal{L}'_i \otimes_{\mathbb{Z}} \mathcal{O}_\lambda / \lambda^{en} \mathcal{L}'_i \otimes_{\mathbb{Z}} \mathcal{O}_\lambda$ jest wolnym $\mathcal{R}_{i,\lambda} / \lambda^{en} \mathcal{R}_{i,\lambda}$-modułem z bazą $\eta_1 \bar{(i)}, \ldots, \eta_{p_i} \bar{(i)}$, gdzie $\eta_k \bar{(i)}$ oznacza obraz $\eta_k(i)$ w $\mathcal{L}'_i \otimes_{\mathbb{Z}} \mathcal{O}_\lambda / \lambda^{en} \mathcal{L}'_i \otimes_{\mathbb{Z}} \mathcal{O}_\lambda$, dla każdego $1 \leqslant k \leqslant p_i$. Niech teraz $T_k(i)$ będzie obrazem elementu $\eta_k \bar{(i)}$ po przez odwzorowanie $z(n, \lambda)$, dla wszystkich $1 \leqslant k \leqslant p_i$ i $1 \leqslant i \leqslant t$. Weźmy teraz $n \in \mathbb{N}$ tak by spełniało nierówność $en > m + em_0 + em_3 + em_4$ i oznaczmy $L := K(A[l^n]) = K(r(A)[l^n])$. Zauważmy, że $A[l^n] \subset A(L)$. Z twierdzenia 2.2 istnieje rodzina punktów domkniętych $w$ w $U_L$ o dodatniej gęstości takich, że $r_w(\omega_k(i)) = 0$, dla $1 \leqslant i \leqslant t$, $k_i + 1 \leqslant k \leqslant u_i$ i $r_w(\omega_k(i)) = r_w(T_k(i))$, dla $1 \leqslant i \leqslant t$, $1 \leqslant k \leqslant k_i$.

Ponieważ $r_w(P) \in r_w(\Gamma)$, więc możemy wybrać $Q \in \Gamma$ w taki sposób, że $r_w(P) = r_w(Q)$. Teraz stosując odwzorowanie redukcji do równania:

$$M_2(P - Q) = \sum_{i=1}^{t} \sum_{k=1}^{k_i} \left( \widetilde{\alpha_k(i)_1} - \widetilde{\beta_k(i)_1} \right) M_0 \widetilde{\omega_k(i)} + \sum_{i=1}^{t} \sum_{k=k_1+1}^{u_i} \left( \widetilde{\alpha_k(i)_1} - \widetilde{\beta_k(i)_1} \right) M_0 \widetilde{\omega_k(i)}$$

dostajemy

$$0 = \sum_{i=1}^{t} \sum_{k=1}^{k_i} \left( \widetilde{\alpha_k(i)_1} - \widetilde{\beta_k(i)_1} \right) M_0 (\widetilde{T_k(i)}).$$

Ponieważ odwzorowanie redukcji jest iniektywne na l-torsyjnej podgrupie w $A(L)$ na mocy twierdzenia 2.1, uzyskujemy:

$$0 = \sum_{i=1}^{t} \sum_{k=1}^{k_i} \left( \widetilde{\alpha_k(i)_1} - \widetilde{\beta_k(i)_1} \right) M_0 (T_k(i)),$$

zatem $\sum_{i=1}^{t} \sum_{k=1}^{k_i} \left( \widetilde{\alpha_k(i)_1} - \widetilde{\beta_k(i)_1} \right) M_0 \widetilde{\eta_k \bar{(i)}} \in \ker z(n\lambda)$, a więc obraz elementu

$$\lambda^{em_0 + em_4} \sum_{i=1}^{t} \sum_{k=1}^{k_i} \left( \widetilde{\alpha_k(i)_1} - \widetilde{\beta_k(i)_1} \right) M_0 \widetilde{\eta_k(i)}$$

w $\mathcal{L}' \otimes_{\mathbb{Z}} \mathcal{O}_\lambda / \lambda^{en} \mathcal{L}' \otimes_{\mathbb{Z}} \mathcal{O}_\lambda$ jest równy zero. Stąd:

$$\sum_{i=1}^{t} \sum_{k=1}^{k_i} \left( \widetilde{\alpha_k(i)_1} - \widetilde{\beta_k(i)_1} \right) M_0 \widetilde{\eta_k(i)} \in \lambda^{en-em_0-em_4} \mathcal{L}' \otimes_{\mathbb{Z}} \mathcal{O}_\lambda.$$

