Uniwersytet im. Adama Mickiewicza w Poznaniu
Wydział Matematyki i Informatyki

Praca magisterska

Bartosz Naskręcki

O pewnym równaniu diofantycznym

Praca napisana pod kierunkiem
prof. dr. hab.
Wojciecha Gajdy

Poznań 2010

Poznań, dnia .....

OŚWIADCZENIE

Ja, niżej podpisany **Bartosz Naskręcki** student Wydziału Matematyki i Informatyki Uniwersytetu im. Adama Mickiewicza w Poznaniu oświadczam, że przedkładaną pracę dyplomową pt: **O pewnym równaniu diofantycznym**, napisałem samodzielnie. Oznacza to, że przy pisaniu pracy, poza niezbędnymi konsultacjami, nie korzystałem z pomocy innych osób, a w szczególności nie zlecałem opracowania rozprawy lub jej części innym osobom, ani nie odpisywałem tej rozprawy lub jej części od innych osób.

Oświadczam również, że egzemplarz pracy dyplomowej w formie wydruku komputerowego jest zgodny z egzemplarzem pracy dyplomowej w formie elektronicznej.

Jednocześnie przyjmuję do wiadomości, że gdyby powyższe oświadczenie okazało się nieprawdziwe, decyzja o wydaniu mi dyplomu zostanie cofnięta.

.....

Spis treści

1 Wstęp

Teoria liczb jest dziedziną matematyki, która koncentruje się wokół znajdowania rozwiązań równań w liczbach całkowitych. Już od starożytności, od czasów Diofantosa i *Arytmetyki* jego autorstwa, wiemy, że poszczególne równania nie dają się rozwiązywać w sposób jednolity. W zasadzie można powiedzieć, że każde równanie wielomianowe o współczynnikach całkowitych, zwane odtąd równaniem diofantycznym, wymaga zazwyczaj zupełnie odrębnego algorytmu, który pozwala znaleźć wszystkie rozwiązania całkowite.

Celem tej pracy jest omówienie metod rozwiązywania równania

$$y^2 = x^3 + Ax + B, \tag{1.1}$$

gdzie liczby A oraz B są ustalonymi liczbami całkowitymi. Ogólniej interesować będzie nas problem znajdowania rozwiązań wymiernych takiego równania (przy założeniu, że $A, B \in \mathbb{Q}$). Przez wyrugowanie mianowników taki problem jest równoważny znajdowaniu rozwiązań całkowitych pewnego równania diofantycznego.

Pytanie o istnienie efektywnego algorytmu znajdującego rozwiązania całkowite bądź wymierne równania (1.1) ma swoje daleko idące uogólnienie zwane X problemem Hilberta:

> Ustalić czy istnieje algorytm, który w skończonej liczbie kroków potrafi rozstrzygnąć dla każdego równania diofantycznego określonego przez wielomian skończonej liczby zmiennych o współczynnikach całkowitych, czy istnieje jego rozwiązanie w liczbach całkowitych.

W szeregu prac M. Davis, H. Putnam i J. Robinson oraz ostatecznie Y. Matiyasevich pokazali, że odpowiedź na powyższe pytanie jest w ogólności negatywna. Mimo to, w szczególnych przypadkach, tzn. gdy równanie diofantyczne jest liniowe (wielomian zadający to równanie jest liniowy) lub kwadratowe, istnieją efektywne algorytmy, które pozwalają nie tylko stwierdzić istnienie rozwiązań, ale również podać efektywny sposób ich znajdowania. Przypadek równania (1.1) jest najprostszym, dla którego nie istnieje w pełni ogólny algorytm rozstrzygający istnienie rozwiązań całkowitych.

Dziesiąty problem Hilberta nie jest rozstrzygnięty do dziś, jeśli współczynniki równania wielomianowego są liczbami wymiernymi i poszukuje się istnienia

rozwiązań wymiernych. Tym bardziej istotne jest poszukiwanie metod rozwiązywania, np. równania (1.1) w liczbach wymiernych.

Możemy powiedzieć dużo więcej o strukturze rozwiązań równania (1.1) jeśli wprowadzimy dodatkowe pojęcia, które ukażą nam geometryczną strukturę tych rozwiązań.

Definicja 1.0.1 (Krzywa eliptyczna)**.** Zbiór rozwiązań zespolonych równania:

$$y^2 = x^3 + Ax + B \tag{1.2}$$

dla $A, B \in \mathbb{Q}$ nazywamy **krzywą eliptyczną** nad ciałem $\mathbb{Q}$ o ile równanie definiujące krzywą ma dobrze określoną prostą styczną w każdym punkcie tej krzywej.

Zapisując równanie 1.1 w postaci rzutowej

$$E : y^2 z = x^3 + Axz^2 + Bz^3,$$

gdzie trójki $[x, y, z]$ oznaczają współrzędne jednorodne (tzn. $[x, y, z] \sim [\lambda x, \lambda y, \lambda z]$ dla dowolnego $\lambda \in K^\times$). Otrzymujemy krzywą rzutową, która ma dokładnie jeden punkt w nieskończoności (tzn. dla $z = 0$). Dla $z = 1$ dostajemy z powrotem krzywą eliptyczną w sensie powyższej definicji. Dla tak określonej krzywej rzutowej definiujemy zbiór

$$E(\mathbb{C}) = \{[x, y, z] \in \mathbb{C}^3 \mid \quad y^2 = x^3 + Ax + B\} \cup \{[0, 1, 0]\}.$$

Najbardziej interesująca będzie dla nas struktura pozdbioru $E(\mathbb{Q}) \subset E(\mathbb{C})$, który zawiera wszystkie rozwiązania równania (1.1) w liczbach wymiernych.

Zadziwiającą własnością zbioru $E(\mathbb{Q})$ jest fakt, że posiada on strukturę grupy abelowej. Działanie dodawania punktów pochodzi od znanej już Diofantosowi metody siecznych (skutecznie wykorzystywanej również przez Fermata). Mając dane dwa punkty wymierne, różne od punktu w nieskończoności $P_1, P_2 \in E(\mathbb{Q})$ prowadzimy przez nie prostą o współczynnikach wymiernych, która przecina krzywą E w trzecim punkcie, o współrzędnych wymiernych. Tak określony punkt R będzie elementem przeciwnym do punktu $P_1 +_E P_2$. Elementem neutralnym działania $+_E$ jest punkt w nieskończoności $\mathcal{O} = [0, 1, 0]$. Ponadto element przeciwny wyznacza się w ten sposób, że jeśli dany jest punkt $Q = [x, y, 1]$, to przeciwny do niego $-Q := [x, -y, 1]$. Szczegółowy opis prawa dodawania (w pozostałych przypadkach, gdy poszczególne punkty są parami równe) zostanie przedstawiony w Przykładzie 4.2.31.

Pionierami badań nad strukturą grupy $E(\mathbb{Q})$ byli H. Poincaré i B. Levi. Beppo Levi zdołał ustalić jak wygląda struktura punktów skończonego rzędu w grupie $E(\mathbb{Q})$ dla różnych wyborów A oraz B, lecz mimo prawie kompletnej listy takich grup, nie udowodnił klasyfikacji w pełnej ogólności. Dopiero w 1977 B. Mazur podał ostateczne rozwiązanie problemu.

Twierdzenie 1.0.2 (Mazur, 1977)**.** *Niech E będzie krzywą eliptyczną nad $\mathbb{Q}$. Grupa wymiernych punktów torsyjnych na krzywej E jest jedną z grup postaci:*

$$\mathbb{Z}/n\mathbb{Z}$$

dla $1 \leq n \leq 10$ albo $n = 12$, albo:

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$$

dla $1 \leq n \leq 4$.

Sformułowana przez B. Leviego hipoteza, że grupa $E(\mathbb{Q})$ jest skończenie generowana, została udowodniona w 1922 roku przez L. Mordella.

Twierdzenie 1.0.3 (Mordell, 1922)**.** *Niech E będzie krzywą eliptyczną nad ciałem $\mathbb{Q}$. Wówczas grupa punktów wymiernych $E(\mathbb{Q})$ wraz z punktem w nieskończoności jest skończenie generowaną grupą abelową.*

Znalezienie efektywnej metody obliczania generatorów grupy $E(\mathbb{Q})$ stało się centralnym tematem teorii krzywych eliptycznych. Do dziś nie jest znane ogólne rozwiązanie tego problemu. Aktualny rekord rangi grupy $E(\mathbb{Q})$ wynosi 28 (patrz Przykłady: równanie (3.9)).

Istnienie efektywnego algorytmu wyznaczającego grupę punktów torsyjnych $E(\mathbb{Q})_{\text{tors}}$ gwarantuje następujące twierdzenie.

Twierdzenie 1.0.4 (Nagell,1935;Lutz,1937)**.** *Niech dana będzie krzywa eliptyczna $E : y^2 = x^3+Ax+B$ nad $\mathbb{Q}$. Niech $P = (x, y)$ będzie punktem torsyjnym niezerowym na krzywej E, tzn. $P \neq \mathcal{O}$. Wówczas albo $2P = \mathcal{O}$, albo*

$$y^2 \mid 4A^3 + 27B^2.$$

Przykład 1.0.5. Niech dana będzie krzywa eliptyczna

$$E : y^2 = x^3 + 9.$$

Wówczas struktura grupy punktów wymiernych jest następująca:

$$E(\mathbb{Q})_{tors} = \{(\mathcal{O}, (0, 3), (0, -3)\},$$

$$E(\mathbb{Q}) = E(\mathbb{Q})_{tors} \oplus \langle(-2, 1)\rangle,$$

gdzie $\langle(-2, 1)\rangle$ jest podgrupą generowaną przez punkt nieskończonego rzędu $(-2, 1)$.

Uogólnienie Twierdzenia 1.0.3 zostało przeprowadzone przez A. Weila (These de doctorat, 1928). Twierdzenie w ogólności stosuje się do rozmaitości abelowych nad ciałami liczbowymi.

Definicja 1.0.6 (Rozmaitość abelowa)**.** Grupę algebraiczną (patrz Definicja 4.1.21) określoną nad ciałem k, która jest rozmaitością rzutową, nazywamy **rozmaitością abelowa** zdefiniowaną nad k.

Przypadek udowodniony przez Weila obejmował również szczególną klasę rozmaitości abelowych - jakobiany krzywych algebraicznych. Posłużymy się tutaj konstrukcją jakobianu krzywej określonej nad ciałem liczb zespolonych $\mathbb{C}$.

Przykład 1.0.7 (Konstrukcja jakobianu)**.** Niech dana będzie zwarta powierzchnia Riemanna X (równoważnie gładka algebraiczna krzywa rzutowa nad $\mathbb{C}$). Przez $H_1(X, \mathbb{Z})$ będziemy oznaczali pierwszą grupę homologii powierzchni X. Jest ona równa ilorazowi grupy wszystkich zamkniętych łańcuchów przez podgrupę brzegów (inaczej można powiedzieć, że jest to po prostu abelianizacja grupy podstawowej $\pi_1(X)$). Zwarta powierzchnia Riemanna jest orientowalna, więc z klasyfikacji powierzchni zwartych dostajemy, że jest homeomorficzna z

sumą spójną g torusów. W szczególności grupa $H_1(X,\mathbb{Z})$ jest abelowa i wolna rangi $2g$. Przestrzeń liniowa $\Omega^1(X)$ holomorficznych form różniczkowych na X ma wymiar g. Określamy homomorfizm

$$\Phi : H_1(X,\mathbb{Z}) \to \mathbb{C}^g$$

wzorem

$$\Phi : \gamma \mapsto \left(\int_\gamma \omega_1, \ldots, \int_\gamma \omega_g \right),$$

gdzie ω_i tworzą bazę w $\Omega^1(X)$. Obraz homomorfizmu Φ jest kratą w $\mathbb{C}^g$ (jako podgrupa dyskretna).Zastosowanie twierdzenia Stokesa oraz fakt, że wszystkie 1-formy holomorficzne na zwartej powierzchni Riemanna są zamknięte gwarantuje nam, że odwzorowanie Φ jest poprawnie określone.

Jakobianem zwartej powierzchni Riemanna X nazywamy wówczas grupę ilorazową

$$J(X) = \mathbb{C}^g / \Phi(H_1(X,\mathbb{Z})),$$

która jest jednocześnie zespolonym torsuem (topologicznie izomorficznym z $(\mathbb{R}/\mathbb{Z})^{2g}$).

Udowodnione przez S. Lefschetza twierdzenie orzeka, że $J(X)$ jest rozmaitością algebraiczną rzutową nad $\mathbb{C}$. Ponadto indukowane z $\mathbb{C}^g$ dodawanie wektorów czyni na mocy Definicji 1.0.6 z $J(X)$ rozmaitość abelową.

Wybierając dowolnie ustalony punkt $p_0 \in X$ możemy zdefiniować odwzorowanie

$$\Psi : X \to J(X)$$

$$\Psi(p) = \left(\int_{p_0}^{p} \omega_1, \ldots, \int_{p_0}^{p} \omega_g \right),$$

gdzie wektor po prawej stronie jest klasą modulo $\Phi(H_1(X,\mathbb{Z}))$. Odwzorowanie Ψ przedłuża się liniowo do $\Psi : \mathrm{Div}(X) \to J(X)$. Grupa dywizorów $\mathrm{Div}(X)$ jest grupą abelową wolną rozpiętą na wszystkich punktach $p \in X$ (patrz Definicja 4.2.1). Twierdzenie Abela-Jacobiego orzeka, że obcięcie Ψ do grupy dywizorów stopnia zero $\mathrm{Div}^0(X)$ ma jądro będące dywizorami funkcji meromorficznych $\mathrm{DPrinc}(X)$. Otrzymujemy w ten sposób izomorfizm grup

$$\mathrm{Pic}^0(X) = \mathrm{Div}^0(X)/\mathrm{DPrinc}(X) \cong J(X).$$

Dzięki temu elementy rozmaitości abelowej $J(X)$ możemy utożsamiać z formalnymi sumami punktów z $\mathrm{Pic}^0(X)$.

Dla wyżej zdefiniowanych rozmaitości abelowych w Rozdziale 2 udowodnimy następującą ogólną postać twierdzenia o randze.

Twierdzenie 1.0.8 (Mordell-Weil)**.** *Niech A będzie rozmaitością abelową określoną nad ciałem liczbowym K. Wówczas grupa punktów K-wymiernych $A(K)$ rozmaitości A jest skończenie generowaną grupą abelową.*

Przykład 1.0.9 (Schaefer,1995)**.** Niech C będzie gładką krzywą rzutową, której część afiniczna zadana jest równaniem

$$y^2 = x(x-2)(x-3)(x-4)(x-5)(x-7)(x-10).$$

Grupa punktów $\mathbb{Q}$-wymiernych jakobianu krzywej C jest postaci

$$J(C)(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^6 \oplus \mathbb{Z}^2$$

i część wolna jest generowana przez niezależne liniowo punkty (reprezentowane przez klasy dywizorów) $(1,36)-(\infty)$ oraz $(6,24)-(\infty)$. Punkt ∞ reprezentuje jedyny punkt w nieskończoności na krzywej C.

Obliczanie rangi dla rozmaitości abelowych, w szczególności dla krzywych eliptycznych stanowi skomplikowane zadanie, które jest zarówno złożone obliczeniowo jak i teoretycznie. Podejście naiwne, polegające na wyczerpującym poszukiwaniu punktów (przy zadanym równaniu lub układzie równań definiujących rozmaitość) wymiernych ma sens tylko dla punktów o bardzo małej wysokości (skomplikowaniu licznika i mianownika współrzędnych punktów). Dowód twierdzenia Mordella-Weila nie wskazuje efektywnej metody znajdowania rangi.

Arytmetyczny niezmiennik rozmaitości abelowych jakim jest ranga ich grupy punktów wymiernych jest powiązana w dość nieoczekiwany sposób z własnościami pewnego szeregu Dirichleta $L(A,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ stowarzyszonego z rozmaitością abelową A (nazywanego L-funkcją rozmaitości abelowej A). Zazwyczaj szereg taki jest zbieżny w pewnym punkcie absolutnie, a przez to również w pewnej półpłaszczyźnie. Dla krzywych eliptycznych E zostało udowodnione przez A. Wilesa w 1994 roku, że szereg $L(E,s)$ przedłuża się do funkcji analitycznej na całej płaszczyźnie zespolonej.

Ponadto B. Birch i P. Swinnerton-Dyer sformułowali hipotezę (problem millenijny), która orzeka, że jeśli istnieje przedłużenie analityczne L-funkcji stowarzyszonej z krzywą eliptyczną E określoną nad $\mathbb{Q}$ do otoczenia $s = 1$, to zachodzi następująca równość:

$$\mathrm{ord}_{s=1} L(E,s) = \mathrm{ranga}(E(\mathbb{Q})).$$

Ponadto równość można uogólnić do przypadku, gdy dana jest dowolna rozmaitość abelowa nad $\mathbb{Q}$ (patrz Hipoteza 2.5.6).

Godne uwagi wydają się metody, w których konstruuje się jawnie rodziny rozmaitości abelowych (zazwyczaj krzywych eliptycznych), które posiadają z góry określone punkty wymierne nieskończonego rzędu. Dowód metodami geometrycznymi liniowej niezależności wybranych punktów wymiernych jest wówczas centralną częścią twierdzenia. W Rozdziale 3 zaprezentujemy szereg metod szukania rangi krzywych eliptycznych, w szczególności dla pewnej rodziny skonstruowanej przez autora.

Twierdzenie 1.0.10 ([Nas10]). *Niech dana będzie krzywa eliptyczna nad* $\mathbb{Q}$ *postaci:*

$$E_{(u^2-u-3)} : y^2 + (u^2-u-3)xy = x^3 + (u^2-u-3)x^2 - x + 1.$$

Istnieje nieskończony podzbiór $S \subset \mathbb{Q}$ *taki, że jeśli* $u \in S$*, to grupa Mordella-Weila punktów wymiernych* $E_{(u^2-u-3)}(\mathbb{Q})$ *zawiera podgrupę rangi* 4 *rozpiętą przez punkty:*

$$(0,1), (1,1), (u,u+1), \left(\frac{1}{9}, \frac{1}{54}(9+3u-3u^2+v)\right),$$

gdzie punkt (u, v) *leży na krzywej:*

$$2569 + 18u - 9u^2 - 18u^3 + 9u^4 = v^2.$$

Istnieje przekształcenie biwymierne powyższej krzywej do postaci:

$$y_0^2 = x_0^3 - 92835x_0 + 1389150.$$

Grupa punktów $\mathbb{Q}$*-wymiernych powyższej krzywej ma rangę* 2. *Ponadto dla* $u_1, u_2 \in S$, $u_1 \neq u_2$ *krzywe* $E_{(u_1^2-u_1-3)}$ *i* $E_{(u_2^2-u_2-3)}$ *nie są ze sobą izomorficzne nad* $\overline{\mathbb{Q}}$.

Dowód opiera się na zastosowaniu Twierdzenia 3.2.3. Skonstruowana rodzina stanowi też przykład, odpowiadający na pytanie postawione w pracy [BM02] o istnienie rodziny krzywych eliptycznych nad $\mathbb{Q}$ rangi co najmniej 4, takich, że niezależność liniowa punktów nieskończonego rzędu dana jest pewnym warunkiem algebraicznym (patrz Lemat 3.2.6).

Przegląd pracy

W Rozdziale 2 będziemy szczegółowo rozważać pojęcie wysokości punktów na rozmaitościach algebraicznych (Podrozdział 2.1). Konstrukcja wysokości stowarzyszonej z dowolnym dywizorem na rozmaitości jest przedstawiona w dowodzie Twierdzenia 2.1.18. Specjalizujemy następnie ogólną sytuację do przypadku rozmaitości abelowych. Kluczową własnością dla dowodu Twierdzenia Mordella-Weila jest związek wysokości na rozmaitościach abelowych z działaniem grupowym (patrz Wniosek 2.1.19). Prowadzi to do konstrukcji wysokości kanonicznej, która jest funkcją o szczególnie pożądanych własnościach (patrz Twierdzenie 2.1.23). Istnienie wysokości kanonicznej dla rozmaitości abelowej pozwala skonstruować iloczynem skalarny w przestrzeni liniowej $A(\overline{K}) \otimes_{\mathbb{Z}} \mathbb{R}$ dla K - ciała liczbowego (Twierdzenie 2.1.31). W konsekwencji wysokość kanoniczna jest dodatnio określoną formą kwadratową na przestrzeni $A(\overline{K}) \otimes_{\mathbb{Z}} \mathbb{R}$, która ze zdefiniowanym na niej iloczynem skalarnym staje się przestrzenią euklidesową.

W Pozdrozdziale 2.2 najważniejszym wynikiem jest Twierdzenie 2.2.1. Jego dowód jest prostą konsekwencją Twierdzenia 2.2.3 i zastosowania własności wysokości kanonicznej rozwiniętych w Pozdrozdziale 2.1. Dowód Twierdzenia 2.2.3 składa się z dwóch odrębnych cześci. Pierwsza z nich to zastosowanie teorii Kummera rozszerzeń abelowych Galois (Twierdzenie 2.2.7) do szczególnego rozszerzenia $L = K(\{[m]^{-1}(x) : x \in A(K)\})$ pochodzącego od brania współrzędnych punktów na rozmaitości abelowej, których ustalone wielokrotności są punktami wymiernymi. Druga cześć dowodu polega na pokazaniu, że rozszerzenie L/K jest nierozgałęzione (Definicja 2.2.24) poza skończonym zbiorem miejsc, dzielących m oraz miejsca złej redukcji rozmaitości abelowej A (Definicja 2.2.9). Ostatecznym krokiem jest zastosowanie Wniosku 2.2.27 dotyczącego maksymalnych abelowych rozszerzeń nierozgałęzionych.

W Podrozdziale 2.3 przedstawiony zostanie szkic dowodu uogólnienia Twierdzenia Mordella-Weila na przypadek ciał skończenie generowanych.

Następnie omówiona jest konstrukcja grupy Szafarewicza-Tate'a i grupy Selmera, które pozwalają zdefiniować przeszkodę (w postaci grupy Ш) do efektywnego znajdowania rangi rozmaitości abelowych. Paragraf o przestrzeniach

jednorodnych jest wstępem do części algorytmicznej przedstawionej w Rozdziale 3.

Pozdrozdział 2.5 poświęcony jest szczegółowemu omówieniu hipotezy Birch-Swinnertona-Dyera w wersji dla rozmaitości abelowych nad $\mathbb{Q}$ (patrz Hipoteza 2.5.6). Przypadek krzywych eliptycznych jest przedstawiony ze szczegółami, ze względu na udowodnione przez A. Wilesa, R.Taylora, C. Breuila, F. Diamonda i B. Conrada twierdzenie o przedłużaniu L-funkcji krzywej eliptycznej nad $\mathbb{Q}$ do funkcji analitycznej na $\mathbb{C}$. Za pomocą formuł analitycznych (patrz Twierdzenie 2.5.7) można obliczać wartość L-funkcji w jedynce i w konswekwencji weryfikować numerycznie hipotezę BSD w wielu konkretnych przypadkach. Paragraf kończy się informacją o udowodnionych przypadkach hipotezy BSD dla krzywych eliptycznych.