Ponieważ $\eta_1(i), \ldots, \eta_{p_i}(i)$ tworzą bazę w $\mathcal{L}_i' \otimes_{\mathbb{Z}} \mathcal{O}_\lambda$ nad $\mathcal{R}_{i,\lambda}$, dostajemy

$$\widetilde{\alpha_k(i)_1} - \widetilde{\beta_k(i)_1} \in \lambda^{en-em_0-em_4} K(i)_{1,\lambda},$$

dla wszystkich $1 \leqslant i \leqslant t$, $1 \leqslant k \leqslant k_i$, ale warunek jest sprzeczny z (3.12), ponieważ wybraliśmy $n$ tak by $en - em_0 - em_4 > m + em_3$

$\square$

# Rozdział 4

# Problem nośnika

## 4.1. Problem nośnika

**Twierdzenie 4.1.** *Niech $A/K$ będzie rozmaitością abelową nad ciałem skończenie generowanym $K$ nad $\mathbb{Q}$. Załóżmy, że $A = A_1^{e_1} \times \cdots A_t^{e_t}$, gdzie $A_i$ są prostymi rozmaitościami abelowymi, parami nieizogenicznymi i niech $P, Q \in A(K)$ będą punktami nieskończonego rzędu. Niech $U \subset S$ będzie zbiorem otwartym. Niech dla każdego $n \in \mathbb{Z}$ i dla każdego domkniętego punktu $v \in U$, zachodzi*

$$nr_v(P) = 0 \Rightarrow nr_v(Q) = 0. \tag{4.1}$$

*Wtedy istnieje liczba naturalna $k$ i endomorfizm $\alpha \in \operatorname{End}_K A$ taki, że zachodzi równość*

$$\alpha(P) = kQ.$$

*Dowód.*
Na początku przyjmijmy oznaczenia:

$$P = [P_1^{j_1}, \ldots, P_t^{j_t}]_{1 \leqslant j_1 \leqslant e_1, \ldots, 1 \leqslant j_t \leqslant e_t}, \qquad Q = [Q_1^{j_1}, \ldots, Q_t^{j_t}]_{1 \leqslant j_1 \leqslant e_1, \ldots, 1 \leqslant j_t \leqslant e_t}$$

i $\mathcal{R} := \operatorname{End} A$, $\mathcal{R}_i = \operatorname{End} A_i$. Niech teraz punkty $P_k^{i_{k_1}}, \ldots, P_k^{i_{k_{e'_k}}}$ będą liniowo niezależne nad $\mathcal{R}_k$. Dlatego mamy, że dla każdego $k$ istnieje stała $c \in \mathbb{N}$, spełniająca równość:

$$cP_k^i = \sum_{j=1}^{e'_k} \beta_k^{i_{k_j}} P_k^{i_{k_j}}.$$

Pokażemy teraz, że punkty $P_k^{i_{k_1}}, \ldots, P_k^{i_{k_{e'_k}}}, Q_k^r$ są liniowo zależne, dla każdego $1 \leqslant r \leqslant e_k$. Załóżmy, że te punkty nie są liniowo zależne nad $\mathcal{R}_k$. Wtedy z twierdzenia 2.2

możemy wybrać taki punkt domknięty $v \in U$, żeby $ord_v(P_k^{j_i}) | l^k c$ i $ord_v(Q_k^r) > l^k c$. Wtedy $cl^k r_v(P) = 0$, ale $cl^k r_v(Q) \neq 0$ daje sprzeczność z założeniem, a więc te punkty muszą być zależne.

Ponieważ te punkty są zależne, więc dla każdego $1 \leqslant r \leqslant e_k$ i $1 \leqslant k \leqslant t$ istnieją endomorfizmy $\alpha_k^t, \beta_k^{i_1}, \ldots, \beta_k^{i_{e'_k}} \in R_k$, $\alpha_k^t \neq 0$, spełniające równość:

$$\alpha_k^s Q_k^t = \sum_{j=1}^{e'_k} \beta_k^{i_j} P_k^{i_{k_j}}.$$

Teraz dla każdego $\alpha_k^s$ istnieje izogenia dualna dla której zachodzi $d_k^t := \widehat{\alpha_k^t} \alpha_k^t$ i niech $d := NWW\{d_k^t\}$, wtedy dostajemy :

$$\alpha(P) = \begin{bmatrix} d & 0 & \cdots & 0 \\ 0 & d & \ddots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & d \end{bmatrix} Q,$$

czyli dostaliśmy tezę $\alpha(P) = dQ$. □

**Wniosek 4.1.** *Niech $A/K$ będzie rozmaitością abelową nad ciałem skończenie generowanym $K$ nad $\mathbb{Q}$ i niech $P, Q \in A(K)$ będą punktami nieskończonego rzędu. Niech dla każdego $n \in \mathbb{Z}$ i dla każdego punktu domkniętego $v \in U$, zachodzi*

$$nr_v(P) = 0 \Rightarrow nr_v(Q) = 0. \tag{4.2}$$

*Wtedy istnieją: liczba naturalna $k$ i endomorfizm $\alpha \in \operatorname{End}_K A$ takie, że*

$$\alpha(P) = kQ$$

*Dowód.*
Wiemy, że istnieje ciało $L/K$ nad którym jest zdefiniowana izogenia $\varphi : A \to A_1^{e_1} \times \cdots A_s^{e_s}$. Istnieje stała $c \in \mathbb{N}$ taka, że spełniony jest warunek

$$nr_w\left(\varphi(P)\right) = 0 \Rightarrow nr_w\left(\varphi(cQ)\right) = 0.$$

dla pewnego $w \in U'$ leżącego nad $v$, gdzie $U'$ jest przeciwobrazem $U$ przy przekształceniu $\operatorname{Spec} R' \to \operatorname{Spec} R$ i $R'$ jest całkowitym domknięciem $R$ w $L$. Niech $B = \prod_{i=q}^t A_i^{e_i}$. Teraz z twierdzenia 4.1 istnieje stała $C \in \mathbb{Z}$ i endomorfizm $\beta \in \operatorname{End}_L(B)$ taki, że

$$C\varphi(cQ) = \beta\varphi(P).$$

Ponieważ $\varphi$ jest izogenią, to istnieje izogenia dualna $\widehat{\varphi}$, dla której prawdziwe jest:

$$[\deg \varphi]CcQ = \widehat{\varphi}\beta\varphi(P).$$

Teraz argumentując tak samo jak w końcowej części dowodu twierdzenia 3.1 dostajemy:

$$kQ = \alpha(P),$$

dla $k \in \mathbb{Z}$ i $\alpha \in \operatorname{End}_K A$. □

## 4.2. Problem multinośnika

W tym podrozdziale przedstawię problem multinośnika który zaproponował S. Barańczuk w [5]

**Twierdzenie 4.2.** *Niech $A$ będzie rozmaitością abelową zdefiniowaną nad ciałem $K$. Niech $P_0, P_1, \dots, P_n, Q_0, Q_1, \dots, Q_n \in A$ będą punktami nieskończonego rzędu.*

*Załóżmy, że dla dowolnej rodziny nieujemnych liczb całkowitych $m_1, m_2, \dots, m_n$ i dla wszystkich punktów domkniętych $v \in U$ mamy:*

$$m_1 r_v(P_1) + \cdots + m_n r_v(P_n) = r_v(P_0) \Rightarrow m_1 r_v(Q_1) + \cdots + m_n r_v(Q_n) = r_v(Q_0).$$

*Wtedy istnieją $k_i \in \mathbb{Z}\backslash\{0\}$ i $\alpha_i \in \operatorname{End}_K(A)\backslash\{0\}$ takie, że $\alpha_i P_i = k_i Q_i$, dla wszystkich $0 \leqslant i \leqslant n$.*

*Dowód.* Załóżmy na początku, że $A = A_1^{e_1} \times \cdots \times A_t^{e_t}$, gdzie $A_i$ są podrozmaitościami prostymi nieizogenicznymi między sobą. Przyjmijmy teraz takie same oznaczenia jak w dowodzie twierdzenia 4.1:

$$P = [P_1^{j_1}, \dots, P_t^{j_t}]_{1 \leqslant j_1 \leqslant e_1, \dots, 1 \leqslant j_t \leqslant e_t}, \qquad Q = [Q_1^{j_1}, \dots, Q_t^{j_t}]_{1 \leqslant j_1 \leqslant e_1, \dots, 1 \leqslant j_t \leqslant e_t}$$