Rozdział 3 poświęcony jest obliczaniu rangi grupy punktów wymiernych krzywych eliptycznych nad ciałami liczbowymi jak i funkcyjnymi (ostatni przykład). Podrozdział 3.1 poświęcony jest wykorzystaniu pojęcia przestrzeni jednorodnych do konstrukcji równań diofantycznych, których rozwiązanie gwarantuje istnienie punktów nieskończonego rzędu na krzywej. Co więcej, spadek metodą 2-izogenii jest zalążkiem metody numerycznego obliczania rangi (zaimplementowanej np. w programie **mwrank** J. Cremony). Ogólny algorytm przedstawiony w Twierdzeniu 3.1.1 jest następnie zilustrowany analizą przypadku krzywej eliptycznej o równaniu

$$E : y^2 = x^3 + 11x^2 + 17x,$$

dla której zachodzi równość $E(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

W Podrozdziale 3.2 zaprezentowane są trzy przykłady rodzin krzywych eliptycznych, dla których obliczana jest ranga grupy punktów wymiernych (co najmniej dolne ograniczenie) zupełnie odrębnymi technikami.

Pierwszy przykład rodziny

$$E_t : y^2 + txy = x^3 + tx^2 - x + 1$$

parametryzowanej przez liczby wymierne $t \in \mathbb{Q}$ pochodzi od autora pracy (i jest skrótem z pracy [Nas10]), przedstawiającej konstrukcję nieskończonej rodziny krzywych eliptycznych nad $\mathbb{Q}$, parami nieizomorficznych, których ranga wynosi co najmniej cztery.

Drugi przykład stanowi konstrukcja J.-F. Mestre, która pozwala konstruować rodziny krzywych eliptycznych nad $\mathbb{Q}(t)$ rangi co najmniej 11, gdzie t jest zmienną (patrz Twierdzenie 3.2.9).

Ostatni przykład pochodzący od D. Ulmera ([Ulm10]) pokazuje, że dla krzywych eliptycznych nad ciałem $\mathbb{F}_p(t)$ istnieje nieskończona rodzina rozszerzeń

$$K_d := \mathbb{F}_p(t)(\mu_d, t^{1/d}),$$

dla których ranga grupy punktów K_d-wymiernych rośnie nieograniczenie wraz ze wzrostem parametru d. Stanowi to jaskrawy przykład różnicy "technologicznej" jaka dzieli przypadek ciał liczbowych (krzywe eliptyczne nad $\mathbb{Q}$ rangi co najwyżej 28 - por. równanie (3.9) w Rozdziale 3).

Ostatni rozdział pracy zawiera zebrane wyniki z geometrii algebraicznej i algebry, które są wykorzystywane w pozostałych rozdziałach.

2

Twierdzenie Mordella-Weila

W tym rozdziale udowodnimy podstawowe twierdzenie arytmetyki rozmaitości abelowych zdefiniowanych nad ciałami liczbowymi.

2.1 Teoria wysokości

Wprowadzimy szereg narzędzi, które umożliwiają mierzenie stopnia "skomplikowania" punktów na rozmaitościach algebraicznych. Skonstruowana do tego celu funkcja wysokości posiada szereg ważnych własności, które wiążą zarówno własności geometryczne jak i arytmeczne danej rozmaitości. Ponadto w przypadku rozmaitości ze strukturą grupową istnieje związek pomiędzy wysokością, a działaniem grupowym zdefiniowanym na rozmaitości. Szczególnie ważna będzie własność, która umożliwi późniejszy dowód twierdzenia Mordella-Weila, tj. własność skończoności zbioru punktów o ograniczonej wysokości (tzw. własność Northcotta).

Rozwinięta poniżej teoria wysokości będzie dotyczyła punktów na rozmaitościach, których współrzędne leżą w ustalonym z góry domknięciu algebraicznym ciała liczb wymiernych $\mathbb{Q}$.

Na ciele liczb wymiernych $\mathbb{Q}$ wprowadzamy funkcję dla ustalonej liczby pierwszej p:

$$\mathrm{ord}_p : \mathbb{Q} \to \mathbb{Z} \tag{2.1}$$

spełniającą $\mathrm{ord}_p(0) = +\infty$ oraz dla $x \in \mathbb{Q}^\times$:

$$p^{\mathrm{ord}_p(x)} \frac{a}{b},$$

gdzie $a, b \in \mathbb{Z}$ i $p \nmid ab$. Zachodzi następujące twierdzenie:

Twierdzenie 2.1.1 (Ostrowski)**.** *Na ciele liczb wymiernych możemy zdefiniować normy (patrz Definicja 4.1.3) wyłącznie trzech poniższych typów.*

(1) Norma trywialna $|x|_0 = \begin{cases} 0 & x = 0 \\ 1 & x \neq 0 \end{cases}$.

(2) Norma archimedesowa $|x|_\infty = \max\{x, -x\}$.

(3) Norma p-adyczna $|x|_p = p^{-ord_p(x)}$*, gdzie p jest liczbą pierwszą.*

Definiujemy zbiór $M_{\mathbb{Q}}$, który składa się ze wszystkich nietrywialnych norm na $\mathbb{Q}$. Ogólniej dla ciała liczbowego $K/\mathbb{Q}$ definiujemy zbiór $M_K = M_K^\infty \cup M_K^0$, gdzie M_K^∞ to zbiór norm, których zawężenie do $\mathbb{Q}$ jest normą archimedesowską, a M_K^0 składa się z norm, których zawężenia do $\mathbb{Q}$ są normami p-adycznymi.

Ponadto jeśli K'/K jest rozszerzeniem ciał liczbowych i $v \in M_{K'}$ oraz $w \in M_K$ to mówimy, że v **dzieli** w i piszemy $v|w$ jeśli w jest zawężeniem normy v do K.

Z zasadniczego twierdzenia arytmetyki wynika następujący wzór dla ciała liczb wymiernych (tzw. formuła iloczynowa):

$$\prod_{v \in M_{\mathbb{Q}}} |x|_v = 1 \text{ dla } x \in \mathbb{Q}^\times. \tag{2.2}$$

Definicja 2.1.2 (Uzupełnienie ciała liczbowego)**.** Dla ciała liczbowego K oraz normy $v \in M_K$ definiujemy uzupełnienie ciała K względem normy v i oznaczamy K_v.

Lemat 2.1.3. *Niech K'/K będzie rozszerzeniem ciał liczbowych i $v \in M_K$ będzie normą. Wówczas zachodzi wzór:*

$$\sum_{\substack{w \in M_{K'} \\ w|v}} [K'_w : K_w] = [K' : K].$$

Definicja 2.1.4. Niech $v \in M_K$ będzie normą ciała liczbowego K. **Stopniem lokalnym** n_v normy v nazywać będziemy liczbę:

$$n_v = [K_v : \mathbb{Q}_v],$$

gdzie $\mathbb{Q}_v$ jest uzupełnieniem ciała $\mathbb{Q}$ względem obcięcia normy v do $\mathbb{Q}$. Ponadto **standardową normą** stowarzyszoną z v nazywamy funkcję:

$$||x||_v = |x|_v^{n_v}.$$

Lemat 2.1.5 (Formuła iloczynowa)**.** *Niech K będzie ciałem liczbowym i $x \in K^\times$. Wówczas*

$$\prod_{v \in M_K} ||x||_v = 1$$

Dowód. Z [Lan70, II,Cor.1.2] wynika, że jeśli $x \in K^\times$ i $v \in M_{\mathbb{Q}}$ to

$$\prod_{\substack{w \in M_K \\ w|v}} ||x||_w = |N_{K/\mathbb{Q}}(x)|_v.$$

Zatem

$$\prod_{w \in M_K} ||x||_w = \prod_{v \in M_{\mathbb{Q}}} \prod_{\substack{w \in M_K \\ w|v}} ||x||_w = \prod_{v \in M_{\mathbb{Q}}} |N_{K/\mathbb{Q}}(x)|_v = 1,$$

gdzie ostatnia równość wynika z formuły iloczynowej dla $\mathbb{Q}$. □

Definicja 2.1.6 (Pierścień liczb S-całkowitych ciała liczbowego)**.** Niech $S \subset M_K$ będzie pewnym podzbiorem norm ciała liczbowego K takim, że $M_K^\infty \subset S$. Wówczas zbiór:

$$\mathcal{O}_{K,S} = \{x \in K : |x|_v \leq 1 \text{ dla } v \in M_K \backslash S\}$$

nazywamy **pierścieniem liczb S-całkowitych** ciała liczbowego K. W szczególności jeśli $S = M_K^\infty$, to pierścień $\mathcal{O}_K := \mathcal{O}_{K,S}$ nazywamy **pierścieniem liczb całkowitych** ciała liczbowego K.

Wysokości na przestrzeni rzutowej

Ustalamy schemat (patrz Definicje 4.1.6 i 4.1.16) $\mathbb{P}^n_{\overline{\mathbb{Q}}}$ (oznaczany od tej pory $\mathbb{P}^n$). Jego punkty domknięte odpowiadają ideałom maksymalnym

$$(\alpha_j T_i - \alpha_i T_j)_{0 \leq i,j \leq n}.$$

Elementy α_i należą do $\overline{\mathbb{Q}}$. Każdy taki punkt można reprezentować za pomocą współrzędnych jednorodnych

$$(\alpha_0, \ldots, \alpha_n)$$

z relacją równoważności $(\lambda\alpha_0, \ldots, \lambda\alpha_n) \sim (\alpha_0, \ldots, \alpha_n)$ dla dowolnego $\lambda \in \overline{\mathbb{Q}}^\times$. Będziemy pisali, że punkt $P \in \mathbb{P}^n(K)$, gdy istnieją współrzędne jednorodne, w których $P = (\alpha_0, \ldots, \alpha_n)$ i $\alpha_i \in K \subseteq \overline{\mathbb{Q}}$.

Uwaga 2.1.7. Symbol $\mathbb{P}^n(K)$ nie oznacza zbioru $\mathrm{Spec}(K)$-punktów schematu $\mathbb{P}^n_{\overline{\mathbb{Q}}}$ (jest to tylko prawdziwe dla $K = \overline{\mathbb{Q}}$).

Ponadto od tej pory wszystkie rozważane punkty na schematach będą punktami domkniętymi (o ile jasno nie będzie powiedziane, że jest inaczej).

W poniższym paragrafie wprowadzimy funkcję wysokości stowarzyszoną z przestrzenią rzutową $\mathbb{P}^n$. Konstrukcja przebiega w dwóch krokach. Najpierw zdefiniujemy wysokość dla punktów o współrzędnych z ustalonego ciała liczbowego, a następnie poprzez odpowiednie skalowanie wysokości względem stopnia rozszerzenia zdefiniujemy funkcję dla punktów o współrzędnych w $\overline{\mathbb{Q}}$.

Niech dane będzie ciało liczbowe K. Określmy dla układu liczb $x_i \in K$ funkcję

$$H_K(x_0, \ldots, x_n) = \prod_{v \in M_K} \max\left\{||x_0||_v, \ldots, ||x_n||_v\right\}, \tag{2.3}$$

gdzie M_K jest zbiorem nietrywialnych norm ciała K i $||\cdot||_v$ będzie standardową normą stowarzyszoną z v. Wówczas zachodzi

Stwierdzenie 2.1.8. *Niech K będzie ciałem liczbowym, a $P \in \mathbb{P}^n(K)$. Wówczas funkcja*

$$H_K : \mathbb{P}^n(K) \to \mathbb{R}$$

określona wzorem (2.3) nie zależy od reprezentacji punktu P we współrzędnych z K.

Dowód. Niech $P = (x_0, \ldots, x_n) \in \mathbb{P}^n(K)$. Wówczas dla ustalonego $\lambda \in K$

$$H_K(\lambda P) = \prod_{v \in M_K} ||\lambda||_v \prod_{v \in M_K} \max\left\{||x_0||_v, \ldots, ||x_n||_v\right\} = H_K(P)$$

ze względu na wzór iloczynowy z Lematu (2.1.5). □

Definicja 2.1.9. Niech dane będzie ciało liczbowe K oraz punkt $P = (x_0, \ldots, x_n) \in \mathbb{P}^n(K)$. Wysokością punktu stowarzyszoną z K nazywamy liczbę

$$H_K(P) = \prod_{v \in M_K} \max\{||x_0||_v, \ldots, ||x_n||_v\}.$$

Ponadto przez **wysokość** elementu $x \in K$ będziemy rozumieli wysokość punktu $(x, 1) \in \mathbb{P}^1(K)$.

Lemat 2.1.10. *Niech K będzie ciałem liczbowym, a $P \in \mathbb{P}^n(K)$ punktem w przestrzeni rzutowej. Wówczas*

(i) $H_K(P) \geq 1$

(ii) Jeśli K'/K jest skończonym rozszerzeniem ciała K, to

$$H_{K'}(P) = H_K(P)^{[K':K]}$$

Dowód. (i) Zauważmy, że skoro na mocy Stwierdzenia 2.1.8 wartość $H_K(P)$ nie zależy od reprezentacji punktu P w przestrzeni rzutowej, to możemy wybrać taką reprezentację, w której na pewnej współrzędnej (bez utraty ogólności można przyjąć, że na pierwszej) jest 1. Wówczas dla każego $v \in M_K^0$

$$\max\{||1||_v, ||x_1||_v, \ldots, ||x_n||_v\} = 1$$

oraz dla $v \in M_K^\infty$

$$\max\{||1||_v, ||x_1||_v, \ldots, ||x_n||_v\} \geq 1.$$

Iloczyn powyższych składników po wszystkich $v \in M_K$ daje $H_K(P) \geq 1$.

(ii) Jeśli K'/K jest skończonym rozszerzeniem, to mamy

$$\begin{aligned} H_{K'}(P) &= \prod_{w \in M_{K'}} \max\{||x_0||_w, ||x_1||_w, \ldots, ||x_n||_w\} \\ &= \prod_{v \in M_K} \prod_{\substack{w \in M_{K'} \\ w|v}} \max\{||x_0||_w, ||x_1||_w, \ldots, ||x_n||_w\} \\ &= \prod_{v \in M_K} \prod_{\substack{w \in M_{K'} \\ w|v}} \max\{|x_0|_v^{n_w}, |x_1|_v^{n_w}, \ldots, |x_n|_v^{n_w}\}. \end{aligned}$$

Z multiplikatywności stopnia rozszerzeń ciał mamy $n_w = [K'_w : \mathbb{Q}_w] = [K'_w : K_v][K_v : \mathbb{Q}_w] = [K'_w : K_v]n_v$, bo $\mathbb{Q}_w = \mathbb{Q}_v$ (skoro w jest rozszerzeniem normy v). Zatem z powyższej równości i Lematu 2.1.3 dostajemy

$$\begin{aligned} H_{K'}(P) &= \prod_{v \in M_K} \prod_{\substack{w \in M_{K'} \\ w|v}} \max\{||x_0||_v, ||x_1||_v, \ldots, ||x_n||_v\}^{[K'_w:K_v]} \\ &= \prod_{v \in M_K} \max\{||x_0||_v, ||x_1||_v, \ldots, ||x_n||_v\}^{[K':K]} \\ &= H_K(P)^{[K':K]} \end{aligned}$$

□

Ostatni lemat pozwala skonstruować wysokość punktów w przestrzeni rzutowej niezależną od ciała definicji współrzędnych punktu.

Definicja 2.1.11 (Wysokość absolutna)**.** Funkcję $H : \mathbb{P}^n(\overline{\mathbb{Q}}) \to [1, +\infty)$ określoną wzorem:

$$H(P) = H_K(P)^{\frac{1}{[K:\mathbb{Q}]}},$$

gdzie K jest dowolnym ciałem liczbowym, dla którego $P \in \mathbb{P}^n(K)$ nazywamy **wysokością absolutną** punktu P. Ponadto funkcję $h(P) = \log(H(P))$ nazywamy **logarytmiczną wysokością absolutną**. Lemat 2.1.10 gwarantuje poprawność określenia funkcji H oraz h.

Ponadto przez **wysokość absolutną elementu** $x \in \overline{\mathbb{Q}}$ będziemy rozumieli wysokość absolutną punktu $(x, 1) \in \mathbb{P}^1(\overline{\mathbb{Q}})$.

Zauważmy, że jeśli dany jest automorfizm $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to jego obcięcie do dowolnego ciała liczbowego K wyznacza izomorfizm ciał $\sigma : K \to \sigma(K)$. Automorfizm indukuje bijekcję zbiorów:

$$\sigma : M_K \to M_{\sigma(K)}, \tag{2.4}$$

gdzie $\sigma(v)$ określona jest wzorem $|\sigma(x)|_{\sigma(v)} := |x|_v$ dla dowolnego $x \in K$ i $v \in M_K$. Ponadto σ indukuje izomorfizm uzupełnień $K_v \simeq \sigma(K)_{\sigma(v)}$ oraz równość lokalnych stopni $n_v = n_{\sigma(v)}$.

Lemat 2.1.12. *Niech dany będzie punkt $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$ oraz automorfizm $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. Wówczas*

$$H(\sigma(P)) = H(P).$$

Dowód. Niech $P = (x_0, \ldots, x_n) \in \mathbb{P}^n(K)$ dla pewnego ciała liczbowego K. Na podstawie powyższych rozważań mamy

$$\begin{aligned}
H_{\sigma(K)}(\sigma(P)) &= \prod_{w \in M_{\sigma(K)}} \max\{||\sigma(x_0)||_w, ||\sigma(x_1)||_w, \ldots, ||\sigma(x_n)||_w\} \\
&= \prod_{w \in M_{\sigma(K)}} \max\{|\sigma(x_0)|_w, |\sigma(x_1)|_w, \ldots, |\sigma(x_n)|_w\}^{n_w} \\
&= \prod_{v \in M_K} \max\left\{|\sigma(x_0)|_{\sigma(v)}, |\sigma(x_1)|_{\sigma(v)}, \ldots, |\sigma(x_n)|_{\sigma(v)}\right\}^{n_{\sigma(v)}} \\
&= \prod_{v \in M_K} \max\{|x_0|_v, |x_1|_v, \ldots, |x_n|_v\}^{n_v} \\
&= \prod_{v \in M_K} \max\{||x_0||_v, ||x_1||_v, \ldots, ||x_n||_v\} \\
&= H_K(P).
\end{aligned}$$

Ponadto $[K : \mathbb{Q}] = [\sigma(K) : \mathbb{Q}]$. Zatem

$$H(\sigma(P)) = H_{\sigma(K)}(\sigma(P))^{\frac{1}{[\sigma(K):\mathbb{Q}]}} = H_K(P)^{\frac{1}{[K:\mathbb{Q}]}} = H(P).$$

□

Udowodnimy teraz główne twierdzenie tego paragrafu.

Twierdzenie 2.1.13 ([HS00, Thm.B.2.3]). *Niech $C, d \in \mathbb{Z}_{\geq 0}$ będą ustalonymi liczbami. Wówczas zbiór*

$$\left\{P \in \mathbb{P}^n(\overline{\mathbb{Q}}) \mid H(P) \leq C, [\mathbb{Q}(P) : \mathbb{Q}] \leq d\right\}$$

jest skończony. Ciało $\mathbb{Q}(P) := \mathbb{Q}(\frac{x_0}{x_j}, \ldots, \frac{x_n}{x_j})$ o ile $x_j \neq 0$.

W szczególności jeśli K jest ustalonym ciałem liczbowym to zbiór

$$\{P \in \mathbb{P}^n(K) \mid H_K(P) \leq C\}$$

jest skończony.

Dowód. Niech dany będzie punkt $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$. Wybierzmy dla niego współrzędne $P = (x_0, \ldots, x_n)$ takie, że $x_j = 1$ dla pewnego $0 \leq j \leq n$. Wtedy ciało definicji $\mathbb{Q}(P) = \mathbb{Q}(x_0, \ldots, x_n)$. Dostajemy ponadto oszacowania

$$\max_{0 \leq i \leq n} \{||x_i||_v\} \geq \max\{||x_j||_v, 1\} \, (0 \leq j \leq n)$$

$$\begin{aligned} H_{\mathbb{Q}(P)}(P) &= \prod_{v \in M_{\mathbb{Q}(P)}} \max_{0 \leq i \leq n} \{||x_i||_v\} \\ &\geq \max_{0 \leq j \leq n} \left(\prod_{v \in M_{\mathbb{Q}(P)}} \max\{||x_j||_v, 1\} \right) = \max_{0 \leq j \leq n} H_{\mathbb{Q}(P)}(x_j). \end{aligned}$$

Podnosząc obie strony do potęgi $\frac{1}{[\mathbb{Q}(P):\mathbb{Q}]}$ otrzymujemy

$$H(P) \leq \max_{0 \leq i \leq n} H(x_i).$$

Zatem jeśli $H(P) \leq C$ oraz $[\mathbb{Q}(P) : \mathbb{Q}] \leq d$, to

$$\max_{0 \leq i \leq n} H(x_i) \leq C \text{ oraz } \max_{0 \leq i \leq n} [\mathbb{Q}(x_i) : \mathbb{Q}] \leq d.$$

Wystarczy zatem pokazać skończoność zbioru

$$\left\{x \in \overline{\mathbb{Q}} | H(x) \leq C \text{ i } [\mathbb{Q}(x) : \mathbb{Q}] = d\right\}.$$

Niech $x \in \overline{\mathbb{Q}}$ i $K = \mathbb{Q}(x)$ oraz $[K : \mathbb{Q}] = d$. Wielomian minimalny elementu x jest postaci:

$$f_x(t) = \prod_{i=1}^{d} (t - x_j) = \sum_{r=0}^{d} (-1)^r s_r(x) t^{d-r},$$

gdzie x_j są elementami sprzężonymi z x nad $\mathbb{Q}$. Dla ustalonego $v \in M_K$ możemy oszacować normy elementów $s_r(x)$:

$$\begin{aligned} |s_r(x)|_v &= \left| \sum_{1 \leq i_1 < \ldots < i_r \leq d} x_{i_1} \cdot \ldots \cdot x_{i_r} \right|_v \\ &\leq c(v, r, d) \max_{1 \leq i_1 < \ldots < i_r \leq d} |x_{i_1} \cdot \ldots \cdot x_{i_r}|_v \\ &\leq c(v, r, d) \max_{1 \leq i \leq d} |x_i|_v^r. \end{aligned}$$

Pierwsza nierówność wynika z nierówności trójkąta, a ponadto $c(v,r,d) = \binom{d}{r} < 2^d$ jeśli v jest normą archimedesowską oraz $c(v,r,d) = 1$ jeśli v jest niearchimedesowska. Dostajemy nierówność

$$\max_{0\leq i\leq d}\{|s_i(x)|_v\} \leq c(v,d)\prod_{i=1}^{d}\max\{|x_i|_v,1\}^d,$$

gdzie $c(v,d) = 2^d$ w przypadku, gdy v jest archimedesowa oraz $c(v,d) = 1$, gdy v niearchimedesowa. Mnożąc obie strony nierówności względem wszystkich $v \in M_K$ oraz wyciągając obustronnie pierwiastek stopnia $[K:\mathbb{Q}]$ otrzymujemy oszacowanie wysokości absolutnej:

$$H(s_0(x),\ldots,s_d(x)) \leq 2^d\prod_{i=1}^{d}H(x_i)^d.$$

Z Lematu 2.1.12 wiemy, że $H(x_i) = H(x)$ dla dowolnego i. Stąd

$$H(s_0(x),\ldots,s_d(x)) \leq 2^d H(x)^{d^2}.$$

Z założenia mamy $H(x) \leq C$, więc $H(s_0(x),\ldots,s_d(x)) \leq 2^d C^{d^2}$. Ponadto jeśli $P \in \mathbb{P}^n(\mathbb{Q})$, to możemy przedstawić punkt w postaci $P = (a_0,\ldots,a_n)$, gdzie $a_i \in \mathbb{Z}$ oraz $NWD(a_0,\ldots,a_n) = 1$. Wówczas

$$H_{\mathbb{Q}}(P) = \max\{|a_0|,\ldots,|a_n|\},$$

gdzie $|x| = \max\{x,-x\}$. Istnieje zatem tylko skończenie wiele punktów $P \in \mathbb{P}^n(\mathbb{Q})$ spełniających warunek $H_{\mathbb{Q}}(P) \leq c$ dla ustalonego c. Skoro wielomian $f_x(t) \in \mathbb{Q}[t]$ oraz $H(s_0(x),\ldots,s_d(x)) = H_{\mathbb{Q}}(s_0(x),\ldots,s_d(x))$, to istnieje tylko skończenie wiele możliwych wielomianów minimalnych $f_x(t)$, a zatem skończenie wiele x spełniających $H(x) \leq C$. □

Stwierdzenie 2.1.14. *Niech $S_{n,m}$ będzie zanurzeniem Segre iloczynu $\mathbb{P}^n \times \mathbb{P}^m$ w $\mathbb{P}^N$ dla $N = (n+1)(m+1)-1$:*

$$S_{n,m} : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^N$$

$$S_{n,m} : ((x_0,\ldots,x_n),(y_0,\ldots,y_m)) \to (x_0y_0, x_0x_1,\ldots,x_iy_j,\ldots,x_ny_m).$$

Niech H_n, H_m i H_N będą hiperpłaszczyznami odpowiednio w $\mathbb{P}^n$, $\mathbb{P}^m$ i $\mathbb{P}^N$. Wówczas:

(i) $S^*_{n,m}(H_N) \sim H_n \times \mathbb{P}^m + \mathbb{P}^n \times H_m \in \mathrm{Div}(\mathbb{P}^n \times \mathbb{P}^m)$ *(por. Definicje 4.2.1, 4.2.4).*

(ii) $h(S_{n,m}(x,y)) = h(x) + h(y)$ *dla wszystkich* $x \in \mathbb{P}^n(\overline{\mathbb{Q}})$ *i* $x \in \mathbb{P}^m(\overline{\mathbb{Q}})$.

Niech odwzorowanie $\Phi_d : \mathbb{P}^n \to \mathbb{P}^N$ ($N = \binom{n+d}{n} - 1$) będzie zanurzeniem stopnia d:

$$\Phi(x) = (M_0(x),\ldots,M_N(x)),$$

gdzie $M_i(x)$ jest jednomianem stopnia d zmiennych $x_0,\ldots,x_n$. Wówczas:

$$h(\Phi_d(x)) = dh(x) \text{ dla } x \in \mathbb{P}^n(\overline{\mathbb{Q}}).$$

Dowód. (i) Niech $(z_0, \ldots, z_N)$ będzie punktem w $\mathbb{P}^N$. Wszystkie hiperpłaszczyzny jako dywizory Weila są ze sobą liniowo równoważne (patrz Definicja 4.2.3). Wybierzmy więc ustalone hiperpłaszczyzny $H_N = \{z_0 = 0\}$, $H_n = \{x_0 = 0\}$ i $H_m = \{y_0 = 0\}$. Wówczas mamy

$$\begin{aligned} S^*_{n,m}(H_N) &= S^*_{n,m}\left(\{(z_0, \ldots, z_N) \in \mathbb{P}^N \mid z_0 = 0\}\right) \\ &= \{(x_0, \ldots, x_n, y_0, \ldots, y_m) \in \mathbb{P}^n \times \mathbb{P}^m \mid x_0 y_0 = 0\} \\ &= H_n \times \mathbb{P}^m + \mathbb{P}^n \times H_m. \end{aligned}$$

(ii) Niech $x \in \mathbb{P}^n(K)$ i $y \in \mathbb{P}^m(K)$ dla pewnego ciała liczbowego K. Niech ponadto $z = S_{m,n}(x, y)$. Wówczas dla ustalonej normy $v \in M_K$ mamy

$$\max_{0 \le k \le N} |z_k|_v = \max_{\substack{0 \le i \le n \\ 0 \le j \le m}} |x_i y_j|_v = \left(\max_{0 \le i \le n} |x_i|_v\right)\left(\max_{0 \le j \le m} |y_j|_v\right).$$

Podnosząc do potęgi $\frac{n_v}{[K:\mathbb{Q}]}$ i mnożąc względem wszystkich $v \in M_K$ oraz wyciągając obustronnie logarytm naturalny dostajemy tezę.

(iii) Z założenia mamy $\Phi(x) = (M_0(x), \ldots, M_N(x))$, gdzie $M_i(x)$ jest jednomianem stopnia d zmiennych $x_0, \ldots, x_n$. Zachodzi nierówność:

$$|M_i(x)|_v \le \max_i |x_i|_v^d.$$

Ponadto zbiór $\{M_i(x)\}_{i=1}^N$ zawiera jednomiany $x_0^d, \ldots, x_n^d$, co pociąga równość:

$$\max_{0 \le j \le N} |M_j(x)|_v = \max_{0 \le i \le n} |x_i|_v^d.$$

Podobnie jak w (ii) podnosimy obustronnie do potęgi $\frac{n_v}{[K:\mathbb{Q}]}$ i mnożymy względem wszystkich $v \in M_K$ i wyciągamy obustronnie logarytm, co kończy dowód stwierdzenia. □

Twierdzenie 2.1.15. *Niech $\phi : \mathbb{P}^n \to \mathbb{P}^m$ będzie odwzorowaniem wymiernym stopnia d zdefiniowanym nad $\overline{\mathbb{Q}}$, tzn. $\phi = (f_0, \ldots, f_m)$ i ϕ jest morfizmem na zbiorze $\mathbb{P}^n \backslash Z$, gdzie Z jest zbiorem wspólnych zer jednorodnych wielomianów f_i stopnia d. Wtedy:*

(i) $h(\phi(P)) \le dh(P) + O(1)$ dla dowolnego $P \in \mathbb{P}^n(\overline{\mathbb{Q}}) \backslash Z$.

(ii) Niech X będzie podrozmaitością w $\mathbb{P}^n$ taką, że $X \cap Z = \emptyset$. Wówczas:

$$h(\phi(P)) = dh(P) + O(1)$$

dla dowolnego $P \in X(\overline{\mathbb{Q}})$.

Dowód. Niech K będzie ustalonym ciałem definicji dla ϕ, tzn. jeśli $\phi = (f_0, \ldots, f_m)$, to $f_i \in K[X_0, \ldots, X_n]$ dla wszystkich i. Wielomiany f_i są jednorodne, więc możemy zapisać je w postaci:

$$f_i(X_0, \ldots, X_n) = \sum_{|e|=d} a_{i,e} X^e,$$

gdzie $e = (e_0, \ldots, e_n)$ i $|e| = e_0 + \ldots + e_n$ oraz $X^e = X_0^e \cdot \ldots \cdot X_n^e$. Wprowadzamy następujące pomocnicze oznaczenia:

$$|P|_v = \max\{|x_0|_v, \ldots, |x_n|_v\}$$

dla $P = (x_0, \ldots, x_n)$ oraz $x_j \in K$ i $v \in M_K$. Ponadto jeśli $f = \sum a_e X^e \in K[X_0, \ldots, X_n]$, to $|f|_v = \max_e |a_e|_v$. Nierówność trójkąta możemy zapisać dla dowolnej normy $v \in M_K$ w postaci:

$$|a_1 + a_2 + \ldots + a_k| \leq \epsilon_v(r) \max\{|a_1|_v, \ldots, |a_k|_v\},$$

gdzie:

$$\epsilon_v(r) = \begin{cases} r & \text{dla } v \in M_K^\infty \\ \\ 1 & \text{dla } v \in M_K^0 \end{cases}.$$

Niech $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$ będzie takim punktem, że $P = (x_0, \ldots, x_n)$ i $x_i \in K$ (rozszerzając K w razie potrzeby). Wówczas dla dowolnego $v \in M_K$ zachodzi:

$$\begin{aligned} |f_i(P)|_v &= \left| \sum_{|e|=d} a_{i,e} x^e \right|_v \\ &\leq \epsilon_v(\binom{n+d}{n})(\max_e |a_{i,e}|_v)(\max_e |x_0^{e_0} \cdot \ldots \cdot x_n^{e_n}|_v) \\ &\leq \epsilon_v(\binom{n+d}{n})|f_i|_v \max_{e,j} |x_j|_v^{e_0+\ldots+e_n} \\ &= \epsilon_v(\binom{n+d}{n})|f_i|_v |P|_v^d. \end{aligned}$$

Zauważmy, że nierówność ta nie zależy od wyboru reprezentacji punktu P, ponieważ f_i jest wielomianem jednorodnym stopnia d. Zauważmy, że korzystając z Lematu 2.1.3 dostajemy tożsamość:

$$\prod_{v \in M_K} \epsilon_v(r)^{n_v} = \prod_{v \in M_K^\infty} r^{n_v} = r^{[K:\mathbb{Q}]}.$$

Ponadto definiujemy:

$$H(\phi) = \prod_{v \in M_K} \max_i \{|f_i|_v\}^{\frac{n_v}{[K:\mathbb{Q}]}}.$$

Dostajemy zatem nierówność:

$$H(\phi(P)) \leq \binom{n+d}{n} H(\phi) H(P)^d$$

i logarytmując stronami otrzymamy:

$$h(\phi(P)) \leq dh(P) + h(\phi) + \ln \binom{n+d}{n},$$

co dowodzi (i). Równość (ii) zostanie udowodniona z wykorzystaniem twierdzenia Hilberta o zerach (patrz [Har06, I,Thm.1.3A]). Ustalmy punkt $P \in X$. Z założenia ϕ jest morfizmem na X, zatem istnieją wielomiany jednorodne $p_1, \ldots, p_r$ takie, że $I(X) = (p_1, \ldots, p_r)$ (w sensie [Har06, I,p.10]). Skoro $X \cap Z = \emptyset$, to zbiór wspólnych zer wielomianów $f_0, \ldots, f_m, p_1, \ldots, p_r$ jest pusty. Z twierdzenia Hilberta o zerach wynika, że:

$$(X_0, \ldots, X_n) \subset \sqrt{(f_0, \ldots, f_m, p_1, \ldots, p_r)}.$$

Ideał $(f_0, \ldots, f_m, p_1, \ldots, p_r)$ jest jednorodny, więc istnieją wielomiany jednorodne g_{ij} oraz p_{ij} oraz liczby naturalne dodatnie $\{k_j\}_{j=0}^n$ takie, że:

$$g_{0j}f_0 + \ldots + g_{mj}f_m + q_{1j}p_1 + \ldots + q_{rj}p_r = X_j^{k_j}$$

dla $0 \leq j \leq n$. Niech $t = \max\{d, k_0, \ldots, k_n\}$. Dla każdego j domnażamy obustronnie równania przez $X_j^{\max\{t-k_j,0\}}$ zastępując wielomiany g_{ij} oraz q_{ij} nowymi wielomianami jednorodnymi. Dostajemy zatem:

$$g_{0j}f_0 + \ldots + g_{mj}f_m + q_{1j}p_1 + \ldots + q_{rj}p_r = X_j^t, \tag{2.5}$$

gdzie $t \geq d$ i $0 \leq j \leq n$. Skoro f_i jest jednorodny stopnia d to g_{ij} jest jednorodny stopnia $t-d$. Powiększając w razie potrzeby ciało K o współczynniki wielomianów g_{ij} i q_{ij} możemy przyjąć, że $P \in X(K)$. Skoro $p_i(P) = 0$ dla dowolnego i, to na podstawie równania (2.5) zachodzi:

$$g_{0j}(P)f_0(P) + \ldots + g_{mj}(P)f_m(P) = x_j^t$$

dla dowolnego $0 \leq j \leq n$ i $P = (x_0, \ldots, x_n)$. Z jednorodności wszystkich wielomianów w równości wynika, że równość jest niezależna od reprezentacji punktu P. Mamy zatem:

$$\begin{aligned}
|P|_v^t &= \max_{0\leq j\leq n} |x_j|_v^t \\
&= \max_{0\leq j\leq n} |g_{0j}(P)f_0(P) + \ldots + g_{mj}(P)f_m(P)|_v \\
&\leq \epsilon_v(m+1)\left(\max_{i,j}|g_{i,j}(P)|_v\right)\left(\max_i |f_i(P)|_v\right) \\
&\leq \epsilon_v(m+1)\left[\epsilon_v\binom{t-d+n}{n}\left(\max_{i,j}|g_{i,j}|_v\right)|P|_v^{t-d}\right]\cdot\left(\max_i |f_i(P)|_v\right).
\end{aligned}$$

Podnosząc obustronnie do potęgi $\frac{n_v}{[K:\mathbb{Q}]}$ i mnożąc stronami względem wszystkich $v \in M_K$ dostaniemy:

$$H(P)^t \leq CH(P)^{t-d}H(\phi(P)),$$

gdzie C jest stałą zależną od wielomianów g_{ij} i f_i oraz liczby t (i niezależna od P). Logarytmując jak w (i) stronami dostaniemy:

$$dh(P) \leq h(\phi(P)) + O(1).$$

□

Wysokości na rozmaitościach algebraicznych

W tym paragrafie przedstawimy metodę, która pozwala skonstruować funkcję wysokości stowarzyszoną z pewnym morfizmem $V \to \mathbb{P}^n$.

Definicja 2.1.16. Niech V będzie rozmaitością rzutową zdefiniowaną nad $\overline{\mathbb{Q}}$. Niech $\phi : V \to \mathbb{P}^n$ będzie morfizmem (np. zanurzeniem z domkniętym obrazem). Funkcję:

$$h_\phi : V(\overline{\mathbb{Q}}) \to \mathbb{R}_+,\ h_\phi(P) = h(\phi(P)),$$

gdzie $h(P)$ jest logarytmiczną wysokością absolutną na $\mathbb{P}^n$ będziemy nazywać wysokością stowarzyszoną z morfizmem ϕ.

Twierdzenie 2.1.17. *Niech V będzie gładką, rzutową rozmaitością zdefiniowaną nad $\overline{\mathbb{Q}}$ i niech $\phi : V \to \mathbb{P}^n$ oraz $\psi : V \to \mathbb{P}^m$ będą morfizmami nad $\overline{\mathbb{Q}}$. Niech H będzie hiperpłaszczyzną w $\mathbb{P}^n$, a H' hiperpłaszczyzną w $\mathbb{P}^m$. Jesli ϕ^*H i ψ^*H' są liniowo równoważne, to istnieje stała $O(1) \in \mathbb{R}$ taka, że:*

$$h_\phi(P) = h_\psi(P) + O(1), \text{ dla dowolnego } P \in V(\overline{\mathbb{Q}}).$$

Stała $O(1)$ jest zależna od V oraz ψ i ϕ, ale nie zależy od P.

Dowód. Dla dowolnej hiperpłaszczyzny H zupełny system liniowy $|H|$ (patrz Definicja 4.2.15) nie ma punktów bazowych ([HS00, Ex.A.3.1.3]), ponieważ zawiera wszystkie hiperpłaszczyzny w $\mathbb{P}^n$. Na mocy Twierdzenia 4.2.18 dywizor ϕ^*H nie ma punktów bazowych. Z definicji wynika zatem, że

$$\bigcap_{\substack{D \sim \phi^*H \\ D \geq 0}} \mathrm{Supp}(D) = \emptyset$$

(patrz Definicja 4.2.4). Istnieje zatem dywizor $D \geq 0$ taki, że $D \sim \phi^*H$. Ustalmy zatem $D \in Div(V)$, dywizor dodatni w klasie równoważności $\phi^*H \sim \psi^*H'$. Zauważmy ponadto, że równoważność ta implikuje, że ψ i ϕ są stowarzyszone z tym samym zupełnym systemem liniowym. Dokładniej, jeśli wybierzemy pewną bazę $\{h_i\}_{i=1}^N$, gdzie $N = \dim L(D)$, to istnieją stałe $a_{ij}, b_{ij} \in \overline{\mathbb{Q}}$ takie, że:

$$f_i = \sum_{j=0}^{N} a_{ij} h_j, \ 0 \leq i \leq n, \tag{2.6}$$

$$g_i = \sum_{j=0}^{N} b_{ij} h_j, \ 0 \leq i \leq n \tag{2.7}$$

oraz $\phi = (f_0, \ldots, f_n)$ i $\psi = (g_0, \ldots, g_m)$.

Niech $\lambda = (h_0, \ldots, h_N)$ będzie morfizmem zadanym przez zupełny system liniowy $|D|$. Zdefiniujmy odwzorowanie wymierne $A : \mathbb{P}^N \to \mathbb{P}^n$ zadane jako $A(x_0, \ldots, x_N) = (\sum_{i=0}^N a_{0j}x_j, \ldots, \sum_{i=0}^N a_{nj}x_j)$. Podobnie definiujemy odwzorowanie B stowarzyszone z macierzą (b_{ij}). Ze względu na równości (2.6) i (2.7) dostajmy następujące przemienne diagramy:

$$\begin{array}{ccc} V & \xrightarrow{\lambda} & \mathbb{P}^N \\ & \searrow^{\phi} & \downarrow{\scriptstyle A} \\ & & \mathbb{P}^n \end{array} \qquad \begin{array}{ccc} V & \xrightarrow{\lambda} & \mathbb{P}^N \\ & \searrow^{\psi} & \downarrow{\scriptstyle B} \\ & & \mathbb{P}^m \end{array}$$

Odwzorowania A i B są dobrze określone na obrazie morfizmu λ. Możemy zatem zastosować Twierdzenie 2.1.15 dla $X = \mathrm{im}\lambda$. Dostajemy:

$$h(A(Q)) = h(Q) + C_1$$

dla stałej C_1 niezależnej od Q i dowolnego $Q \in \lambda(V(\overline{\mathbb{Q}}))$. Podobnie:

$$h(B(Q)) = h(Q) + C_2$$

dla pewnej stałej C_2 niezależnej od Q i dowolnego $Q \in \lambda(V(\overline{\mathbb{Q}}))$. Stosując powyższe diagramy przemienne i biorąc punkt $Q = \lambda(P)$, gdzie $P \in V(\overline{\mathbb{Q}})$ dostajemy:

$$\begin{aligned} h(\phi(P)) &= h(A(\lambda(P))) = h(\lambda(P)) + C_1 \\ &= h(B(\lambda(P))) + C_1 - C_2 = h(\psi(P)) + C_1 - C_2, \end{aligned}$$

co kończy dowód twierdzenia. □

Sformułujemy teraz i udowodnimy twierdzenie, które pozwala stowarzyszyć dowolny dywizor Weila na rozmaitości V z pewną funkcją wysokości.

Twierdzenie 2.1.18 ("Maszyna Weila", [HS00, Thm. B.3.2])**.** *Niech K będzie ciałem liczbowym. Wówczas dla ustalonej gładkiej rozmaitości rzutowej V/K istnieje odwzorowanie:*

$$h_V : Div(V) \to \{\text{funkcje } V(\overline{K}) \to \mathbb{R}\}$$

spełniające następujące własności (przyjmujemy oznaczenie $h_{V,D} := h_V(D)$).

(a) (Normalizacja) Niech $H \subset \mathbb{P}^n$ będzie hiperpłaszczyzną. Wówczas istnieje stała $C \in \mathbb{R}$ zależna tylko od H taka, że:

$$h_{\mathbb{P}^n,H}(P) = h(P) + C \text{ dla dowolnego } P \in \mathbb{P}^n(\overline{K}).$$

(b) (Funktorialność) Niech $\phi : V \to W$ będzie morfizmem rozmaitości rzutowych i $D \in Div(W)$ ustalonym dywizorem. Wówczas istnieje stała $C \in \mathbb{R}$ zależna tylko od ϕ i D taka, że:

$$h_{V,\phi^* D}(P) = h_{W,D}(\phi(P)) + C \text{ dla dowolnego } P \in V(\overline{K}).$$

(c) (Addytywność) Niech $D, E \in Div(V)$. Wówczas:

$$h_{V,D+E}(P) = h_{V,D}(P) + h_{V,E}(P) + C \text{ dla dowolnego } P \in V(\overline{K})$$

dla pewnej niezależnej od P stałej $C \in \mathbb{R}$.

(d) (Liniowa równoważność) Niech $D, E \in Div(V)$ będą dywizorami równoważnymi liniowo. Wówczas:

$$h_{V,D}(P) = h_{V,E}(P) + C \text{ dla dowolnego } P \in V(\overline{K})$$

dla pewnej niezależnej od P stałej $C \in \mathbb{R}$.

(e) (Dodatnia określoność) Niech $D \in Div(V)$ będzie efektywnym dywizorem ($D \geq 0$) i niech B będzie zbiorem punktów bazowych zupełnego systemu liniowego $|D|$. Wówczas:

$$h_{V,D}(P) \geq C \text{ dla dowolnego } P \in (V \setminus B)(\overline{K})$$

dla pewnej stałej $C \in \mathbb{R}$ niezależnej od punktu P.

(f) (Własność Northcotta) Niech $D \in Div(V)$ będzie dywizorem szerokim. Wówczas dla dowolnego skończonego rozszerzenia K'/K i dowolnej stałej $B \in \mathbb{R}$, zbiór:

$$\{P \in V(K') | h_{V,D}(P) \leq B\}$$

jest skończony.

Dowód. Niech dany będzie dywizor $D \in \mathrm{Div}(V)$ bez punktów bazowych. Morfizm $\phi_D : V \to \mathbb{P}^n$ jest stowarzyszony z zupełnym systemem liniowym $|D|$ (tzn. dla dowolnej hiperpłaszczyzny H spełnia warunek $\phi^* H \sim D$). Możemy określić dla tak wybranego dywizora funkcję

$$h_{V,D}(P) = h(\phi_D(P))$$

dobrze określoną dla dowolnego $P \in V(\overline{K})$.

Będziemy stosować oznaczenie $f(P) = g(P) + O(1)$ jeśli dwie funkcje będą różnić się o stałą niezależną od P.

Pokażemy najpierw, że skonstruowana funkcja nie zależy od wyboru morfizmu ϕ_D. Przypuśćmy, że $\psi_D : V \to \mathbb{P}^m$ będzie innym morfizmem stowarzyszonym z dywizorem D bez punktów bazowych. Wówczas na mocy Twierdzenia 2.1.17 skoro $\phi_D^* H \sim D \sim \psi_D^* H'$ dla pewnych hiperpłaszczyzn H i H', to zachodzi równość:

$$h(\phi_D(P)) = h(\psi_D(P)) + O(1)$$

dla $P \in V(\overline{K})$.

Korzystając z Twierdzenia 4.2.17 zapisujemy dowolnie wybrany dywizor $D \in \mathrm{Div}(V)$ jako $D_1 - D_2$, różnicę dywizorów bardzo szerokich. Bardzo szeroki dywizor nie ma punktów bazowych, więc możemy zdefiniować funkcję:

$$h_{V,D}(P) = h_{V,D_1}(P) - h_{V,D_2}(P),$$

gdzie $P \in V(\overline{K})$.