i $\mathcal{R} := \operatorname{End}_K A$, $\mathcal{R}_i = \operatorname{End}_K A_i$. Ponieważ teza ma zachodzić dla dowolnej rodziny nieujemnych liczb całkowitych to możemy przyjąć że $m_i = 0$, dla wszystkich $i = 1, \dots, t$. Wtedy dostajemy warunek:

$$r_v(P_0) = 0 \Rightarrow r_v(Q_0) = 0$$

Argumentując tak samo jak w dowodzie twierdzenia 4.1 dostajemy, że

$$k_0 Q_0 = \alpha P_0.$$

Przyjmijmy teraz, że $m_i = 1$ i $m_j = 0$, dla $j \neq i$, wtedy nasz warunek jest postaci

$$r_v(P_i) = r_v(P_0) \Rightarrow r_v(Q_i) = r_v(Q_0).$$

Niech $l \nmid k_0$. Pokażemy teraz, że punkty $P_i$ i $Q_i$ są liniowo zależne. Załóżmy, że nie są, wtedy z twierdzenie 2.2 możemy przyjąć, że $r_v(P_i) = 0$ i $r_v(Q_i) \neq 0$ w $\mathcal{A}_v(k_v)_l$. Jednak punkty $P_0$ i $Q_0$ są liniowo zależne, a więc $0 = r_v(P_i) = r_v(P_0) = r_v(Q_0)$ ale

$$0 \neq r_v(Q_i) = r_v(Q_0) = 0$$

Sprzeczność, czyli punkty $P_i$ i $Q_i$ są liniowo zależne.

Teraz możemy argumentować podobnie jak w dowodzie twierdzenia 4.1 żeby dostać:

$$\alpha_i P_i = k_i Q_i$$

Teraz używając metody rozwiniętej w dowodzie wniosku 4.1 dostajemy tezę. □

Poniższe twierdzenie w przypadku ciał liczbowych zostało udowodnione przez A. Schinzela [29]. W przypadku rozmaitości abelowych nad ciałem liczbowym zostało udowodnione przez W. Gajdę i K. Górnisiewicza w [11].

**Twierdzenie 4.3.** *Niech $A$ będzie rozmaitością abelową zdefiniowaną nad ciałem $K$. Niech $P_1, \ldots, P_n, Q_1, \ldots, Q_n \in A$ będą punktami nieskończonego rzędu. Załóżmy, że dla dowolnej rodziny nieujemnych liczb całkowitych $m_1, m_2, \ldots, m_n$ i dla wszystkich punktów domkniętych $v \in U$, gdzie $U$ otwarty w $S$, mamy:*

$$m_1 r_v(P_1) + \cdots + m_n r_v(P_n) = 0 \Rightarrow m_1 r_v(Q_1) + \cdots + m_n r_v(Q_n) = 0.$$

*Wtedy istnieje $k_i \in \mathbb{Z} \setminus \{0\}$ i $\alpha_i \in \mathrm{End}(A) \setminus \{0\}$ takie, że $\alpha_i P_i = k_i Q_i$, dla wszystkich $0 \leqslant i \leqslant n$.*

*Dowód.* Dowód jest analogiczny do poprzedniego dowodu. □

# Bibliografia


[1] G. Banaszak, *On a Hasse principle for Mordel-Weil groups.* Comptes Rendus Mathematique 347 (2009), 709–714.

[2] G. Banaszak, W. Gajda i Krasoń P, *Detecting linear dependence by reduction maps.* Journal of Number Theory 115(2) (2005), 322–342.

[3] G. Banaszak, W. Gajda i Krasoń P, *On reduction map for étale $K$-theory of curves.* Homology, Homotopy and Applications, Proceedings of Victor's Snaith 60th Birthday Conference 7(3) (2005), 1–10.

[4] G. Banaszak i Krasoń P, *On arithmetic in Mordell-Weil groups.* Preprint.

[5] S. Barańczuk, *On reduction maps and support problem in $K$-theory and abelian varieties.* Journal of Number Theory 119 (2006), 1–17.

[6] S. Bosch, W. Lülkebohmert i M. Raynaud, *Néron Models.* Springer-Verlag, Berlin-Heidelberg-New York, 1990.

[7] C. Corralez-Rodrigáñez i R. Schoof, *Support problem and its elliptic analogue.* Journal of Number Theory 64 (1997), 276–290.