(c) *(Addytywność dla dywizorów bez punktów bazowych)*

Niech D oraz E będą dywizorami bez punktów bazowych i niech $\phi_D : V \to \mathbb{P}^n$ oraz $\phi_E : V \to \mathbb{P}^m$ będą morfizmami stowarzyszonymi z zupełnymi systemami liniowymi, odpowiednio $|D|$ i $|E|$. Niech $\phi_D \times \phi_E : V \to \mathbb{P}^n \times \mathbb{P}^m$ będzie iloczynem tych odwzorowań. Wówczas biorąc zanurzenie Segre $S_{n,m} : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^N$, gdzie $N = (n+1)(m+1) - 1$ dostajemy morfizm:

$$\phi_D \otimes \phi_E : V \to \mathbb{P}^N$$

zadany wzorem:

$$\phi_D \otimes \phi_E(P) = S_{n,m}(\phi_D(P), \phi_E(P)).$$

Ze Stwierdzenia 2.1.14 dostajemy:

$$(\phi_D \otimes \phi_E)^* H \sim D + E,$$

gdzie H jest pewną hiperpłaszczyzną. Ponieważ H nie ma punktów bazowych, to korzystając ze Stwierdzenia 4.2.18 otrzymujemy, że $D + E$ nie ma punktów

bazowych. Z dokładnością do stałej wysokość stowarzyszona z $D+E$ nie zależy od wyboru odwzorowania stowarzyszonego z dywizorem, możemy więc napisać:

$$h_{V,D+E}(P) = h((\phi_D \otimes \phi_E)(P)) + O(1)$$

dla $P \in V(\overline{K})$. Zatem:

$$\begin{aligned} h_{V,D+E}(P) &= h((\phi_D \otimes \phi_E)(P)) + O(1) \\ &= h(S_{n,m}(\phi_D(P), \phi_E(P))) + O(1) \\ &= h(\phi_D(P)) + h(\phi_E(P)) + O(1) \\ &= h_{V,D}(P) + h_{V,E}(P) + O(1), \end{aligned}$$

gdzie przedostatnia równość wynika ze Stwierdzenia 2.1.14. Zauważmy, że jeśli dywizor:

$$D = D_1 - D_2 = E_1 - E_2$$

zapiszemy jako różnicę dwóch dywizorów bez punktów bazowych na dwa sposoby, to $D_1 + E_2 = D_2 + E_1$ i korzystając z addytywności dla dywizorów bez punktów bazowych:

$$\begin{aligned} h_{V,D_1} + h_{V,E_2} &= h_{V,D_1+E_2} + O(1) \\ &= h_{V,D_2+E_1} + O(1) \\ &= h_{V,D_2} + h_{V,E_1} + O(1). \end{aligned}$$

W takim razie:

$$h_{V,D_1} - h_{V,D_2} = h_{V,E_1} - h_{V,E_2} + O(1).$$

(c)(Addytywność dla dowolnych dywizorów) Niech $D, E \in \mathrm{Div}(V)$ będą dowolnymi dywizorami. Na podstawie Twierdzenia 4.2.17 możemy zapisać je jako różnice bardzo szerokich dywizorów (zatem bez punktów bazowych)

$$D = D_1 - D_2 \text{ oraz } E = E_1 - E_2.$$

Z tego samego twierdzenia wynika też, że $D_1 + E_1$ oraz $D_2 + E_2$ są bardzo szerokie, więc nie mają punktów bazowych. Zachodzą zatem równości:

$$\begin{aligned} h_{V,D+E} &= h_{V,D_1+E_1} - h_{V,D_2+E_2} + O(1) \\ &= h_{V,D_1} + h_{V,E_1} - h_{V,D_2} - h_{E_2} + O(1) \\ &= (h_{V,D_1} - h_{D_2}) + (h_{V,E_1} - h_{V,E_2}) + O(1) \\ &= h_{V,D} + h_{V,E} + O(1). \end{aligned}$$

(a)(Normalizacja) Wystarczy zauważyć, że $\mathrm{id} : \mathbb{P}^n \to \mathbb{P}^n$ spełnia własność $\mathrm{id}^* H \sim H$ (istotnie zachodzi nawet równość) dla dowolnej hiperpłaszczyzny H w $\mathbb{P}^n$. Zatem id jest stowarzyszona z dywizorem H, czyli:

$$h_{\mathbb{P}^n,H}(P) = h(id(P)) + O(1) = h(P) + O(1).$$

(b)(Funktorialność) Dowolny dywizor $D \in \mathrm{Div}(W)$ zapisujemy jako różnicę $D = D_1 - D_2$ dywizorów bardzo szerokich (czyli również bez punktów bazowych) na podstawie Twierdzenia 4.2.17. Niech ϕ_{D_1} i ϕ_{D_2} będą stowarzyszonymi z nimi morfizmami W w $\mathbb{P}^n$. Jeśli $\phi : V \to W$ jest ustalonym morfizmem rozmaitości rzutowych, to na mocy Stwierdzenia Stwierdzenia 2.1.14

dywizory ϕ^*D_1 i ϕ^*D_2 nie mają punktów bazowych i stowarzyszone są z nimi odwzorowania, odpowiednio $\phi_{D_1} \circ \phi$ oraz $\phi_{D_2} \circ \phi$. Ponadto z addytywności ϕ^* mamy $\phi^*D = \phi^*D_1 - \phi^*D_2$. Stąd równości:

$$\begin{aligned} h_{V,\phi^*D} &= h_{V,\phi^*D_1} - h_{V,\phi^*D_2} + O(1) \\ &= h \circ \phi_{D_1} \circ \phi - h \circ \phi_{D_2} \circ \phi + O(1) \\ &= h_{W,D_1} \circ \phi - h_{W,D_2} \circ \phi + O(1) \\ &= h_{W,D} \circ \phi + O(1). \end{aligned}$$

(d)(Liniowa równoważność) Niech $D \sim E$ będą liniowo równoważnymi dywizorami w $\mathrm{Div}(V)$. Zapisując oba jako różnice bardzo szerokich dywizorów: $D = D_1 - D_2$ oraz $E = E_1 - E_2$, dostajemy równoważność liniową $D_1 + E_2 \sim D_2 + E_1$. Oba dywizory są szerokie i stowarzyszone z nimi morfizmy $\phi_{D_1+E_2}$ oraz $\phi_{D_2+E_1}$ spełniają na mocy Twierdzenia 2.1.17 równość:

$$h(\phi_{D_1+E_2}(P)) = h(\phi_{D_2+E_1}(P)) + O(1)$$

dla dowolnego $P \in V(\overline{K})$. Na mocy addytowności (c):

$$h_{V,D_1} + h_{V,E_2} = h_{V,D_1+E_2} + O(1) = h_{V,D_2+E_1} + O(1) = h_{V,D_2} + h_{V,E_1} + O(1).$$

Zatem:

$$h_{V,D} = h_{V,D_1} - h_{V,D_2} + O(1) = h_{V,E_1} - h_{V,E_2} + O(1) = h_{V,E} + O(1).$$

(e)(Dodatnia określoność) Niech $D \geq 0$ (czyli $D = \sum n_Y Y$ i $n_Y \geq 0$) i zapiszmy $D = D_1 - D_2$ jako różnicę dywizorów bardzo szerokich. Przestrzeń $L(D_2)$ jest skończenie wymiarowa (bo V jest rozmaitością rzutową), więc możemy wybierać w niej bazę $f_0, \ldots, f_n$ funkcji regularnych na V, które ją rozpinają. Z definicji przestrzeni $L(D_2)$ mamy $D + \mathrm{div}(f_i) \geq 0$ dla wszystkich i, a ponadto:

$$D_1 + \mathrm{div}(f_i) = D + D_2 + \mathrm{div}(f_i) \geq 0,$$

bo D jest efektywnym dywizorem. Niezależne liniowo funkcje f_i należą również do $L(D_1)$, bo $D_1 \geq D_2$. Z twierdzenia Steiniza o bazie możemy uzupełnić zbiór $\{f_i\}_{i=0}^n$ wektorów liniowo niezależnych do bazy $\{f_i\}_{i=0}^m$ $(m \geq n)$ przestrzeni $L(D_1)$. Wybrane bazy określają stowarzyszone z D_1 i D_2 morfizmy:

$$\phi_{D_1} = (f_0, \ldots, f_m) : V \to \mathbb{P}^m,$$

$$\phi_{D_2} = (f_0, \ldots, f_n) : V \to \mathbb{P}^n.$$

Funkcje $f_0, \ldots, f_m$ są regularne we wszystkich punktach poza nośnikiem $\mathrm{Supp}(D_1)$. Zatem dla $P \notin \mathrm{Supp}(D_1)$ mamy:

$$\begin{aligned} h_{V,D}(P) &= h_{V,D_1} - h_{V,D_2}(P) + O(1) \\ &= h(\phi_{D_1}(P)) - h(\phi_{D_2}(P)) + O(1) \\ &= h(f_0(P), \ldots, f_m(P)) - h(f_0(P) \ldots, f_n(P)) + O(1) \\ &\geq O(1). \end{aligned}$$

Łatwo zauważyć, że ostatnia nierówność wynika z następującej:

$$\prod_{v \in M_K} \max_{0 \leq i \leq m} \{||f_i(P)||_v\} \geq \prod_{v \in M_K} \max_{0 \leq i \leq n} \{||f_i(P)||_v\},$$

która wynika z faktu, że $m \geq n$ i maksimum po mniejszym zbiorze jest mniejsze. W takim razie dostaliśmy oszacowanie z tezy dla wszystkich $P \notin \mathrm{Supp}(D_1)$.

Zauważmy, że z Twierdzenia 4.2.17 wynika, że istnieje bardzo szeroki dywizor $H \in \mathrm{Div}(V)$ taki, że $D + H$ jest bardzo szeroki. Wówczas biorąc stowarzyszone z dywizorem zanurzenie $\phi_H : V \hookrightarrow \mathbb{P}^n$ generujemy dywizory $H_i = \phi_H^* \{x_i = 0\}$. Z definicji morfizmu stowarzyszonego z dywizorem H wynika, że $H_i \sim H$. Czyli istnieje $g \in K(V)^*$ takie, że $H_i = H + \mathrm{div}(g)$. Ale wówczas odwzorowanie $L(H_i) \to L(H) : f \mapsto fg$ jest izomorfizmem przestrzeni liniowych. Zatem:

$$\begin{aligned}
|H| &= \{D \in Div(V) : D \geq 0, D \sim H\} \\
&= \{D \in Div(V) : D = H + \mathrm{div}(h), h \in L(H)\} \\
&= \{D \in Div(V) : D = H + \mathrm{div}(fg), f \in L(H_i)\} \\
&= \{D \in Div(V) : D = H + \mathrm{div}(g) + \mathrm{div}(f), f \in L(H_i)\} \\
&= \{D \in Div(V) : D = H_i + \mathrm{div}(f), f \in L(H_i)\} \\
&= |H_i|.
\end{aligned}$$

Skoro dywizor H jest bardzo szeroki, to H_i są bardzo szerokie dla wszystkich i. Ponadto $D+H \sim D+H_i$, zatem $D+H_i$ jest bardzo szeroki i $D = (D+H_i)-H_i$. Ponadto z konstrukcji H_i wynika, że $\mathrm{Supp}(H_0) \cap \ldots \cap \mathrm{Supp}(H_n) = \emptyset$. W takim razie zachodzi nierówność $h_{V,D}(P) \geq O(1)$ dla wszystkich punktów P poza nośnikiem D (jeśli $P \notin \mathrm{Supp}(D)$, to istnieje $P \notin \mathrm{Supp}(H_i)$ dla pewnego i oraz $P \notin \mathrm{Supp}(D + H_i)$ i korzystamy z podanego wyżej rozkładu D i wcześniejszych obliczeń). Ponadto zauważmy, że nośnik dywizora $D \in \mathrm{Div}(V)$ jest zbiorem domkniętym. Baza $B(|D|) = \bigcap_{D' \in |D|} \mathrm{Supp}(D')$ zupełnego systemu liniowego $|D|$ jest zbiorem domkniętym. Istnieje zatem skończony zbiór dywizorów $\{D_1, \ldots, D_s\} \in |D|$ taki, że $B(|D|) = \bigcap_{i=1}^{s} \mathrm{Supp}(D_i)$. Ponadto $h_{V,D} = h_{V,D_i} + O(1)$ i jeśli $P \in \mathrm{Supp}(D)$, ale $P \notin B(|D|)$, to istnieje i takie, że $P \notin \mathrm{Supp}(D_i)$. Zachodzi zatem wzór:

$$h_{V,D}(P) \geq O(1)$$

dla dowolnego $P \in (V \setminus B(|D|))(\overline{K})$.

(f) Niech dany będzie dywizor szeroki $D \in \mathrm{Div}(V)$. Wówczas istnieje liczba naturalna m taka, że mD jest bardzo szeroki. Wówczas z addytowności:

$$h_{V,mD} = m h_{V,D} + C$$

dla pewnej stałej C niezależnej od $P \in V(\overline{K})$. Otrzymujemy równoważność:

$$h_{V,mD}(P) \leq B \Leftrightarrow h_{V,D}(P) \leq \frac{B - C}{m}.$$

Wystarczy zatem udowodnić nierówność dla dywizorów bardzo szerokich. Przypuśćmy zatem, że D jest bardzo szeroki i stowarzyszone jest z nim zanurzenie $\phi : V \hookrightarrow \mathbb{P}^n$ i dla dowolnej hiperpłaszczyzny H w $\mathbb{P}^n$ $\phi^* H \sim D$. Z własności (a) i (b) dostajemy:

$$h_{V,D} = h_{V,\phi^* H} = h_{\mathbb{P}^n,H} \circ \phi + O(1) = h \circ \phi + O(1).$$

Wystarczy pokazać, że istnieje skończenie wiele punktów o ograniczonej wysokości w $\mathbb{P}^n(K')$. Ta własnośc wynika z Twierdzenia 2.1.13. □

Wniosek 2.1.19. *Niech A będzie rozmaitością abelową zdefiniowaną nad ciałem liczbowym K oraz niech $D \in Div(A)$ będzie dywizorem na A.*

(i) Niech m będzie liczbą całkowitą, a $P \in A(\overline{K})$, wówczas:

$$h_{A,D}([m]P) = \frac{m^2+m}{2}h_{A,D}(P) + \frac{m^2-m}{2}h_{A,D}(-P) + O(1),$$

gdzie $O(1)$ jest stałą niezależną od P.

W szczególności jeśli $[-1]^*D \sim D$ (D jest dywizorem symetrycznym), to:

$$h_{A,D}([m]P) = m^2 h_{A,D}(P) + O(1).$$

(ii) Jeśli D jest dywizorem symetrycznym, to dla dowolnych dwóch punktów $P, Q \in A(\overline{K})$:

$$h_{A,D}(P+Q) + h_{A,D}(P-Q) = 2h_{A,D}(P) + 2h_{A,D}(Q) + O(1).$$

Dowód. (a)Ze wzoru Mumforda (Twierdzenie 4.2.20) wynika:

$$[m]^*D \sim \frac{m^2+m}{2}D + \frac{m^2-m}{2}[-1]^*D.$$

Korzystając z Twierdzenia 2.1.18 dostajemy równości:

$$\begin{aligned} h_{A,D}([m]P) &\overset{(b)}{=} h_{A,[m]^*D}(P) + O(1) \\ &\overset{(d)}{=} h_{A,\frac{m^2+m}{2}D+\frac{m^2-m}{2}[-1]^*D}(P) + O(1) \\ &\overset{(c)}{=} \frac{m^2+m}{2}h_{A,D}(P) + \frac{m^2-m}{2}h_{A,[-1]^*D}(P) + O(1) \\ &\overset{(b)}{=} \frac{m^2+m}{2}h_{A,D}(P) + \frac{m^2-m}{2}h_{A,D}(-P) + O(1). \end{aligned}$$

Ponadto zauważmy, że jeśli $[-1]^*D \sim D$, to $h_{A,D} \circ [-1] = h_{A,D} + O(1)$ i dostajemy wówczas $h_{A,D}([m]P) = m^2 h_{A,D}(P) + O(1)$.

(b) Rozważmy morfizmy $\sigma, \delta, \pi_1, \pi_2 : A \times A \to A$ zdefiniowane w Twierdzeniu 4.2.22. Wówczas na mocy tego twierdzenia dla dowolnego dywizora $D \in \mathrm{Div}(A)$ zachodzi relacja:

$$\sigma^*D + \delta^*D \sim 2\pi_1^*D + 2\pi_2^*D$$

w grupie $\mathrm{Div}(A \times A)$. Na mocy Twierdzenia 2.1.18 mamy zatem:

$$\begin{aligned} h_{A\times A,\sigma^*D}(P,Q) + h_{A\times A,\delta^*D}(P,Q) &\overset{(c),(d)}{=} 2h_{A\times A,\pi_1^*D}(P,Q) + 2h_{A\times A,\pi_2^*}(P,Q) + O(1), \\ h_{A,D}(\sigma(P+Q)) + h_{A,D}(\delta(P,Q)) &\overset{(b)}{=} 2h_{A,D}(\pi_1(P,Q)) + 2h_{A,D}(\pi_2(P,Q)) + O(1), \\ h_{A,D}(P+Q) + h_{A,D}(P-Q) &= 2h_{A,D}(P) + 2h_{A,D}(Q) + O(1). \end{aligned}$$

□

Wysokość kanoniczna

Skonstruujemy teraz pewną szczególną funkcję wysokości stowarzyszoną z dywizorem. W zastosowaniach do twierdzenia Mordella-Weila najbardziej przydatna będzie konstrukcja dająca wysokość, która będzie formą kwadratową na kracie punktów wymiernych (modulo punkty torsyjne).

Twierdzenie 2.1.20 (Néron, Tate)**.** *Niech V będzie gładką rozmaitością rzutową zdefiniowaną nad ciałem liczbowym K oraz $D \in Div(V)$ pewnym dywizorem. Niech dany będzie $\phi : V \to V$, morfizm taki, że:*

$$\phi^* D \sim \alpha D$$

*dla pewnego $\alpha > 1$ całkowitego. Wówczas istnieje jedyna funkcja (zwana **wysokością kanoniczną** na V) stowarzyszona z morfizmem ϕ i dywizorem D:*

$$\hat{h}_{V,\phi,D} : V(\overline{K}) \to \mathbb{R},$$

spełniająca następujące własności:

(i) $\hat{h}_{V,\phi,D}(P) = h_{V,D}(P) + O(1)$ *dla wszystkich* $P \in V(\overline{K})$.

(ii) $\hat{h}_{V,\phi,D}(\phi(P)) = \alpha \hat{h}_{V,\phi,D}(P)$ *dla wszystkich* $P \in V(\overline{K})$. *Wysokość kanoniczna zależy tylko do klasy liniowej równoważności dywizora D. Ponadto zachodzi wzór:*

$$\hat{h}_{V,\phi,D}(P) = \lim_{n\to\infty} \frac{1}{\alpha^n} h_{V,D}(\phi^n(P)),$$

gdzie $\phi^n = \phi \circ \ldots \circ \phi$.

Dowód. Z własności (b),(c) i (d) Twierdzenia 2.1.18 dostajemy równość:

$$h_{V,D}(\phi(Q)) = \alpha h_{V,D}(Q) + C \tag{2.8}$$

dla wszystkich $Q \in V(\overline{K})$ i pewnej stałej $C \in \mathbb{R}$. Pokażemy teraz, że ciąg $\{a_n(P)\}_{n=1}^{\infty}$ o wyrazie ogólnym:

$$a_n(P) = \frac{1}{\alpha^n} h_{V,D}(\phi^n(P))$$

jest zbieżny (udowodnimy, że jest ciągiem Cauchy'ego). Dla $n \geq m$:

$$\begin{aligned}
&\left| \frac{1}{\alpha^n} h_{V,D}(\phi^n(P)) - \frac{1}{\alpha^m} h_{V,D}(\phi^m(P)) \right| \\
&\qquad = \left| \sum_{i=m+1}^{n} \frac{1}{\alpha^i} \left(h_{V,D}(\phi^i(P)) - \alpha h_{V,D}(\phi^{i-1}(P)) \right) \right| \\
&\qquad \leq \sum_{i=m+1}^{n} \frac{1}{\alpha^i} \left| h_{V,D}(\phi^i(P)) - \alpha h_{V,D}(\phi^{i-1}(P)) \right| \\
&\qquad \leq \sum_{i=m+1}^{n} \frac{1}{\alpha^i} C \\
&\qquad \left(\frac{\alpha^{-m} - \alpha^{-n}}{\alpha - 1} \right) C,
\end{aligned}$$

gdzie ostatnia nierówność wynika ze wzoru (2.8) dla $Q = \phi^{i-1}(P)$, a przedostatnia z nierówności trójkąta. Wybierając dowolny punkt $P \in V(\overline{K})$ i $\epsilon > 0$ zawsze znajdziemy takie $N < n \leq m$, że $|a_n(P) - a_m(P)| < \epsilon$. Skoro ciąg $\{a_n(P)\}_{n=1}^{\infty}$ jest zbieżny to możemy zdefiniować jego granicę:

$$\hat{h}_{V,\phi,D}(P) = \lim_{n\to\infty} \frac{1}{\alpha^n} h_{V,D}(\phi^n(P))$$

dla dowolnego $P \in V(\overline{K})$. Ponadto kładąc w powyższej nierówności $m = 0$ i biorąc granicę przy $n \to \infty$ dostajemy nierówność:

$$\left|\hat{h}_{V,\phi,D}(P) - h_{V,D}(P)\right| \leq \frac{C}{\alpha - 1},$$

co dowodzi podpunktu (i).

(ii) Z definicji wysokości kanonicznej jako granicy mamy:

$$\begin{aligned}\hat{h}_{V,\phi,D}(\phi(P)) &= \lim_{n\to\infty} \frac{1}{\alpha^n} h_{V,D}(\phi^n(\phi(P))) \\ &= \lim_{n\to\infty} \frac{\alpha}{\alpha^{n+1}} h_{V,D}(\phi^{n+1}(P)) \\ &= \alpha \hat{h}_{V,\phi,D}(P).\end{aligned}$$

(Jedyność wysokości kanonicznej) Przypuśćmy, że dla ustalonego dywizora $D \in \mathrm{Div}(V)$ i morfizmu $\phi : V \to V$ spełniających założenia twierdzenia istnieją dwie funkcje $\hat{h}$ i $\hat{h}'$ o własnościach (i) i (ii). Wówczas istnieje stała C taka, że:

$$g(P) = \hat{h}(P) - \hat{h}'(P) = C$$

dla dowolnych $P \in V(\overline{K})$. Z własności (ii) mamy $g \circ \phi = \alpha g$. Iterując dostajemy $g \circ \phi^n = \alpha^n g$. Zatem:

$$|g(P)| = \frac{|g(\phi^n(P))|}{\alpha^n} = \frac{|C|}{\alpha^n} \xrightarrow{n\to\infty} 0.$$

To dowodzi $g(P) = 0$ dla wszystkich P, w szczególności $\hat{h} = \hat{h}'$. □

Wniosek 2.1.21. *Niech V będzie gładką rozmaitością rzutową zdefiniowaną nad ciałem liczbowym K oraz niech dany będzie morfizm $\phi : V \to V$ spełniający dla ustalonych dywizorów D_1, D_2 warunki $\phi^* D_i \sim \alpha D_i$ $(i = 1, 2)$ dla pewnego $\alpha > 1$. Wówczas:*

(i) $\hat{h}_{V,\phi,D_1+D_2} = \hat{h}_{V,\phi,D_1} + \hat{h}_{V,\phi,D_2}$

(ii) Jeśli $D_1 \sim D_2$, to $\hat{h}_{V,\phi,D_1} = \hat{h}_{V,\phi,D_2}$

Dowód. (i) Na mocy Twierdzenia 2.1.20 i addytywności wysokości stowarzyszonej z dywizorem istnieje stała C taka, że:

$$\hat{h}_{V,\phi,D_1+D_2} - (\hat{h}_{V,\phi,D_1} + \hat{h}_{V,\phi,D_2}) = C.$$

Korzystając z własności (ii) Twierdzenia 2.1.20 dostajemy:

$$\hat{h}_{V,\phi,D_1+D_2} - (\hat{h}_{V,\phi,D_1} + \hat{h}_{V,\phi,D_2}) = \frac{C}{\alpha^n}$$

dla dowolnego n. Przechodząc z $n \to \infty$ dostajemy tezę. (ii) Na mocy Twierdzenia 2.1.18 $h_{V,D_1} = h_{V,D_2} + C$ dla pewnej stałej C. Korzystając ponownie z własności (i) Twierdzenia 2.1.20 i argumentując jak w podpunkcie (i) dostajemy tezę. □

Twierdzenie 2.1.22. *Niech $\phi : V \to V$ będzie morfizmem gładkiej rozmaitości rzutowej zdefiniowanej nad ciałem liczbowym K. Niech $D \in \mathrm{Div}(V)$ będzie szerokim dywizorem takim, że $\phi^* D \sim D$ dla pewnego $\alpha > 1$ i niech $\hat{h}_{V,\phi,D}$ będzie stowarzyszoną wysokością kanoniczną. Wówczas $\hat{h}_{V,\phi,D}(P) \geq 0$ dla dowolnego $P \in V(\overline{K})$ oraz:*

$$\hat{h}_{V,\phi,D}(P) = 0 \Leftrightarrow \{P, \phi(P), \ldots, \phi^n(P), \ldots\} \text{ jest zbiorem skończonym.}$$

Dowód. Z definicji dywizora D istnieje taka liczba naturalna $k \in \mathbb{N}$, że kD jest bardzo szeroki, czyli nie ma punktów bazowych, a zatem z konstrukcji w Twierdzeniu 2.1.18 wynika, że $h_{V,kD}(P) \geq 0$ dla wszystkich $P \in V(\overline{K})$. Zatem z definicji wysokości kanonicznej $\hat{h}_{V,\phi,kD}(P) \geq 0$. Wniosek 2.1.21 pociąga równość $\hat{h}_{V,\phi,kD}(P) = k\hat{h}_{V,\phi,D}(P)$, zatem $\hat{h}_{V,\phi,D}(P) \geq 0$.

Udowodnimy teraz równoważność. Niech $P \in V(\overline{K})$. Przypuśćmy, że zbiór $\{P, \phi(P), \ldots, \phi^n(P), \ldots\}$ jest skończony. Wówczas ciąg $\{\phi^n(P)\}_{n=1}^{\infty}$ powtarza się, co pociąga, że ciąg $\{h_{V,D}(\phi^n(P))\}_{n=1}^{\infty}$ jest ograniczony. Z definicji $\hat{h}_{V,\phi,D}(P) = \lim_{n\to\infty} \frac{1}{\alpha^n} h_{V,D}(\phi^n(P)) = 0$.

Z drugiej strony przypuśćmy, że $\hat{h}_{V,\phi,D}(P) = 0$ dla pewnego $P \in V(\overline{K})$. Mamy równość

$$h_{V,D}(\phi^n(P)) = \hat{h}_{V,\phi,D}(\phi^n(P)) + O(1) = \alpha^n \hat{h}_{V,\phi,D}(P) + O(1) = O(1)$$

dla dowolnego $n \geq 1$. Możemy bez utraty ogólności przyjąć, że $P \in V(K)$ oraz D i ϕ są zdefiniowane nad K, zastępując K jego skończonym rozszerzeniem. Wówczas $\phi^n(P) \in V(K)$ dla dowolnego n. Istnieje stała B taka, że:

$$O_\phi(P) = \left\{P, \phi(P), \ldots, \phi^k(P), \ldots\right\} \subset \{Q \in V(K) | h_{V,D}(Q) \leq B\} = O_K(B).$$

Twierdzenie 2.1.18, podpunkt (f) implikuje, że zbiór $O_K(B)$ jest skończony, co pociąga, że zbiór $O_\phi(P)$ jest skończony. □

Twierdzenie 2.1.23 (Néron,Tate)**.** *Niech A będzie rozmaitością abelową zdefiniowaną nad ciałem liczbowym K oraz niech $D \in Div(A)$ będzie dywizorem symetrycznym ($[-1]^* D \sim D$). Wówczas istnieje funkcja:*

$$\hat{h}_{A,D} : A(\overline{K}) \to \mathbb{R},$$

*(nazywana **wysokością kanoniczną na rozmaitości A** względem dywizora D). Spełnia ona następujące warunki:*

(i) $\hat{h}_{A,D}(P) = h_{A,D}(P) + O(1)$ *dla wszystkich $P \in A(\overline{K})$.*

(ii) Dla dowolnej liczby całkowitej $m \in \mathbb{Z}$, zachodzi wzór:

$$\hat{h}_{A,D}([m]P) = m^2 \hat{h}_{A,D}(P)$$

dla wszystkich $P \in A(\overline{K})$

(iii) Zachodzi prawo równoległoboku:

$$\hat{h}_{A,D}(P+Q) + \hat{h}_{A,D}(P-Q) = 2\hat{h}_{A,D}(P) + 2\hat{h}_{A,D}(Q)$$

dla dowolnych $P, Q \in A(\overline{K})$.

(iv) Wysokość kanoniczna $\hat{h}_{A,D} : A(\overline{K}) \to \mathbb{R}$ *jest formą kwadratową nad* $\mathbb{Z}$. *Stowarzyszone z nią odwzorowanie dwuliniowe* $\langle \cdot, \cdot \rangle_D : A(\overline{K}) \times A(\overline{K}) \to \mathbb{R}$ *ma postać:*

$$\langle P, Q \rangle_D = \frac{\hat{h}_{A,D}(P+Q) - \hat{h}_{A,D}(P) - \hat{h}_{A,D}(Q)}{2}.$$

(v) Wysokość kanoniczna $\hat{h}_{A,D}$ *zależy tylko od wyboru dywizora* D *i własności (i) oraz własności (ii) dla dowolnie ustalonej liczby* $m \geq 2$.

Dowód. Niech $\phi = [2]$ oraz $V = A$. Z Twierdzenia 4.2.20 dostajemy $\phi^* D \sim 4D$ i stosując Twierdzenie 2.1.20 możemy skonstruować wysokość kanoniczną stowarzyszoną z morfizmem $\phi = [2]$:

$$\hat{h}_{A,D}(P) = \lim_{n \to \infty} \frac{1}{4^n} h_{A,D}([2^n]P).$$

Ponadto Twierdzenie 2.1.20 implikuje równości $\hat{h}_{A,D} = h_{A,D} + O(1)$ oraz $\hat{h}_{A,D} \circ [2] = 4\hat{h}_{A,D}$. Zatem zachodzą własności (i) i (ii) dla $m = 2$. Z Wniosku 2.1.19 wynika, że wysokość Weila $h_{A,D}$ spełnia własności:

$$h_{A,D}([m]Q) = m^2 h_{A,D}(Q) + C$$

dla stałej C i dowolnego punktu $Q \in A(\overline{K})$. Kładąc $Q = [2]^n P$ i dzieląc obustronnie przez 4^n oraz biorąc granicę przy $n \to \infty$ dostajemy:

$$\begin{aligned} \hat{h}_{A,D}([m]P) &= \lim_{n \to \infty} \frac{1}{4^n} h_{A,D}([2^n m]P) \\ &= \lim_{n \to \infty} \frac{1}{4^n} \left(m^2 h_{A,D}([2^n]P) + C \right) \\ &= m^2 \hat{h}_{A,D}(P). \end{aligned}$$

W celu udowodnienia własności (iii) stosujemy ponownie Wniosek 2.1.19. Zastępujemy P i Q w prawie równoległoboku przez $[2^n]P$ i $[2^n]Q$ odpowiednio, dzielimy przez 4^n i przechodzimy do granicy z $n \to \infty$.

Własność (iv) wynika z (iii) oraz Lematu 4.1.2.

Własność (v) wynika z Twierdzenia 2.1.20, bo $\hat{h}_{A,D}$ jest wysokością kanoniczną względem dowolnego morfizmu $[m] : A \to A$ dla $m \geq 2$. □

Rozszerzanie odwzorowań dwuliniowych

Pokażemy teraz w jaki sposób rozszerzyć formę kwadratową $\hat{h}_{A,D} : A(\overline{K}) \to \mathbb{R}$ do dodatnio określonej formy kwadratowej określonej na przestrzeni liniowej $A(\overline{K}) \otimes_{\mathbb{Z}} \mathbb{R}$.

Będziemy rozważać $\mathbb{Z}$-moduł M, na którym określona jest symetryczna forma dwuliniowa $g : M \times M \to \mathbb{R}$.

Definicja 2.1.24 (Jądro symetrycznej formy dwuliniowej)**.** Niech dana będzie symetryczna forma dwuliniowa $g : M \times M \to L$ o wartościach w $\mathbb{Z}$-module L. Moduł:

$$N = \{x \in M | g(x, y) = 0 \text{ dla dowolnego } y \in M\}$$

nazywamy **jądrem** symetrycznej formy dwuliniowej g.

Forma dwuliniowa g indukuje zatem odwzorowanie dwuliniowe $\overline{g}$ na module ilorazowym $\overline{M} := M/N$:

$$\overline{g} : \overline{M} \to \mathbb{R}$$

$$\overline{g}(\overline{m_1}, \overline{m_1}) = \overline{g(m_1, m_2)}.$$

Zauważmy, że jądro $\overline{g}$ jest zerowe oraz jeśli $\overline{x} \in \overline{M}$ jest elementem torsyjnym, to istnieje naturalne n takie, że $n\overline{x} = \overline{0}$,czyli $nx \in N$. Wówczas:

$$ng(x, y) = g(nx, y) = 0 \text{ dla dowolnego } y \in M,$$

a skoro g przyjmuje wartości w $\mathbb{R}$, to $g(x, y) = 0$ dla dowolnego $y \in M$. Zatem:

$$\overline{g}(\overline{x}, \overline{y}) = 0$$

dla dowolnych $\overline{y} \in \overline{M}$, więc $\overline{x}$ należy do jądra $\overline{g}$, które jest zerowe. Stąd wynika, że część torsyjna modułu $\overline{M}$ jest grupą trywialną (ponadto torsja modułu M zawarta jest w jądrze g).

Odwzorowanie kanoniczne:

$$\phi : \overline{M} \to \overline{M}_{\mathbb{R}} = \overline{M} \otimes_{\mathbb{Z}} \mathbb{R}$$

$$\phi : \overline{m} \mapsto \overline{m} \otimes 1$$

jest injekcją (jeśli $\phi(\overline{m}) = 0$, to $\overline{m}$ jest torsyjny lub $\overline{0}$, ale torsja $\overline{M}$ jest zerowa).

Ponadto możemy nadać modułowi $\overline{M} \otimes_{\mathbb{Z}} \mathbb{R}$ naturalną strukturę przestrzeni liniowej definiując mnożenie przez skalar jako:

$$\alpha \cdot \overline{m} \otimes x = \overline{m} \otimes (\alpha x)$$

i rozszerzając je liniowo na sumy dowolnych elementów postaci $\overline{m} \otimes x$.

Stwierdzenie 2.1.25. *Niech $K \subset \overline{M}$ będzie $\mathbb{Z}$ modułem skończenie generowanym w module beztorsyjnym $\overline{M}$ określonym wyżej. Wówczas obcięcie formy dwuliniowej $\overline{g} : \overline{M} \times \overline{M} \to \mathbb{R}$ do K(który jest automatycznie modułem wolnym z twierdzenia klasyfikacyjnego dla grup abelowych) rozszerza się jednoznacznie do formy dwuliniowej na $K_{\mathbb{R}}$.*

Dowód. Niech $\{e_i\}_{i=1}^n$ będzie bazą wolnego modułu K (odpowiada jej baza liniowa przestrzeni $K_{\mathbb{R}}$ postaci $\{e_i \otimes 1\}_{i=1}^n$). Wówczas definiujemy:

$$g_{ij} := \overline{g}(e_i, e_j).$$

Określamy rozszerzenie:

$$\overline{g}_{\mathbb{R}} \left(\sum_{i=1}^n e_i \otimes x_i, \sum_{j=1}^n e_j \otimes x_j \right) := \sum_{i=1}^n \sum_{j=1}^n x_i x_j g_{ij}.$$

Odwzorowanie $\overline{g}_{\mathbb{R}}$ jest symetryczną formą dwuliniową na $K_{\mathbb{R}}$ oraz jeśli utożsamimy obraz $K \to K_{\mathbb{R}} : k \to k \otimes 1$ kanonicznego izomorfizmu z modułem K, to:

$$\overline{g}_{\mathbb{R}}(k \otimes 1, l \otimes 1) = \overline{g}(k, l). \tag{2.9}$$

Ponadto jeśli $h_{\mathbb{R}}$ jest innym rozszerzeniem obcięcia $\overline{g}$ do K spełniającym (2.9), to z liniowości wynika, że $h_{\mathbb{R}} = \overline{g}_{\mathbb{R}}$. □

Niech $\overline{M}'$ będzie skończenie generowanym podmodułem w $\overline{M}$ (jest zatem wolny). Zauważmy, że inkluzja $i : \overline{M}' \to \overline{M}$ indukuje odwzorowanie $i \otimes \mathrm{id} : \overline{M}' \otimes_{\mathbb{Z}} \mathbb{Q} \to \overline{M} \otimes_{\mathbb{Z}} \mathbb{Q}$.

Fakt 2.1.26. *Homomorfizm $i \otimes id$ $\mathbb{Z}$-modułów jest injekcją*

Dowód. Niech $\sum_i \overline{m}_i \otimes \frac{a_i}{b_i} = 0$ w $\overline{M} \otimes \mathbb{Q}$. Skoro $\overline{M}'$ jest wolny, to:

$$\overline{m}_i = \sum_k c_{ik}\overline{e}_k,$$

gdzie $\{\overline{e}_k\}_{k=1}^n$ jest bazą wolną. Wówczas:

$$\sum_i \sum_k c_{ik}\overline{e}_k \otimes \frac{a_i}{b_i} = 0$$

$$\sum_k \overline{e}_k \otimes \left(\sum_i \frac{c_{ik}a_i}{b_i} \right) = 0.$$

Istnieje m całkowite takie, że jeśli $A_k = \sum_i \frac{c_{ik}a_i}{b_i}$, to $A_k m \in \mathbb{Z}$. Wówczas:

$$\sum_k \overline{e}_k \otimes_{\mathbb{Z}} (A_k m) = 0$$

$$\left(\sum_k (A_k m)\overline{e}_k \right) \otimes_{\mathbb{Z}} 1 = 0.$$

Skoro $\overline{M}$ jest beztorsyjny, to $\sum_k (A_k m)\overline{e}_k = 0$ w $\overline{M}$ i w $\overline{M}'$. Skoro $\overline{M}'$ jest wolny, to $A_k m = 0$ dla dowolnego k, stąd $A_k = 0$ dla wszystkich k (bo $m \neq 0$). Zatem element $\sum_i \overline{m}_i \otimes \frac{a_i}{b_i} = 0$ w $\overline{M}' \otimes_{\mathbb{Z}} \mathbb{Q}$. □

Zauważmy, że

$$(\overline{M}' \otimes_{\mathbb{Z}} \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{R} \cong \overline{M}' \otimes_{\mathbb{Z}} \mathbb{R}.$$

Skoro zachodzi inkluzja $\overline{M}'_{\mathbb{Q}} \subset \overline{M}_{\mathbb{Q}}$, to zachodzi też $\overline{M}'_{\mathbb{R}} \subset \overline{M}_{\mathbb{R}}$. Implikuje to równość zbiorów:

$$\overline{M} \otimes_{\mathbb{Z}} \mathbb{R} = \bigcup_{\overline{M}' \subset \overline{M}} \overline{M}' \otimes_{\mathbb{Z}} \mathbb{R},$$

gdzie suma jest po skończenie generowanych modułach.

Moduł $\overline{M} \otimes_{\mathbb{Z}} \mathbb{R}$ wyposażamy w topologię finalną (topologię granicy prostej) pochodzącą od rodziny inkluzji:

$$f_{\overline{M}'} : \overline{M}' \otimes_{\mathbb{Z}} \mathbb{R} \hookrightarrow \overline{M} \otimes_{\mathbb{Z}} \mathbb{R}$$

indeksowaną wszystkimi skończenie generowanymi podmodułami $\overline{M}'$ w $\overline{M}$. Topologia na $V = \overline{M}' \otimes_{\mathbb{Z}} \mathbb{R}$ pochodzi z topologii naturalnej indukowanej przez $\mathbb{R}$ na $V \cong \mathbb{R}^n$ dla pewnego n. Zbiór U jest otwarty w $\overline{M} \otimes_{\mathbb{Z}} \mathbb{R}$ wtedy i tylko wtedy, gdy dla dowolnego skończenie generowanego podmodułu $\overline{M}' \subset \overline{M}$ $f^{-1}_{\overline{M}'}(U)$ jest otwarty w $\overline{M}' \otimes_{\mathbb{Z}} \mathbb{R}$.

Powyższa równość i jednoznaczność rozszerzenia formy $\overline{g}$ (Stwierdzenie 2.1.25) implikują, że rozszerzenia $\overline{g}_{\mathbb{R}}$ na przecięciach $\overline{M^{(1)}}_{\mathbb{R}} \cap \overline{M^{(2)}}_{\mathbb{R}}$ różnych par skończenie generowanych podmodułów $\overline{M^{(1)}}, \overline{M^{(2)}} \subset \overline{M}$ pokrywają się. Zatem istnieje jedyne rozszerzenie formy $\overline{g}$ na $\overline{M}$ do formy $\overline{g}_{\mathbb{R}}$ na $\overline{M}_{\mathbb{R}}$.

Twierdzenie 2.1.27. *Niech $g : M \times M \to \mathbb{R}$ będzie symetryczną formą dwuliniową nad $\mathbb{Z}$. Wówczas jeśli N jest jądrem odwzorowania g oraz $\overline{M} = M/N$, to istnieje jedyne rozszerzenie $\overline{g}_{\mathbb{R}}$ formy dwuliniowej $\overline{g} : \overline{M} \times \overline{M} \to \mathbb{R}$ na $\overline{M} \otimes_{\mathbb{Z}} \mathbb{R}$.*

Uwaga 2.1.28. Analogiczne twiedzenie zachodzi jeśli zbiór liczb rzeczywistych $\mathbb{R}$ zastąpimy liczbami wymiernymi $\mathbb{Q}$.

Fakt 2.1.29. *Niech forma $\overline{g} : \overline{M} \times \overline{M} \to \mathbb{R}$ będzie dodatnio określona, tj. $\overline{g}(x,x) > 0$ dla $x \in \overline{M} \setminus \{0\}$. Wówczas $\overline{g}_{\mathbb{R}}(x,x) \geq 0$ dla $x \in \overline{M}_{\mathbb{R}}$.*

Dowód. Zauważmy najpierw, że inkluzja $\mathbb{Q} \subset \mathbb{R}$ indukuje $\overline{M}_{\mathbb{Q}} \subset \overline{M}_{\mathbb{R}}$.

Niech $x \in \overline{M}_{\mathbb{Q}}$, wówczas istnieje $m \in \mathbb{Z}$ takie, że $mx \in \overline{M}$ (utożsamiamy $\overline{M}$ z obrazem przez kanoniczną injekcję $\overline{M} \to \overline{M}_{\mathbb{Q}}$). Zatem $m^2 \overline{g}_{\mathbb{Q}}(x,x) = \overline{g}_{\mathbb{Q}}(mx,mx) = \overline{g}(mx,mx) > 0$, a stąd $\overline{g}_{\mathbb{Q}}(x,x) > 0$.

Zauważmy, że funkcja $f(x) = \overline{g}_{\mathbb{R}}(x,x)$ jest ciągła w topologii finalnej na $\overline{M} \otimes \mathbb{R}$, ponieważ jej obcięcie do $\overline{M}' \otimes \mathbb{R}$ jest ciągłe.

W takim razie z inkluzji $\overline{M}_{\mathbb{Q}} \subset \overline{M}_{\mathbb{R}}$ i ciągłości otrzymujemy, że

$$\overline{g}_{\mathbb{R}}(x,x) \geq 0.$$

□

Lemat 2.1.30. *Forma dwuliniowa $\overline{g}_{\mathbb{R}}$ jest dodatnio określona na $\overline{M}_{\mathbb{R}}$ wtedy i tylko wtedy, gdy dla dowolnego skończenie generowanego podmodułu $\overline{M}' \subset \overline{M}$ i dowolnej stałej $C > 0$ zbiór:*

$$\left\{ x \in \overline{M}' \mid \overline{g}_{\mathbb{R}}(x,x) \leq C \right\}$$

jest skończony.

Dowód. Bez utraty ogólności możemy założyć, że $\overline{M}$ jest skończenie generowanym modułem. Kanoniczna injekcja $i : \overline{M} \to \overline{M}_{\mathbb{R}} : \overline{m} \mapsto \overline{m} \otimes 1$ pozwala utożsamić $\overline{M}$ z kratą generowaną przez obraz modułu w $\overline{M}_{\mathbb{R}}$. Krata w skończenie generowanej przestrzeni liniowej nad $\mathbb{R}$ jest dyskretna, więc w ograniczonym otoczeniu zera w przestrzeni liniowej $\overline{M}_{\mathbb{R}}$ istnieje skończenie wiele punktów kratowych. Jeśli $\overline{g}_{\mathbb{R}}$ jest dodatnio określone , to zbiór z tezy jest skończony dla dowolnego $C > 0$.

Załóżmy teraz, że $\overline{g}_{\mathbb{R}}$ nie jest dodatnio określona. Gdyby istniało nieskończenie wiele $x \in \overline{M}_{\mathbb{R}}$ takich, że $\overline{g}_{\mathbb{R}}(x,x) < 0$ to zbiór $\left\{ x \in \overline{M} | \overline{g}_{\mathbb{R}}(x,x) \leq C \right\}$ byłby nieskończony. Niech zatem forma $\overline{g}_{\mathbb{R}}$ będzie nieujemnie określona. Istnieje $y \in \overline{M}_{\mathbb{R}} \setminus \{0\}$ takie, że $\overline{g}_{\mathbb{R}}(y,y) = 0$. Z twierdzenia Cauchy'ego-Schwarza (dla form dwuliniowych nieujemnie określonych):

$$0 \leq |\overline{g}_{\mathbb{R}}(x,y)|^2 \leq \overline{g}_{\mathbb{R}}(x,x) \cdot \overline{g}_{\mathbb{R}}(y,y)$$

dla dowolnego $x \in \overline{M}_{\mathbb{R}}$ wynika, że y należy do jądra formy $\overline{g}_{\mathbb{R}}$.

Zauważmy, że obcięcie formy $\overline{g}_{\mathbb{R}}$ do kraty $i(\overline{M})$ ma trywialne jądro. Zatem $y \notin \overline{M}_{\mathbb{Q}}$ (biorąc naturalną inkluzję $\overline{M}_{\mathbb{Q}} \subset \overline{M}_{\mathbb{R}}$ indukowaną przez $\mathbb{Q} \hookrightarrow \mathbb{R}$).

Wybieramy bazę $\{e_i\}_{i=1}^r$ w $\overline{M}$. Obraz $i(\{e_i\}_{i=1}^r) = \{e_i \otimes 1\}$ jest bazą w $\overline{M}_{\mathbb{R}}$. Dla każdego $n \in \mathbb{N}$ istnieje takie $y_n \in i(\overline{M})$, że współrzędne

$$y_n - ny$$

należą do przedziału $[0,1]$ (wybieramy pewną bazę w $\overline{M}_{\mathbb{R}} \cong \mathbb{R}^r$ i współrzędne x_i). Elementy $y_n - ny$ należą do zwartej kostki:

$$\left\{ \sum_{i=1}^{r} \alpha_i x_i \mid 0 \leq \alpha_i \leq 1 \right\}.$$

Z drugiej strony:

$$\overline{g}_{\mathbb{R}}(y_n - ny, y_n - ny) = \overline{g}_{\mathbb{R}}(y_n, y_n),$$

gdyż y należy do jądra $\overline{g}_{\mathbb{R}}$.