[8] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern.* Inv. Math. 73 (1983), 349–366.

[9] G. Faltings, *Complements to Mordell.* A publication of the Max-Planck-instutute für Mathematik, Bonn, 1992. Rational points. Seminar Bonn/Wuppertal 1983/1984, 203–227.

[10] G. Faltings i C-L. Chai, *Degeneration of abelian varieties.* Springer-Verlag, Berlin-Heidelberg-New York, 1980.

[11] W. Gajda i K. Górnisiewicz, *Linear dependence in Mordell-Weil groups.* Journal für die reine und angew. Math. 630 (2009), 219–233.

[12] N.M. Katz, *Galois properties of torsion points on abelian varieties.* Invent. Math, 62 (1981), 481–502.

[13] Hartshorne r., *Algebraic Geometry.* Springer-Verlag, Berlin-Heidelberg-New York, 1997.

[14] C. Khare, *Compatible systems of mod p Galois rpresentations and Hecke characters.* Math. Res. Letters, 10 (2003), 71–83.

[15] S. Lang, *Number theory III, diophantine geometry.* Springer-Verlag, Berlin-Heidelberg-New York, 1991.

[16] M. Larsen, *The support problem for abelian varieties.* Jurnal of Number Theory 101 (2003), 398-403.

[17] M. Larsen i R. Schoof, *Whitehead's Lemmas and Galois cohomology of abelian varieties.* Preprint.

[18] J.S. Milne, *Abelian varieties.* Springer-Verlag, Berlin-Heidelberg-New York, 1986. Arithmetic Geometry, G. Cornell, J.H. Silverman eds.

[19] J.S. Milne, *Étale cohomology.* Princeton Univ. Press, Princeton, New Jersey, 1980.

[20] D. Mumford, *Abelian varieties.* Oxford Univ. Press, Bombay, 1970.

[21] D. Mumford, *Geometric Invariant theory.* Splinger-Verlag, Heidelberg, 1970.

[22] R. Noot, *Abelian varieties - properties of ordinary reduction.* Compos. Math. 97 (1995), 161–171.

[23] R. Pink, *On the order of the reduction of a point on an abelian variety.* Mathematische Annalen 330 (2004), 275–291.

[24] A. Perucca, *The $l$-adic support problem for abelian varieties.* Preprint.

[25] I. Reiner, *Maximal orders.* Academic Press, London, New York, San Francisco, 1975.

[26] K. A. Ribet, *Kummer theory on extensions of abelian varieties by tori.* Duke Mathematical Journal 46(4) (1979), 745–761.

[27] Rosen M., *Number Theory in Function Fields.* Springer-Verlag, Berlin-Heidelberg-New York, 2001.

[28] A. Schinzel, *On power residues and exponential congruences.* Acta Arithmetica 27 (1975), 397–420.

[29] A. Schinzel, *O pokazatelnych sravneniach.* Mat. Zapiski 2 2 (1996), 121–126.

[30] J-P. Serre, *Lettre á Ken Ribet du 7/3/1986.*

[31] J-P. Serre, *Sur les groupes de congruence des variétés abéliennes. II.* Izviestia Akademii Nauk CCCP 35 (1971), 731-737.

[32] J-P. Serre i J. Tate, *Good reduction of abelian varieties.* Annals of Math 68 (1968), 492–517.

[33] A. Skorobogatov i Yu. G. Zarhin, *A finiteness theorem for Brauer groups of abelian varieties and K3 surfaces.* J. Algebraic Geometry 17 (2008), 481-502.

[34] J. Silverman, *The arithmetic of elliptic curves.* Springer-Verlag, Berlin-Heidelberg-New York, 1986.

[35] J. Tate, *Relation between $K_2$ and Galois cohomology.* Invent. Math. 36 (1976), 257–274.

[36] T. Weston, *Kummer theory of abelian varieties and reductions of Mordell-Weil groups.* Acta Arithmetica 110 (2003), 77–88.

[37] J.G. Zarhin, *A finiteness theorem for unpolarized Abelian varieties over number fields with prescribed places of bad reduction.* Invent. math. 79 (1875), 309–321.

[38] J.G. Zarhin, *Abelian varieties in charactersitic p.* Mat. Zamietki 19(3) (1876), 240–400.

[39] J.G. Zarhin, *Abelian varieties without homotheties.* Math. Res. Lett. 14 (2007), 157–164.