Odwzorowanie $f(x) = \overline{g}_{\mathbb{R}}(x,x)$ jest ciągłe, zatem ograniczone na zwartej kostce zdefiniowanej powyżej. Skoro $y \notin \overline{M}_{\mathbb{Q}}$, to zbiór $\{y_n | n \in \mathbb{N}\}$ jest nieskończony i zawarty w zbiórze:

$$\left\{ x \in \overline{M} | \overline{g}_{\mathbb{R}}(x,x) \leq C \right\}.$$

□

Twierdzenie 2.1.31. *Niech A będzie rozmaitością abelową nad ciałem liczbowym K. Jeśli $D \in \mathrm{Div}(A)$ jest szerokim dywizorem symetrycznym, to stowarzyszona z nim kanoniczna wysokość $\hat{h} = \hat{h}_{A,D} : A(\overline{K}) \to \mathbb{R}$ rozszerza się jednoznacznie do dodatnio określonej formy kwadratowej $\hat{h}_{\mathbb{R}} : A(\overline{K}) \otimes_{\mathbb{Z}} \mathbb{R} \to \mathbb{R}$ nad $\mathbb{R}$. Dokładniej, istnieje jedyny iloczyn skalarny $\langle \cdot, \cdot \rangle_{\mathbb{R}} : (A(\overline{K}) \otimes_{\mathbb{Z}} \mathbb{R}) \times (A(\overline{K}) \otimes_{\mathbb{Z}} \mathbb{R}) \to \mathbb{R}$ taki, że:*

$$\hat{h}(P) = \langle P \otimes 1, P \otimes 1 \rangle$$

dla dowolnego $P \in A(\overline{K})$.

Ponadto $\hat{h}(P) = 0$ wtedy i tylko wtedy, gdy P jest punktem torsyjnym w $A(\overline{K})$.

Dowód. Z Twierdzenia 2.1.23 wynika, że na $\mathbb{Z}$-module $A(\overline{K})$ istnieje odwzorowanie dwuliniowe $\langle \cdot, \cdot \rangle : A(\overline{K}) \times A(\overline{K}) \to \mathbb{R}$ symetryczne i nieujemnie określone ($\langle P, P \rangle \geq 0$ dla dowolnego $P \in A(\overline{K})$).

Udowodnimy teraz, że $\hat{h}_{A,D}(P) = 0$ wtedy i tylko wtedy, gdy P jest torsyjny w $A(\overline{K})$.

Niech $P \in A(\overline{K})$. Twierdzenie 2.1.22 zastosowane do $\phi = [2]$ i $V = A$ oraz dywizora D implikuje, że $\hat{h}_{A,D}(P) \geq 0$ i równość zachodzi wtedy i tylko wtedy, gdy punkt zbioru $O_P = \{P, [2]P, \ldots, [2^n]P, \ldots\}$ jest skończony. Jeśli zbiór O_P jest skończony, to istnieją k, n naturalne takie, że $[2^k]P = [2^{k+n}]P$, co pociąga $[2^{k+n} - 2^k]P = O$, czyli punkt P jest torsyjny. Z drugiej strony jeśli punkt P jest rzędu n i $NWD(n,2) = 1$, to z twierdzenia Eulera $2^{\phi(n)} \equiv 1 (\mathrm{mod}\ n)$. Wówczas $[2^{\phi(n)}]P = P$ i zbiór O_P jest skończony. Jeśli natomiast $n = 2^k r$ dla pewnego $k > 0$ i $NWD(r,2) = 1$, to z twierdzenia Eulera wiemy, że $2^{\phi(r)} \equiv 1 (\mathrm{mod}$ r, czyli istnieje m naturalne takie, że $(2^{\phi r} - 1) = rm$ oraz $2^k(2^{\phi r} - 1) = 2^k rm = nm$. W takim razie $[2^k(2^{\phi r} - 1) + 1]P = P$, co pociąga skończoność zbioru O_P.

Obliczmy teraz jądro N odwzorowania dwuliniowego na $A(\overline{K})$:

$$N = \left\{ P \in A(\overline{K}) \mid \langle P, Q \rangle = 0 \text{ dla dowolnego } Q \in A(\overline{K}) \right\}.$$

Jeśli $P \in N$, to w szczególności $0 = \langle P, P \rangle = \hat{h}_{A,D}(P)$, co pociąga, że P jest punktem torsyjnym, czyli $N \subset A(\overline{K})_{tors}$. Wiemy ponadto, że z własności

odwzorowania dwuliniowego $\langle \cdot, \cdot \rangle$ wynika, że $A(\overline{K})_{tors} \subset N$, stąd $A(\overline{K})_{tors} = N$.

Ciąg dokładny:

$$A(\overline{K})_{tors} \to A(\overline{K}) \to A(\overline{K})/A(\overline{K})_{tors} \to 0$$

tensorujemy z prawej strony $\mathbb{R}$ i korzystamy z prawej dokładności operacji tensorowania. Skoro $A(\overline{K})_{tors} \otimes_{\mathbb{Z}} \mathbb{R} = 0$, to dostajemy izomorfizm:

$$A(\overline{K}) \otimes_{\mathbb{Z}} \mathbb{R} \cong (A(\overline{K})/A(\overline{K})_{tors}) \otimes_{\mathbb{Z}} \mathbb{R}. \tag{2.10}$$

Ponadto w notacji Twierdzenia 2.1.27 $M = A(\overline{K})$ oraz $N = A(\overline{K})_{tors}$, więc $\overline{M} = M/N = A(\overline{K})/A(\overline{K})_{tors}$ i izomorfizm (2.10) implikuje, że $\overline{M}_{\mathbb{R}} \cong M \otimes_{\mathbb{Z}} \mathbb{R}$. Zatem na mocy Twierdzenia 2.1.27 istnieje jedyne rozszerzenie formy dwuliniowej $\langle \cdot, \cdot \rangle$ na $A(\overline{K})$ do formy dwuliniowej $\langle \cdot, \cdot \rangle_{\mathbb{R}}$ na $A(\overline{K}) \otimes_{\mathbb{Z}} \mathbb{R}$. Konstrukcja z Twierdzenia 2.1.23 oraz Fakt 2.1.29 gwarantują nam, że forma $\langle \cdot, \cdot \rangle_{\mathbb{R}}$ jest nieujemna.

Ponadto Twierdzenie 2.1.18 podpunkt (f) oraz Lemat 2.1.30 pociągają, że rozszerzenie formy dwuliniowej na $A(\overline{K})$:

$$\langle \cdot, \cdot \rangle_{\mathbb{R}} : (A(\overline{K}) \otimes_{\mathbb{Z}} \mathbb{R}) \times (A(\overline{K}) \otimes_{\mathbb{Z}} \mathbb{R}) \to \mathbb{R}$$

jest dodatnio określoną symetryczną formą dwuliniowa, czyli iloczynem skalarnym.

Z jedyności rozszerzenia formy dwuliniowej $\langle \cdot, \cdot \rangle$ wynika także, że:

$$\hat{h}_{A,D}(P) = \langle P, P \rangle = \langle P \otimes \mathbb{R}, P \otimes \mathbb{R} \rangle_{\mathbb{R}}$$

dla dowolnego punktu $P \in A(\overline{K})$. □

2.2 Twierdzenie Mordella-Weila

Twierdzenie 2.2.1 (Mordell-Weil)**.** *Niech A będzie rozmaitością abelową zdefiniowaną nad ciałem liczbowym K. Wówczas grupa punktów K-wymiernych $A(K)$ rozmaitości A jest skończenie generowaną grupą abelową.*

Z twierdzenia klasyfikacyjnego dla grup abelowych skończenie generowanych otrzymujemy następujący bezpośredni wniosek.

Twierdzenie 2.2.2. *Niech A będzie rozmaitością abelową zdefiniowaną nad ciałem liczbowym K. Wówczas istnieje skończony zbiór punktów $\{P_1, \ldots, P_k\}$ oraz skończony zbiór $T \subset A(K)$ takie, że:*

$$A(K) = T \oplus \mathbb{Z}P_1 \oplus \ldots \mathbb{Z}P_k, \tag{2.11}$$

gdzie punkty P_i są nieskończonego rzędu, a punkty ze zbioru T są skończonego rzędu w $A(K)$.

Dowód Twierdzenia 2.2.1 oparty jest na poniższych twierdzeniach, które zostaną dowiedzione w dalszej części rozdziału.

Twierdzenie 2.2.3 ("Słabe" twierdzenie Mordella-Weila)**.** *Niech A będzie rozmaitością abelową określoną nad ciałem liczbowym K. Niech $m \geq 2$ będzie liczbą całkowitą. Wówczas grupa $A(K)/mA(K)$ jest skończona.*

Twierdzenie 2.2.4 (O spadku na grupach abelowych)**.** *Niech G będzie grupą abelową wyposażoną w formę kwadratową (patrz Definicja 4.1.1):*

$$q : G \to \mathbb{R} \tag{2.12}$$

taką, że zbiór $\{x \in G : q(x) \leq C\}$ jest skończony dla dowolnego $C > 0$ oraz $q(x) \geq 0$ dla dowolnego $x \in G$. Załóżmy ponadto, że grupa G/mG jest skończona dla pewnego $m \geq 2$ całkowitego. Niech funkcja $|x| := \sqrt{q(x)}$ spełnia nierówności:

$$|x \pm y| \leq |x| + |y|$$

oraz własność jednorodności:

$$|mx| = m|x|$$

dla dowolnych $x, y \in G$. Wówczas grupa G jest skończenie generowana. Dokładniej - istnieje zbiór $\{g_1, \ldots, g_s\}$ reprezentantów klas w G/mG taki, że G jest generowane przez zbiór:

$$\{x \in G : q(x) \leq C_0\}, \tag{2.13}$$

gdzie $C_0 = \max_i q(g_i)$.

Dowód. Określmy zbiór $S = \{x \in G : |x| \leq c_0\}$, gdzie $c_0 = \sqrt{C_0}$. Pokażemy, że zbiór S generuje grupę G. Niech $x_0 \in G$. Jeśli $x_0 \in S$ to koniec dowodu. Przypuśćmy zatem, że $x_0 \in G \setminus S$. W takim razie $|x_0| > c_0$. Istnieje i takie, że:

$$x_0 = g_i + mx_1 \tag{2.14}$$

dla pewnego $x_1 \in G$. Z nierówności $|x + y| \leq |x| + |y|$ oraz $|g_i| \leq c_0 < |x_0|$:

$$m|x_1| = |x_0 - g_i| \leq |x_0| + |g_i| < 2|x_0| \tag{2.15}$$

Ponieważ $m \geq 2$, to $|x_1| < |x_0|$. Indukcyjnie dostaniemy ciąg punktów x_i spełniających nierówności:

$$|x_0| > |x_1| > |x_2| > \ldots.$$

W grupie G istnieje tylko skończenie wiele punktów, dla których $|x| < |x_0|$, zatem dla pewnego t musi zachodzić $x_t \in S$, czyli x_0 jest kombinacją liniową elementów z S. □

Dowód Twierdzenia 2.2.1 przy założeniu Twierdzenia 2.2.3. Na mocy Twierdzenia 4.2.23 istnieje bardzo szeroki dywizor symetryczny $D \in \mathrm{Div}(A)$. Wysokość kanoniczna $\widehat{h}_{A,D} : A(K) \to \mathbb{R}$ posiada wszystkie własności z Twierdzenia 2.1.31. Ponadto własność (f) z Twierdzenia 2.1.18 implikuje, że:

$$\{x \in A(K) : \widehat{h}_{A,D}(x) \leq C\}$$

jest skończony dla dowolnej stałej $C > 0$. Zastosowanie Twierdzenia 2.2.3 oraz Twierdzenia 2.2.4 implikuje tezę. □

Pokażemy teraz, że 'słabe' twierdzenie Mordella-Weila wystarczy udowodnić dla pewnego skończonego rozszerzenia L ciała liczbowego K.

Lemat 2.2.5. *Dla dowolnego rozszerzenia skończonego L ciała K naturalnie określone odwzorowanie:*

$$f : A(K)/mA(K) \to A(L)/mA(L) \tag{2.16}$$

ma skończone jądro.

Dowód. Niech jądro $\ker f = A(K) \cap mA(L)/mA(K)$. Możemy założyć ponadto, że L/K jest rozszerzeniem Galois i $G = Gal(L/K)$. Dla dowolnej warstwy $x + mA(K)$ w $\ker f$ ustalmy element $y \in A(L)$ taki, że $[m](y) = x$. Zdefiniujmy odwzorowanie:

$$f_x : G \to A[m](L)$$
$$f_x : \sigma \mapsto \sigma(y) - y.$$

Niech $[m](y) = [m](y') = x$. Wówczas $(y - y') \in A[m] \subset A(K)$. Zatem dla dowolnego $\sigma \in Gal(L/K)$:

$$\sigma(y) - y - (\sigma(y') - y') = \sigma(y - y') - (y - y') = 0,$$

czyli odwzorowanie f_x nie zależy od wyboru reprezentanta y. Zbiór odwzorowań $Odwz(G, A[m])$ jest skończony, bo obie grupy są skończone. Zatem wystarczy pokazać, że odwzorowanie $\phi : \ker f \to Odwz(G, A[m])$ takie, że $\phi(x) = f_x$ jest injekcją. Przypuśćmy, że $f_x = f_{x'}$ i $[m](y) = x$ oraz $[m](y') = x'$. Wówczas:

$$\sigma(y) - y = f_x(\sigma) = f_{x'}(\sigma) = \sigma(y') - y' \tag{2.17}$$

dla każdego $\sigma \in G$. Ale w takim razie $\sigma(y - y') = y - y'$ dla dowolnego $\sigma \in G$, stąd $y - y' \in A(K)$. Zatem $x - x' = [m](y - y') \in mA(K)$, czyli x i x' reprezentują tę samą klasę w $\ker f$. Zatem ϕ jest injekcją i zbiór $\ker f$ jest skończony. □

Możemy bez utraty ogólności założyć, że $A[m] \subset A(K)$ oraz $\mu_m \subset K$. Ciało, które otrzymamy nadal jest ciałem liczbowym, bo $A[m]$ jest zbiorem skończonym, a μ_m zawiera wszystkie pierwiastki z jedności stopnia m, czyli skończenie wiele elementów.

Definicja 2.2.6. Dla $x \in A(K)$ i dowolnego $\sigma \in Gal(\overline{K}/K)$ wybieramy $y \in A(\overline{K})$ takie, że $[m](y) = x$. Definiujemy odwzorowanie:

$$t(\sigma, x) := \sigma(y) - y \tag{2.18}$$

Wartość $t(\sigma, x)$ zależy od x, ale nie zależy od wyboru y (podobnie jak w dowodzie powyżej dla f_x).

Twierdzenie 2.2.7 (Odwzorowanie Kummera)**.** *Funkcja $t(\sigma, x) = \sigma(y) - y$ jest poprawnie określona i definiuje odwzorowanie dwuliniowe $t : Gal(\overline{K}/K) \times A(K) \to A[m]$. Niech L będzie rozszerzeniem K powstałym przez dołączenie współrzędnych punktów $y \in A(\overline{K})$ takich, że $[m](y) \in A(K)$. Wówczas mamy niezdegenerowane (lewostronne i prawostronne jądra są trywialne) odwzorowanie indukowane:*

$$\bar{t} : Gal(L/K) \times A(K)/mA(K) \to A[m]. \tag{2.19}$$

W szczególności, $A(K)/mA(K)$ jest skończone wtedy i tylko wtedy, gdy L jest skończonym rozszerzeniem K.

Dowód. Zauważmy, że $[m](t(\sigma,x)) = [m](\sigma(y)) - [m](y) = \sigma([m](y)) - [m](y) = \sigma(x) - x = 0$, bo morfizm $[m]$ jest zdefiniowany nad K i $[m](y) = x$. Dwuliniowość odwzorowania jest natychmiastową konsekwencją faktu, że dodawanie punktów na rozmaitości abelowej A jest zdefiniowane nad ciałem K i $\sigma \in Gal(\overline{K}/K)$:

$$\begin{aligned} t(\sigma\sigma', x) &= \sigma\sigma'(y) - y = \sigma(\sigma'(y) - y) + (\sigma(y) - y) \\ &= \sigma(t(\sigma', x)) + t(\sigma, x) = t(\sigma', x) + t(\sigma, x). \end{aligned}$$

Ostatnia równość wynika z założenia $t(\sigma', x) \in A[m] \subset A(K)$. Z drugiej strony mamy:

$$t(\sigma, x+x') = \sigma(y+y') - (y+y') = (\sigma(y) - y) + (\sigma(y') - y') = t(\sigma, x) + t(\sigma, x').$$

Obliczymy teraz lewe jądro odwzorowania t, tj.

$$\ker_l(t) = \{\sigma \in Gal(\overline{K}/K) : t(\sigma, x) = 0 \text{ dla dowolnego } x \in A(K)\}.$$

Zauważmy, że $\sigma \in \ker_l(t)$ wtedy i tylko wtedy, gdy $\sigma(y) = y$ dla dowolnego $y \in A(\overline{K})$ spełniającego $[m](y) \in A(K)$. Z definicji ciała L wynika, że $\sigma \in Gal(\overline{K}/L)$. Zatem $\ker_l(t) = Gal(\overline{K}/L)$. Analogicznie definiujemy

$$\ker_p(t) = \{x \in A(K) : t(\sigma, x) = 0 \text{ dla dowolnego } \sigma \in Gal(\overline{K}/K)\}.$$

Zauważmy, że $mA(K) \subset \ker_p(t)$. Pokażemy, że zachodzi równość obu zbiorów. Niech $x \in \ker_p(t)$. Z definicji prawego jądra mamy $\sigma(y) = y$ dla dowolnego $[m](y) = x$ oraz $\sigma \in Gal(\overline{K}/K)$. Ale w takim razie $y \in A(K)$, zatem $x \in mA(K)$. Wydzielając przez prawe i lewe jądro otrzymujemy niezdegenerowane odwzorowanie dwuliniowe:

$$\bar{t} : Gal(\overline{K}/K)/Gal(\overline{K}/L) \times A(K)/mA(K) \to A[m]$$

i z zasadniczego twierdzenia teorii Galois wiemy, że $Gal(\overline{K}/K)/Gal(\overline{K}/L) = Gal(L/K)$. Ponadto skoro odwzorowanie jest niezdegenerowane to otrzymujemy injekcje:

$$\begin{aligned} \phi_l &: Gal(L/K) \to Hom(A(K)/mA(K), A[m]) \\ \phi_p &: A(K)/mA(K) \to Hom(Gal(L/K), A[m]) \end{aligned}$$

z czego wynika, że $A(K)/mA(K)$ jest skończone wtedy i tylko wtedy, gdy $Gal(L/K)$ jest skończoną grupą, czyli L jest skończonym rozszerzeniem K. □

Ciało L jest złożeniem ciał $K(y)$ dla $[m](y) = x \in A(K)$, więc musimy zbadać własności ciał $K(y)$.

Twierdzenie 2.2.8. *Niech $x \in A(K)$ i $y \in A(\overline{K})$ będą takie, że $[m](y) = x$. Wówczas rozszerzenie $K(y)$ jest Galois i $Gal(K(y)/K)$ jest izomorficzna (w sposób kanoniczny) z pewną podgrupą grupy $A[m]$.*

Dowód. Jeśli $\sigma \in Gal(\overline{K}/K)$ to $(\sigma(y) - y) \in A[m] \subset A(K)$, zatem współrzędne wszystkich elementów sprzężonych z y należą do $K(y)$. Zatem $K(y)$ jest Galois. Ponadto odwzorowanie:

$$\phi : Gal(K(y)/K) \to A[m]$$

określone wzorem $\phi(\sigma) = t(\sigma, x) = \sigma(y) - y$ jest injekcją na mocy poprzedniego twierdzenia. □

Redukcja rozmaitości abelowej i grupy formalne

W tym podrozdziale pokażemy, że jeśli liczba pierwsza $p \nmid m$ to istnieje taka rozmaitość abelowa $\tilde{A}/\mathbb{F}_p$ nad ciałem skończonym, że zachodzi inkluzja

$$A[m](K) \hookrightarrow \tilde{A}(\mathbb{F}_p).$$

Redukcje rozmaitości abelowych

Definicja 2.2.9 (Dobra redukcja, zła redukcja)**.** Niech A/K będzie rozmaitością abelową nad ciałem i niech R_v będzie pierścieniem z waluacją dyskretną w K. Mówimy, że A ma **dobrą redukcję** w v jeśli istnieje gładki właściwy ([Har06, str. 100, df.]) schemat $\overline{A}$ nad $\mathrm{Spec}(R_v)$, którego włókno specjalne $\overline{A}_{\mathrm{Spec}(k(\eta))}$ nad punktem generycznym η jest izomorficzne z A jako schemat nad $K = k(\eta)$.

Ponadto z definicji wynika, że włókno $\overline{A}_{\mathrm{Spec}(k(v))}$ jest rozmaitością abelową nad $k(v)$ (patrz [BLR90, Prop.1.4.2]).

Jeżeli powyższa sytuacja nie zachodzi, to mówimy, że rozmaitość A ma w v **złą redukcję**.

Definicja 2.2.10 (Model rozmaitości abelowej)**.** Niech A/K będzie rozmaitością abelową nad ciałem ułamków pierścienia Dedekinda R i niech $S = \mathrm{Spec}(R)$. **Modelem** A nad S jest schemat $\mathcal{A} \to S$ (patrz Definicja 4.1.8), którego włókno generyczne jest izomorficzne z A nad $Spec(K)$.

Definicja 2.2.11 ([BLR90, Def.1.2.1], Model Nérona)**.** Niech R będzie pierścieniem Dedekinda i $K = \mathrm{Frac}(R)$. Niech A/K będzie rozmaitością abelową nad K. **Modelem Nérona** dla A nad $S = \mathrm{Spec}(R)$ nazywamy model $\mathcal{A} \to S$ dla A, który jest rozdzielony, gładki i skończonego typu oraz spełnia własność uniwersalności:

Dla dowolnego gładkiego schematu $Y \to S$ i $\mathrm{Spec}(K)$-morfizmu $u_K : Y_{\mathrm{Spec}(K)} \to A$ istnieje jedyny S-morfizm $u : Y \to \mathcal{A}$ rozszerzający (w sensie produktu rozwłóknionego) u_K.

Twierdzenie 2.2.12 ([BLR90, Thm.1.4.3])**.** *Niech A/K będzie rozmaitością abelową nad $K = \mathrm{Frac}(R)$ (R jest pierścieniem Dedekinda) i $S = \mathrm{Spec}(R)$. Istnieje model Nérona rozmaitości A nad S. Ponadto jeśli $S' \subset S$ zawiera wszystkie domknięte punkty dobrej redukcji A oraz punkt generyczny, to S' jest gęstym otwartym podschematem w S oraz $A \times_S S'$ (patrz Definicja 4.1.9) jest abelowym schematem nad S', tzn. włókna nad każdym punktem v domknietym z S' są rozmaitościami abelowymi nad ciałem $k(v)$.*

Przykład 2.2.13. Jeśli dana jest krzywa eliptyczna o rzutowym równaniu w postaci Weierstrassa:

$$E : y^2z = x^3 + axz^2 + bz^3$$

i wyróżniku $\Delta = 4a^3 + 27b^2$ nad ciałem liczbowym K, to elementy Δ, a, b oraz Δ^{-1} należą do prawie wszystkich pierścieni $O_{K,\mathfrak{p}}$ lokalizacji pierścienia liczb całkowitych $\mathcal{O}_K$ poza ideałem pierwszym $\mathfrak{p}$. Istnieje otwarty $S' \subset S$ taki, że a, b, Δ przedłużają się do sekcji na $\mathcal{O}_S(S')$ i Δ oraz 2 są odwracalne w $\mathcal{O}(S')$. Stąd dostajemy schemat abelowy $\overline{E} \to S'$, którego włókna są krzywymi eliptycznymi, a zatem $\overline{E}$ jest modelem Nérona dla E/K (patrz [BLR90, Prop. 1.4.2]).

Wprowadzimy teraz elementy teorii grup formalnych, aby udowodnić twierdzenie o redukcji dla rozmaitości abelowych (patrz Twierdzenie 2.2.23).

Grupy formalne

Definicja 2.2.14 (Grupa formalna)**.** Niech dany będzie pierścień R oraz dodatnia liczba naturalna g. Wybieramy elementy

$$F_1, \ldots, F_g \in S = R[[X_1, \ldots, X_g, Y_1, \ldots, Y_g]]$$

pierścienia szeregów formalnych $2g$ zmiennych. Wówczas wektor $F = (F_1, \ldots, F_g)$ nazywamy grupą formalną wymiaru g jeśli spełnione są warunki:

(i) $F_i = X_i + Y_i + h$, gdzie $h \in (\{X_i Y_j\}_{i,j})$,

(ii) $F(X, F(Y, Z)) = F(F(X, Y), Z)$ dla dowolnych wektorów X, Y, Z.

(iii) Istnieje jedyny wektor $i(X) = (i_1(X), \ldots, i_g(X))$ taki, że $i_k(X)$ nie mają wyrazów stałych oraz $F(X, i(X)) = 0 = F(i(X), X)$.

Ponadto grupa formalna jest **przemienna** jeśli spełnia warunek:

$$F(X, Y) = F(Y, X).$$

Przykład 2.2.15. Niech G będzie grupą algebraiczną wymiaru g nad ciałem k (patrz Definicja 4.1.21) i niech $e \in G(k)$ będzie elementem neutralnym. Grupa algebraiczna jest zawsze gładka (por. Wniosek 4.1.22), więc zachodzi równość $dim_{k(e)}(m_{e,G}/m_{e,G}^2) = g$ i generatory $x_1, \ldots, x_g$ przestrzeni liniowej $m_{e,G}/m_{e,G}^2$ określają parametry lokalne wokół e. Ponadto uzupełnienie pierścienia lokalnego $\mathcal{O}_{e,G}$ ze względu na ideał maksymalny $m_{e,G}$ jest izomorficzne z:

$$k[[x_1, \ldots, x_g]]$$

na mocy [Har06, Thm.5.5A]. Zachodzi inkluzja:

$$\mathcal{O}_{e,G} \hookrightarrow k[[x_1, \ldots, x_g]],$$

która jest określona przez przyporządkowanie elementom z $\mathcal{O}_{e,G}$ rozwinięć w szereg Taylora wokół e. Podobnie dla identyczności (e, e) w grupie $G \times G$ wybieramy parametry lokalne:

$$y_i = x_i \circ p_1 \text{ oraz } z_i = x_i \circ p_2$$

dla pierścienia $\mathcal{O}_{(e,e),G\times G}$. Funkcje p_1 i p_2 są projekcjami na pierwszy i drugi składnik. Otrzymujemy inkluzję:

$$\mathcal{O}_{(e,e),G\times G} \hookrightarrow k[[y_1, \ldots, y_g, z_1, \ldots, z_g]].$$

Mnożenie $\mu : G \times G \to G$ w grupie G indukuje homomorfizm:

$$\mu^* : k[[x_1, \ldots, x_g]] \to k[[y_1, \ldots, y_g, z_1, \ldots, z_g]].$$

Definiujemy

$$F_i = \mu^*(x_i).$$

Pokażemy, że $F = (F_1, \ldots, F_g)$ określa przemienną grupę formalną nad ciałem k.

Niech $j_1, j_2 : G \to G \times G$ będą takie, że $j_1(g) = (g, e)$ oraz $j_1(g) = (e, g)$. Zachodzą równości $m \circ j_1 = \mathrm{id}_G = m \circ j_2$ oraz $(m \circ j_i)^* = j_i^* \circ m^*$. Ponadto na poziomie pierścieni lokalnych:

$$j_1^* : \begin{cases} y_i & \mapsto & x_i \\ z_i & \mapsto & 0 \end{cases}$$

i podobnie dla j_2^* zamieniając y_i i z_i rolami. Skoro z jednej strony $(m \circ j_i)^* = id_G^*$, to:

$$(m \circ j_i)^* : x_i \mapsto x_i.$$

Z drugiej strony:

$$j_1^* \circ m^* : x_i \mapsto F_i(y_1, \ldots, y_g, z_1 \ldots, z_g) \mapsto F_i(x_1, \ldots, x_g, 0, \ldots, 0).$$

Zatem $F_i(x_1, \ldots, x_g, 0, \ldots, 0) = x_i$. Analogicznie dla j_2 dostajemy równość $F_i(0, \ldots, 0, x_1, \ldots, x_g) = x_i$, a stąd wynika już własność (i) z definicji grupy formalnej.

Rozważmy teraz dwa następujące odwzorowania:

$$\Phi_1 : \begin{cases} G \times G \times G & \to & G \times G & \to & G \\ (x, y, z) & \mapsto & (\mu(x, y), z) & \mapsto & \mu(\mu(x, y), z) \end{cases},$$

$$\Phi_2 : \begin{cases} G \times G \times G & \to & G \times G & \to & G \\ (x, y, z) & \mapsto & (x, \mu(y, z)) & \mapsto & \mu(x, \mu(y, z)) \end{cases},$$

które są równe $\Phi_1 = \Phi_2$ na mocy łączności mnożenia μ w G. Biorąc mapy stowarzyszone na poziomie pierścieni lokalnych wokół identyczności dostaniemy równości $F(X, F(Y, Z) = F(F(X, Y), Z)$.

Ponadto morfizm $\mathrm{inv} : G \to G$ postaci $\mathrm{inv}(g) = g^{-1}$ oraz odwzorowanie pseudodiagonalne $\Delta : G \to G \times G$ określone wzorem $\Delta(g) = (g, \mathrm{inv}(g))$ dają nam złożenie:

$$\Phi : \begin{cases} G & \xrightarrow{\Delta} & G \times G & \to & G \\ g & \mapsto & (g, \mathrm{inv}(g)) & \mapsto & \mu(g, \mathrm{inv}(g)) = e \end{cases}.$$

Tak określone złożenie daje nam równość $F(X, i(X)) = 0$, gdzie $i(X)$ pochodzi od $\mathrm{inv}^* : k[[x_1, \ldots, x_g]] \to k[[x_1, \ldots, x_g]]$. Analogiczna równość $F(i(X), X) = 0$ wynika z zastosowania $\Delta'(g) = (\mathrm{inv}(g), g)$. Ponadto z konstrukcji wynika, że $i(X)$ nie ma wyrazów wolnych. Jedyność jest formalną własnością. Gdyby istniały dwie funkcje $i(X)$ i $j(X)$ spełniające własność (iii), to:

$$\begin{aligned} i(X) &= F(F(X, j(X)), i(X)) = F(F(j(X), X), i(X)) \\ &= F(j(X), F(X, i(X))) = j(X). \end{aligned}$$

Jeśli ponadto grupa G jest przemienna, to na mocy $\mu(x, y) = \mu(y, x)$ łatwo wynika, że $F(X, Y) = F(Y, X)$.

Przykładowo możemy stowarzyszyć z grupą addytywną $\mathbb{G}_a$ grupę formalną $F_{\mathbb{G}_a}(X, Y) = X + Y$. Dla grupy multiplikatywnej $\mathbb{G}_m$ otrzymujemy $F_{\mathbb{G}_m}(X, Y) = X + Y + XY$. Obie grupy formalne są jednowymiarowe i przemienne, co wynika z przemienności działania grupowego. Pomimo nieprzemienności grupy

GL(n) dla $n \geq 2$ dostajemy przemienną grupę formalną zadaną funkcjami $F_{ij}(X,Y) = X_{ij} + Y_{ij} + \sum_{k=1}^{n} X_{ik}Y_{kj}$.

Dalszym celem naszych rozważań będą grupy formalne stowarzyszone z rozmaitościami abelowymi.

Definicja 2.2.16 (Homomorfizm grup formalnych)**.** Niech $F = (F_1, \ldots, F_g)$ oraz $G = (G_1, \ldots, G_h)$ określają dwie grupy formalne nad pewnym pierścieniem R wymiaru, odpowiednio g i h. **Homomorfizmem grup formalnych** F do G nad R nazywamy taki wektor $f = (f_1, \ldots, f_h)$, gdzie $f_i \in R[[x_1, \ldots, x_g]]$ (bez wyrazów stałych), który spełnia własność:

$$G(f(X), f(Y)) = f(F(X,Y)).$$

Jeśli istnieje ponadto $f' = (f_1', \ldots, f_g')$, gdzie f_i' nie mają wyrazów stałych oraz:

$$f'(f(X)) = f(f'(X)) = X,$$

to f nazywamy **izomorfizmem** grup formalnych.

Zauważmy ponadto, że f' musi być homomorfizmem grup formalnych:

$$F(f'(X), f'(Y)) = f'(f(F(f'(X), f'(Y)))) = f'(G(f(f'(X)), f(f'(Y)))) = f'(G(X,Y)).$$

Lemat 2.2.17. *Niech $f = (f_1, \ldots, f_n) \in R[[x_1, \ldots, x_n]]^n$ będzie wektorem szeregów formalnych takim, że:*

$$f_i = \sum_{j=1}^{n} f_{ij}x_j + (\textit{wyrazy stopnia } \geq 2).$$

Wyznacznik $\det(f_{ij}) \in R^*$ *jest odwracalny w R wtedy i tylko wtedy, gdy istnieje jedyny wektor $g \in R[[x_1, \ldots, x_n]]^n$ bez wyrazów stałych taki,że:*

$$f(g(X)) = g(f(X)) = X.$$

Dowód. Jeśli zachodzi równość $f(g(X)) = g(f(X)) = X$, to istnieje macierz $A = (g_{ij}) \in M_{n,n}(R)$ pochodząca od części liniowych szeregów g_k taka, że $A \cdot (f_{ij}) = I = (f_{ij})A$, gdzie I jest macierzą identycznościową. Stąd wynika, że (f_{ij}) jest odwracalna i $\det(f_{ij}) \in R^*$.

Jeśli z kolei $\det(f_{ij}) \in R^*$, to konstruujemy szeregi g_i indukcyjnie. Niech $g^{(1)} = (g_1^{(1)}, \ldots, g_n^{(1)})$ będzie taki, że

$$g_i^{(1)} = \sum_{j=1}^{n} g_{ij}x_j$$

i $(g_{ij}) = (f_{ij})^{-1}$. Określmy rodzinę ideałów:

$$I_j := (\{x_{i_1} \cdot \ldots \cdot x_{i_k} : i_1 + \ldots + i_k = j\})$$

generowanych przez wszystkie jednomiany stopnia j. W ten sposób otrzymujemy układ kongruencji:

$$g^{(1)}(f(x_1, \ldots, x_n)) \equiv (x_1, \ldots, x_n) (\text{mod } I_2).$$

Załóżmy teraz, że mamy skonstruowane $g^{(m)}$ spełniające kongruencję

$$g^{(m)}(f(x)) \equiv x(\text{mod } I_{m+1}),$$

gdzie $x = (x_1, \ldots, x_n)$. Niech $h(x)$ będzie uporządkowaną n-tką wielomianów jednorodnych stopnia $m+1$ spełniających

$$g^{(m)}(f(x)) - x \equiv h(x)(\text{mod } I_{m+2}).$$

Kładąc $r(x) = h((g_{ij})x)$ (gdzie x traktujemy jako wektor kolumnowy, który mnożymy przez macierz (g_{ij})) możemy wziąć

$$g^{(m+1)}(x) = g^{(m)}(x) - r(x).$$

Wówczas zachodzi:

$$g^{(m+1)}(f(x)) \equiv x(\text{mod } I_{m+2}).$$

Stąd dostajemy wektor $g = (g_1, \ldots, g_n)$, gdzie $g \equiv g^{(i)}(\text{mod } I_{i+1})$ spełniający:

$$g(f(X)) = X.$$

Z konstrukcji wynika, że g jest jedyne takie, które spełnia relację $g(f(X)) = X$. Analogicznie konstruujemy g' takie, że $f(g'(X)) = X$. Wówczas:

$$g(X) = g(f(g'(X))) = (g \circ f)(g'(X)) = g'(X).$$

□

Interesuje nas teraz, kiedy homomorfizm mnożenia przez $[m]$ określony nastepująco:

$$[-1](X) = i(X), \quad [0](X) = 0, \quad [1](X) = X,$$

$$[m](X) = F(X, [m-1](X)), \quad [m](X) = F(i(X), [m+1](X))$$

jest izomorfizmem nad R przemiennej grupy formalnej F. Łatwo sprawdzić z definicji, że $[m](x_1, \ldots, x_n) = m(x_1 + \ldots + x_n) + \ldots$ i z kryterium z Lematu 2.2.17 jest on izomorfizmem F w siebie wtedy i tylko wtedy, gdy m jest odwracalne w R.

Zauważmy teraz, że jeżeli mamy rozmaitość abelową A nad ciałem liczbowym K oraz normę $v \in M_K^0$, to inkluzja $K \subset K_v$ pozwala nam rozszerzyć A do rozmaitości nad K_v i wówczas $A(K) \subset A(K_v)$. Ponadto pierścień liczb całkowitych w $\mathcal{O}_K \subset \mathcal{O}_v$ oraz $\text{Frac}(\mathcal{O}_v) = K_v$ i $\mathcal{O}_v$ jest zupełny ze względu na topologię proskończoną pochodzącą od jedynego ideału maksymalnego $M_v \subset \mathcal{O}_v$. Ciało reszt $k = \mathcal{O}_v/M_v$ ma dodatnią charakterystykę i jeśli rozmaitość abelowa A/K_v ma dobrą redukcję w v, to schemat nad $\text{Spec}(\mathcal{O}_v)$, do którego przedłuża się A ma nad jedynym punktem domkniętym (odpowiadającym M_v) włókno, które jest rozmaitością abelową $\tilde{A}$ nad ciałem reszt k. Z własności dobrej redukcji wynika ponadto, że morfizm dodawania $\mu : A \times A \to A$ redukuje się do morfizmu $\tilde{\mu} : \tilde{A} \times \tilde{A} \to \tilde{A}$. Ponadto zachodzi następujący lemat.

Lemat 2.2.18. *Niech $R = \mathcal{O}_v$ i $\mathcal{M} = M_v$ oraz A i $\tilde{A}$ będą zdefiniowane jak wyżej. Istnieją parametry lokalne $x_1, \ldots, x_g$ wokół identyczności e w A, które redukują się do parametrów lokalnych $\tilde{x}_1, \ldots, \tilde{x}_g$ w $\tilde{e}$ na $\tilde{A}$. Grupa formalna stowarzyszona z A ma składowe $F_i \in R[[X_1, \ldots, X_g, Y_1, \ldots, Y_g]]$.*

Dowód. Redukcja grupy formalnej $F = (F_1, \ldots, F_g)$ do grupy formalnej wokół $\tilde{e}$ przy zachowaniu wyżej wskazanych parametrów lokalnych daje tezę (patrz [HS00, Lemma C.2.4]). □

Rozważanie grupy formalnej F o współczynnikach w pierścieniu lokalnym i zupełnym R ma tę zaletę, że pozwala zdefiniować "prawdziwą" grupę, tj. określić strukturę grupową na zbiorze punktów $F(\mathcal{M})$, gdzie $\mathcal{M}$ jest ideałem maksymalnym w R. Zbieżność szeregów po podstawieniu elementów z $\mathcal{M}$ będzie wynikać z definicji topologii $\mathcal{M}$-adycznej na R, tj. $\lim_{n\to\infty} x_n = x \in R$ wtedy i tylko wtedy, gdy dla dowolnego k istnieje n_k takie, że dla $n > n_k$ $x - x_n \in \mathcal{M}^k$.

Definicja 2.2.19 (Grupa stowarzyszona z grupą formalną)**.** Niech F będzie przemienną grupą formalną wymiaru g określoną nad zupełnym pierścieniem lokalnym R z ideałem maksymalnym $\mathcal{M}$. **Grupą stowarzyszoną** z F nad R i oznaczaną przez $F(\mathcal{M})$ nazywamy zbiór $\mathcal{M}^g$ wektorów wyposażonych w prawo dodawania:

$$+_F : \mathcal{M}^g \times \mathcal{M}^g \to \mathcal{M}^g,$$
$$X +_F Y := F(X, Y).$$

Poprawność określenia tego działania oraz jego własności grupowe wynikają z definicji grupy formalnej oraz wspomnianych własności topologii $\mathcal{M}$-adycznej.

W szczególności zachodzi własność.

Stwierdzenie 2.2.20. *Niech R i $\mathcal{M}$ będą określone jak wyżej i niech ciało reszt $k = R/\mathcal{M}$ ma charakterystykę równą $p > 0$. Niech F będzie przemienną grupą formalną nad R. Wówczas grupa punktów l-torsyjnych w $F(\mathcal{M})$ jest trywialna o ile $p \nmid l$.*

Dowód. Jeśli $p \nmid l$, to $l \in R^*$ i $[l]$ jest izomorfizmem grupy formalnej F w siebie, a zatem jest automorfizmem grupy $F(\mathcal{M})$. Stąd jądro $[l] : F(\mathcal{M}) \to F(\mathcal{M})$ jest trywialne. □

Specjalizujemy teraz sytuację do przypadku, gdy mamy daną normę $v \in M_K^0$ dla ciała liczbowego K i otrzymujemy uzupełnienie $K_v/\mathbb{Q}_p$, skończone rozszerzenie ciała liczb p-adycznych dla pewnego p. Otrzymujemy zupełny pierścień lokalny $R_v = \{x \in K_v : |x|_v \geq 0\}$ i $\mathcal{M}_v = \{x \in K_v : |x|_v > 0\}$ oraz ciało reszt $k(v) = R_v/M_v$. Rozszerzamy dla rozmaitości abelowej A/K ciało definicji i otrzymujemy A/K_v. Wówczas jeśli v jest miejscem dobrej redukcji, to istnieje gładki i właściwy schemat $\mathcal{A} \to \mathrm{Spec}(R_v)$, który jest jednocześnie modelem Nérona dla A/K_v (patrz [BLR90, 10.3.9]). Własność uniwersalności modelu Nérona pozwala przedłużyć dowolny punkt $\mathrm{Spec}(K_v) \to A$ do punktu $\mathrm{Spec}(R_v) \to \mathcal{A}$ w jedyny sposób. Zamiana bazy $\mathrm{Spec}(k(v)) \to \mathrm{Spec}(R_v)$ (dla równań afinicznych oznaczająca redukcję 'modulo' $\mathcal{M}_v$) da nam pewien punkt $\mathrm{Spec}(k(v)) \to \mathcal{A}_v = \tilde{A}$. W ten sposób otrzymaliśmy odwzorowanie redukcji.

Definicja 2.2.21 (Homomorfizm redukcji)**.** Niech dana będzie rozmaitość abelowa A nad ciałem liczbowym K oraz norma $v \in M_K^0$. **Homomorfizmem redukcji** nazywamy odwzorowanie:

$$\mathrm{red} : A(K_v) = \mathrm{Mor}(\mathrm{Spec}(K_v), A) \to \mathrm{Mor}(\mathrm{Spec}(k(v)), \tilde{A}) = \tilde{A}(k(v)),$$

które na mocy powyższej dyskusji jest poprawnie określone.

Twierdzenie 2.2.22 ([HS00, Thm.C.2.6]). *Jądro*

$$A_1(K_v) := \ker\{\mathrm{red} : A(K_v) \to \tilde{A}(k(v))\}$$

jest izomorficzne z $F(\mathcal{M}_v)$, gdzie F jest przemienną grupą formalną nad R_v stowarzyszoną z A.

Dowód. Pokażemy, że istnieją dwa odwzorowania $\phi : F(\mathcal{M}_v) \to A_1(K_v)$ i $\psi : A_1(K_v) \to F(\mathcal{M}_v)$ wzajemnie odwrotne i takie, że ϕ jest homomorfizmem grup addytywnych. Wówczas:

$$\begin{aligned}\psi(g+h) &= \psi(\phi(\psi(g)) + \phi(\psi(h))) = \psi(\phi(\psi(g) + \psi(h))) \\ &= \psi(g) + \psi(h).\end{aligned}$$

Zatem ψ również jest homomorfizmem i oba są w konsekwencji izomorfizmami.

Wybierzmy teraz parametry lokalne $x_1, \ldots, x_g$ wokół identyczności e w A (spełniające warunki Lematu 2.2.18). Istnieje takie otoczenie afiniczne otwarte $U = \mathrm{Spec}(K_v[x_1, \ldots, x_n]/I)$, gdzie I ideał zadający relacje. Elementy $x_{g+1}, \ldots, x_n$ możemy wyrazić przez szeregi potęgowe:

$$x_j = f_j(x_1, \ldots, x_g) \in R_v[[x_1, \ldots, x_g]].$$

Redukcja modulo $\mathcal{M}_v$ da nam:

$$\tilde{x}_j = \tilde{f}_j(\tilde{x}_1, \ldots, \tilde{x}_g),$$

gdzie $\tilde{f}_j \in k(v)[[\tilde{x}_1, \ldots, \tilde{x}_g]]$ oraz $\tilde{x}_1, \ldots, \tilde{x}_g$ są parametrami lokalnymi wokół $\tilde{e}$ w $\tilde{A}$. Wówczas odwzorowanie:

$$\phi : (X_1, \ldots, X_g) \mapsto (X_1, \ldots, X_g, f_{g+1}(X_1, \ldots, X_g), \ldots, f_n(X_1, \ldots, X_g))$$

jest odwzorowaniem różnowartościowym (wystarczy porównać pierwszych g współrzednych) oraz homomorfizmem, co wynika z zastosowania konstrukcji grupy formalnej stowarzyszonej z rozmaitością A.

Odwzorowanie ψ określamy jako projekcję:

$$\psi : (x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_g).$$

Jeśli $\psi(x_1, \ldots, x_n) = \psi(y_1, \ldots, y_n)$, to $x_i = y_i$ dla $1 \leq i \leq g$ i z definicji $A_1(K_v)$ wynika, że $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in U$, a stąd $x_1, \ldots, x_g$ są parametrami lokalnymi i $x_j = f_j(x_1, \ldots, x_g)$ dla $g+1 \leq j \leq n$ i podobnie dla y_j. Zatem zachodzi równość $(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$, czyli ψ jest różnowartościowa, co kończy dowód twierdzenia. □

Twierdzenie 2.2.23. *Niech A będzie rozmaitością abelową zdefiniowaną nad ciałem liczbowym K i niech v będzie skończonym miejscem K, w którym A ma dobrą redukcję. Ciało reszt $\tilde{k}$ w v ma charakterystykę p, a włókno specjalne oznaczamy $\tilde{A}$. Wtedy dla każdego $m \geq 1$ takiego, że p nie dzieli m odwzorowanie redukcji:*

$$A[m](K) \to \tilde{A}(\tilde{k})$$

jest injekcją.

Dowód. Niech K będzie ciałem liczbowym i $v \in M_K^0$ miejscem dobrej redukcji dla A. Inkluzja $A(K) \subset A(K_v)$ pociąga $A[m](K) \subset A[m](K_v)$. Ciało reszt $k(v)$ ma charakterystykę $p \nmid m$. Wówczas jeśli $P \in A[m](K)$, to P nie należy do $A_1(K_v)$ na mocy Twierdzenia 2.2.22 i Stwierdzenia 2.2.20. Istnieje zatem naturalna inkluzja:

$$A[m](K) \hookrightarrow A[m](K_v) \hookrightarrow \tilde{A}(k(v)).$$

□

Teoria Kummera i rozszerzenia nierozgałęzione

W tym rozdziale dokończymy dowód "słabego" twierdzenia Mordella-Weila korzystając z teorii rozszerzeń nierozgałęzionych. Pokażemy, że roszerzenie L/K postaci $L = K(\{[m]^{-1}(x) : x \in A(K)\})$ jest Galois i skończonego stopnia.

Przyjmujemy ponadto konwencję, że zbiór waluacji S zawsze zawiera M_K^∞.

Definicja 2.2.24 (Rozszerzenie nierozgałęzione)**.** Niech dane będzie skończone rozszerzenie ciał L/K rozdzielcze oraz waluacja $w \in M_L^0$, która po ograniczeniu do K jest równa v. Rozszerzenie L/K nazywamy **nierozgałęzionym** w waluacji w jeżeli rozszerzenie ciał reszt $k(v)/k(w)$ jest rozdzielcze oraz zachodzi równość

$$[L_w : K_v] = [k(w) : k(v)].$$

Jeśli dane jest rozszerzenie Galois ciał liczbowych L/K oraz rozszerzenie waluacji $w|v$, $w \in M_L^0$ i $v \in M_K^0$, to można pokazać ([BG06, B.2.19]), że rozszerzenie uzupełnień L_w/K_v jest Galois, podobnie ciało reszt $k(w)/k(v)$ oraz istnieje surjektywny homomorfizm

$$\varepsilon : \mathrm{Gal}(L_w/K_v) \to \mathrm{Gal}(k(w)/k(v)).$$

Ponadto podgrupa $D \subset \mathrm{Gal}(L/K)$ elementów spełniających $\sigma(w) = w$ nazywa się **grupą dekompozycji** w nad v i jest ona izomorficzna z grupą $\mathrm{Gal}(L_w/K_v)$. Jądro wyżej zdefiniowanego homomorfizmy ε nazywamy **grupą inercji** i przez powyższe utożsamienia możemy identyfikować ją z pewną podgrupą w $Gal(L/K)$.

W szczególności rozszerzenie ciał liczbowych L/K jest nierozgałęzione dla $w|v$ wtedy i tylko wtedy, gdy grupa inercji dla $w|v$ jest trywialna.

Złożenie wszystkich skończonych rozszerzeń ciała K nierozgałęzionych w v (zawartych w $\overline{K}$) nazywać będziemy maksymalnym nierozgałęzionym rozszerzeniem K w v. Każde podrozszerzenie maksymalnego nierozgałęzionego rozszerzenia K nazywać będziemy nierozgałęzionym w v.

Twierdzenie 2.2.25. *Niech $m \geq 1$ będzie liczbą całkowitą i niech S zawiera zbiór miejsc, w których A ma złą redukcję oraz takich, które dzielą m. Wówczas dla wszystkich $x \in A(K)$ oraz y takich, że $[m](y) = x$ rozszerzenie $K(y)/K(x)$ jest nierozgałęzione poza S. Ponadto $L = K(\{[m]^{-1}(x) : x \in A(K)\})$ jest nierozgałęzione poza S.*

Dowód. Wybierzmy punkt $y \in A(\overline{K})$ taki, że $[m](y) = x$ i niech $K' = K(y)$. Niech ponadto v jest miejscem skończonym spoza S i w niech będzie dowolnym jego rozszerzeniem do K'. Rozważmy odwzorowanie redukcji:

$$A(K') \to \tilde{A}_w(k(w)').$$

Jeśli $\sigma \in \mathrm{Gal}(K'/K)$ należy do grupy dekompozycji w, to otrzymamy przez redukcję automorfizm $\tilde{\sigma} \in \mathrm{Gal}(k(w)'/k(v))$. Ponadto σ należy do grupy inercji dla w wtedy i tylko wtedy, gdy $\tilde{\sigma} = 1$. Przypuśćmy zatem, że σ należy do grupy inercji dla w. Wówczas $\tilde{\sigma}$ działa trywialnie na $\tilde{A}_w(k(w)')$ i $\tilde{\sigma}(\tilde{y}) = \tilde{y}$. Zachodzi zatem następujący ciąg równości:

$$\widetilde{t(\sigma, x)} = \widetilde{\sigma(y) - y} = \tilde{\sigma}(\tilde{y}) - \tilde{y} = \tilde{0}$$

z definicji t. Z poprzedniego twierdzenia wiemy, że m-torsja $A(K')$ odwzorowuje się injektywnie w $\tilde{A}_w(\tilde{K}'_w)$, ale z tego wynika, że:

$$t(\sigma, x) = 0.$$

W takim razie σ działa trywialnie na K', bo $\sigma(y) = y$, czyli $\sigma = 1$. Zatem grupa inercji dla w jest trywialna, czyli rozszerzenie K'/K jest nierozgałęzione w v. Z dowolności wyboru v i w dostajemy, że $K' = K(y)$ jest nierozgałęzione we wszystkich miejscach poza S. □

Lemat 2.2.26. *Niech ciało k zawiera pierwiastek pierwotny z jedynki stopnia m. Dla $\alpha \in k^\times$ definiujemy ciało $K := k(\sqrt[m]{\alpha})$ i wybieramy miejsce v w k nie dzielące m. Wówczas K/k jest nierozgałęzione w v wtedy i tylko wtedy, gdy $ord_v(\alpha) \equiv 0 (mod\ m)$.*

Dowód. Wprowadźmy upraszczające oznaczenie $\omega = \sqrt[m]{\alpha}$. Wyróżnik elementu ω wynosi $m^m \alpha^{m-1}$. Zatem wyróżnik ciała K/k dzieli $m^m \alpha^{m-1}$. Ponieważ $\mathrm{ord}_v(m) = 0$ z założenia, wiec jeśli $\mathrm{ord}_v(\alpha) = 0$, to K/k jest nierozgałęzione w v. Rozważmy teraz przypadek $\mathrm{ord}_v(\alpha) > 0$. Z jednej strony jeśli $\mathrm{ord}_v(\alpha) \equiv 0 (\mathrm{mod\ m})$, to istnieje $t \in \mathbb{N}$ takie, że $\mathrm{ord}_v(\alpha) = mt$. Wybierzmy uniformizator π dla v (tzn. $\mathrm{ord}_v(\pi) = 1$). Wówczas element $\beta = \alpha\pi^{-mt}$ ma $\mathrm{ord}_v(\beta) = 0$ i $K = k(\sqrt[m]{\alpha}) = k(\sqrt[m]{\beta})$ i z powyższego warunku K/k jest nierozgałęzione w v. W drugą stronę dowód przeprowadźmy przez kontrapozycję. Załóżmy, że $\mathrm{ord}_v(\alpha) \not\equiv 0 (\mathrm{mod\ m})$. Niech $r = \mathrm{ord}_v(\alpha)$ oraz $\mathfrak{p}$ niech będzie ideałem pierwszym w $\mathcal{O}_k$ odpowiadającym miejscu v. Wówczas:

$$\alpha\mathcal{O}_k = \mathfrak{p}^r\mathfrak{A}$$

dla pewnego ideału $\mathfrak{A}$ względnie pierwszego z $\mathfrak{p}$. Ideał $\mathfrak{p}$ rozłada się w $\mathcal{O}_K$ na iloczyn potęg ideałów pierwszych $\mathfrak{p}\mathcal{O}_K = \mathfrak{B}_1^{e_1} \cdots \mathfrak{B}_s^{e_s}$. Wówczas:

$$\alpha\mathcal{O}_K = \mathfrak{B}_1^{re_1} \cdots \mathfrak{B}_s^{re_s}\mathfrak{A}'$$

jest rozkładem (α), gdzie ideał $\mathfrak{A}'$ jest względnie pierwszy z $\mathfrak{B}_i^{re_i}$. Skoro $\alpha = \omega^m$, to $m | re_i$ dla wszystkich $1 \leq i \leq s$. Ale z założenia $m \nmid r$, więc $e_i \geq 2$, czyli K/k jest rozgałęzione w v. □

Wniosek 2.2.27. *Niech k będzie ciałem liczbowym i $\mu_m \subset k$ oraz S zawiera wszystkie miejsca dzielące m i takie, że pierścień $\mathcal{O}_{k,S}$ liczb S-całkowitych w k jest dziedziną ideałów głównych. Niech K będzie maksymalnym abelowym rozszerzeniem k o wykładniku m, które jest nierozgałęzione we wszystkich miejscach $v \notin S$. Wtedy:*

- $K = k((\mathcal{O}_{k,S})^{\frac{1}{m}})$=*(ciało powstałe przez dołączenie wszystkich pierwiastków stopnia m z elementów $\mathcal{O}_{k,S}^{\times}$).*
- *Ciało K jest skończonym rozszerzeniem Galois ciała k i*

$$Gal(K/k) \cong (\mathbb{Z}/m\mathbb{Z})^{1+r(S)},$$

gdzie $r(S)$ jest rangą grupy jedności $\mathcal{O}_{k,S}^{\times}$.

Dowód. Niech $K' = k((\mathcal{O}_{k,S})^{\frac{1}{m}})$. Ponieważ dla dowolnego $v \notin S$ $\mathrm{ord}_v(\sqrt[m]{\alpha}) = 0$ dla $\alpha \in \mathcal{O}_{k,S}^{\times}$ (co wynika z definicji $\mathcal{O}_{k,S}^{\times}$), więc na podstawie poprzedniego lematu $K' \subset K$. Z teorii Kummera wiemy, że K jest złożeniem rozszerzeń postaci $k(\sqrt[m]{\alpha})$ i z poprzedniego lematu możemy przyjąć, że $\mathrm{ord}_v(\alpha) \equiv 0(\mathrm{mod\ m})$ dla wszystkich $v \notin S$ ($\mathrm{ord}_v(\alpha) = mr_v$ dla pewnego r_v), a ponadto α jest liczbą algebraiczną całkowitą. Niech $v \notin S$ i $\mathfrak{p}_v$ będzie ideałem pierwszym odpowiadającym v w $\mathcal{O}_{k,S}$. Wówczas ideał

$$\prod_{v \notin S} \mathfrak{p}_v^{r_v}$$

jest ideałem głównym o generatorze β (ponieważ $\mathcal{O}_{k,S}$ jest dziedziną ideałów głównych z założenia). Element $\alpha' = \alpha\beta^{-m}$ należy do $\mathcal{O}_{k,S}$ i $\mathrm{ord}_v(\alpha') = 0$ dla wszystkich $v \notin S$ i $\alpha' \in \mathcal{O}_{k,S}$. Zatem $k(\sqrt[m]{\alpha}) \subset K'$ i złożenie K rozszerzeń $k(\sqrt[m]{\alpha})$ również zawiera się w K'. Wówczas odwzorowanie dwuliniowe:

$$\phi : Gal(K/k) \times \mathcal{O}_{k,S}^{\times}/(\mathcal{O}_{k,S}^{\times})^m \to \mu_m$$

jest niezdegenerowanym odwzorowaniem dwuliniowym. Zatem:

$$Gal(K/k) \hookrightarrow Hom(\mathcal{O}_{k,S}^{\times}/(\mathcal{O}_{k,S}^{\times})^m, \mu_m)$$

jest grupą skończoną na mocy twierdzenia Dirichleta o S-jednościach. Ponadto $Hom(\mathcal{O}_{k,S}^{\times}/(\mathcal{O}_{k,S}^{\times})^m, \mu_m) \cong \mathcal{O}_{k,S}^{\times}/(\mathcal{O}_{k,S}^{\times})^m$ i skoro obie grupy w dziedzine ϕ są skończone, to

$$Gal(K/k) \cong \mathcal{O}_{k,S}^{\times}/(\mathcal{O}_{k,S}^{\times})^m.$$

□

Uwaga 2.2.28. Skoro grupa klas pierścienia $\mathcal{O}_{k,S}$ jest skończona, to powiększając S o skończoną liczbę miejsc v odpowiadających klasom reprezentantów ideałów pierwszych w grupie klas $\mathcal{O}_{k,S}$ zawsze możemy uzyskać takie skończone S, że $\mathcal{O}_{k,S}$ będzie dziedzina ideałów głównych.

Dowód Twierdzenia 2.2.3. Ciało $L = K(\{[m]^{-1}(x) : x \in A(K)\})$ jest rozszerzeniem Galois ciała K i na mocy Twierdzenia 2.2.25 jest nierozgałęzione. Ponadto grupa $\mathrm{Gal}(L/K)$ ma wykładnik m i jest abelowa na mocy Twierdzenia 2.2.7. Zatem na mocy Wniosku 2.2.27 rozszerzenie L jest skończone i dalej Twierdzenie 2.2.7 pociąga, że grupa $A(K)/mA(K)$ jest skończona. □

2.3 Twierdzenie Mordella-Weila nad ciałami skończenie generowanymi

Celem tego paragrafu jest szkicowe opisanie metody dowodu uogólnienia twierdzenia Mordella-Weila, które pochodzi z pracy [Kah09]. Niech K będzie ciałem skończenie generowanym nad swoim ciałem pierwszym. Wówczas grupa punktów K-wymiernych rozmaitości abelowej A/K jest skończenie generowana. W rzeczywistości udowodnimy nieco silniejsze stwierdzenie. Do jego sformułowania potrzebujemy dodatkowe definicje.

Definicja 2.3.1 (Rozszerzenia liniowo niezależne)**.** Niech E, F będą rozszerzeniami ciała K. Wówczas E, F są **liniowo niezależne** wtedy i tylko wtedy, gdy dowolne elementy $x_1, \ldots, x_n \in E$ liniowo niezależne nad K są liniowo niezależne nad F oraz, gdy dowolne elementy $x_1, \ldots, x_n \in F$ liniowo niezależne nad K są liniowo niezależne nad E.

Definicja 2.3.2 (Rozszerzenie regularne ciał)**.** Rozszerzenie ciał L/K jest **regularne** jeśli domknięcie algebraiczne $\overline{K}$ ciała K jest liniowo niezależne od L nad ciałem K.

Wniosek 2.3.3. *Rozszerzenie K/F skończenie generowane nad swoim ciałem pierwszym F jest regularne.*

Twierdzenie 2.3.4 ([Con06, Thm.6.2])**.** *Niech A/K będzie rozmaitością abelową i K/k rozszerzeniem regularnym ciał. Istnieje para (A_0, τ_0), gdzie A_0 jest rozmaitością abelową nad k, a odwzorowanie τ_0 jest morfizmem rozmaitości abelowych nad K:*

$$\tau : A_0 \times_{Spec(k)} Spec(K) \to A$$

o następującej własności: jeśli dana jest para (B, f): B - rozmaitość abelowa nad k i morfizm rozmaitości abelowych nad K:

$$f : B_K \to A,$$

to istnieje jedyny morfizm $f^* : B \to A_0$ rozmaitości abelowych nad k spełniający:

$$\tau_0 \circ f^* = f.$$

Definicja 2.3.5 (K/k-ślad)**.** Parę (A_0, τ_0) określoną w poprzednim twierdzeniu nazywamy **K/k śladem** rozmaitości A i oznaczamy $(\mathrm{Tr}_{K/k}(A), \tau)$.

Zachodzi zatem następujące uogólnienie Twierdzenia 2.2.1.

Twierdzenie 2.3.6 ([LN59])**.** *Niech A będzie rozmaitością abelową nad ciałem K, które jest rozszerzeniem regularnym ciała k. Wówczas grupa $A(K)/\tau(Tr_{K/k})(k)$ jest skończenie generowana.*

Wniosek 2.3.7 (Twierdzenie Mordella-Weila dla ciał skończenie generowanych)**.** *Niech A/K będzie rozmaitością abelową nad ciałem K skończenie generowanym nad swoim ciałem pierwszym. Wówczas grupa $A(K)$ jest skończenie generowaną grupą abelową.*

Dowód. Z definicji $K = F(t_1, \ldots, t_n)$, gdzie t_i transcendentne nad F oraz $[F : \mathbb{Q}] < \infty$ lub $[F : \mathbb{F}_p] < \infty$ dla pewnej liczby pierwszej p. Rozszerzenie K/F jest regularne i na mocy Twierdzenia 2.3.4 grupa $A(K)/\tau(\mathrm{Tr}_{K/F}(A))(F)$ jest skończenie generowana. Na mocy Twierdzenia 2.2.1 grupa $\tau(\mathrm{Tr}_{K/F}(A))(F)$ jest skończenie generowana jeśli F jest ciałem liczbowym. W przypadku, gdy F jest ciałem skończonym grupa ta nawet jest skończona. Zatem $A(K)$ jest grupą skończenie generowaną. □

Podamy teraz wzorując się na [Kah09] szkic dowodu Twierdzenia 2.3.6.

Dowód. Dla ułatwienia notacji będziemy utożsamiać obraz $\tau(\mathrm{Tr}_{K/k}(A))$ z rozmaitością $\mathrm{Tr}_{K/k}(A)$.

W dowodzie używać będziemy oznaczenia $\mathrm{Pic}(\mathcal{A})$ na grupę snopów odwracalnych zdefiniowaną w [Har06, II,Sec.6]. Podobna uwaga dotyczy grupy $\mathrm{NS}(\mathcal{A})$. Z własności śladu $\mathrm{Tr}_{K/k}(A)$ wystarczy udowodnić twierdzenie dla ciała k algebraicznie domkniętego (patrz [Con06, Lem. 7.3]). Ponadto wystarczy udowodnić twierdzenie dla rozmaitości $\widehat{A} = \mathrm{Pic}^0(A)$ dualnej do rozmaitości A (wystarczy zauważyć, że obie rozmaitości są izogeniczne, zatem rangi ich grup punktów K-wymiernych są takie same). Skończona generowalność grupy Nérona-Severiego $\mathrm{NS}(A)$ (patrz [BG71, Exp. XIII, Thm.5.1]) oraz krótki ciąg dokładny (wynikający z Definicji 4.2.24) i równość $\mathrm{Pic}^0(A) = \widehat{A}$:

$$0 \to \mathrm{Pic}^0(A) \to \mathrm{Pic}(A) \to \mathrm{NS}(A) \to 0$$

pociągają, że $\widehat{A}(K)/\mathrm{Tr}_{K/k}(\widehat{A})(k)$ jest skończenie generowana wtedy i tylko wtedy, gdy grupa $\mathrm{Pic}(A)/\mathrm{Tr}_{K/k}(\widehat{A})(k)$ jest skończenie generowana.

Ponadto dla ciała K skończenie generowanego nad k istnieje jego model gładki X/k, tzn. rozmaitość gładka nad k, której ciało funkcji wymiernych jest równe K. Model X można wybrać tak, że A przedłuża się do schematu abelowego $p : \mathcal{A} \to X$ nad X. Włókno $\mathcal{A}_\eta = A$ i istnieje kanoniczny monomorfizm $j : \mathcal{A}_\eta \to \mathcal{A}$, co wynika z faktu, że $\mathrm{Spec}(k(\eta)) \to X$ jest monomorfizmem i z własności produktu rozwłóknionego (por. Definicja 4.1.9).

Istnieje następujący diagram przemienny:

$$\begin{array}{ccccccc}
\Gamma(A, \mathbb{G}_m) & \longrightarrow & \bigoplus_{x \in (\mathcal{A}-A)^{(1)}} \mathbb{Z} & \longrightarrow & \mathrm{Pic}(\mathcal{A}) & \xrightarrow{j^*} & \mathrm{Pic}(A) \longrightarrow 0 \\
\sim\uparrow & & \sim\uparrow & & p^*\uparrow & & \uparrow \\
K^* & \longrightarrow & \bigoplus_{x \in X^{(1)}} \mathbb{Z} & \longrightarrow & \mathrm{Pic}(X) & \longrightarrow & 0
\end{array}$$

Ponadto istnieje sekcja $\Psi : X \to \mathcal{A}$, której odpowiada identyczność na każdym włóknie $\mathcal{A}_v$. Z definicji sekcji zachodzi równość $p \circ \Psi = \mathrm{id}_X$. Niech $\mathcal{L} \in \mathrm{Pic}(X)$ oraz $p^*(\mathcal{L}) = 0 \in \mathrm{Pic}(\mathcal{A})$. Wówczas funktorialność operacji $(\cdot)^*$ implikuje:

$$\mathcal{L} = (\mathrm{id}_X)^*(\mathcal{L}) = (p \circ \Psi)^*(\mathcal{L}) = \Psi^* \circ p^*(\mathcal{L}) = \Psi^*(0) = 0.$$

Powyższy diagram przemienny oraz istnienie sekcji implikują istnienie następującego ciągu dokładnego:

$$0 \to \mathrm{Pic}(X) \xrightarrow{p^*} \mathrm{Pic}(\mathcal{A}) \xrightarrow{j^*} \mathrm{Pic}(A) \to 0.$$

Następnie należy zauważyć, że grupa cykli algebraicznie równoważnych zeru $A^{(1)}(\mathcal{A}) \subset \mathrm{Pic}(\mathcal{A})$. Grupa $A^{(1)}$ pochodzi z ciągu dokładnego:

$$0 \to A^{(1)}(\mathcal{A}) \to \mathrm{Pic}(\mathcal{A}) \to \mathrm{NS}(\mathcal{A}) \to 0.$$

Z kolei argument [Kah09, Lm. 1.2] pokazuje, że $j^*A^{(1)}(\mathcal{A}) \subset \mathrm{Tr}_{K/k}(\widehat{A})(k)$. To pociąga istnienie surjekcji:

$$\mathrm{NS}(\mathcal{A}) \twoheadrightarrow \mathrm{Pic}(A)/\mathrm{Tr}_{K/k}(\widehat{A})(k).$$

Skończona generowalność grupy $\mathrm{NS}(\mathcal{A})$ implikuje tezę twierdzenia. □

2.4 Grupa Selmera i Szafarewicza-Tate'a

W tym paragrafie pokażemy w jaki sposób można przeformułować Twierdzenie 2.2.1 w języku kohomologii Galois. Dzięki temu uzyskamy dwie grupy, które pozwolą nam później precyzyjnie zdefiniować przeszkodę w konstrukcji efektywnego algorytmu znajdującego generatory grupy Mordella-Weila rozmaitości abelowej A nad ciałem liczbowym.

Niech K będzie ustalonym ciałem liczbowym oraz

$$G = Gal(\overline{K}/K) = \varprojlim_{L/K} Gal(L/K)$$

absolutną grupą Galois z topologią proskończoną zadaną przez granicę odwrotną po rozszerzeniach L/K skończonych i Galois. Niech $A[m]$ będzie grupą m-torsyjnych punktów w $A(\overline{K})$. Przez $H^1(G, A[m])$ będziemy oznaczali pierwszą grupę kohomologii grupy G działającej na module $A[m]$.

Odwzorowanie Kummera z Twierdzenia 2.2.7 indukuje:

$$t(\cdot, y) : G \to A[m] : \sigma \mapsto y^\sigma - y,$$

gdzie $y \in A(\overline{K})$ oraz $my \in A(K)$. Zachodzi ponadto równość:

$$t(\sigma\sigma', y) = t(\sigma', y)^\sigma + t(\sigma, y)$$

oraz jeśli $my = my'$, to $t(\sigma, y) - t(\sigma, y') = b^\sigma - b$ dla $b = y - y' \in A[m]$. Zatem dostajemy dobrze określone odwzorowanie:

$$\delta : A(K) \to H^1(G, A[m]) : x = my \mapsto t(\cdot, y),$$

gdzie klasa odwzorowania $t(\cdot, y)$ nie zależy od wyboru y spełniającego $x = my$.

Powyższa konstrukcja daje się uogolnić do przypadku dowolnej niezerowej izogenii $\alpha : A \to B$ (patrz Definicja 4.2.19) nad K dowolnych rozmaitości abelowych A, B nad ciałem liczbowym K (a nawet nad dowolnym ciałem doskonałym, tj. takim, że $\overline{K^{sep}} = K^{sep}$).

Twierdzenie 2.4.1. *Niech $\alpha : A \to B$ będzie izogenią (niezerową, zdefiniowaną nad K). Krótki ciąg dokładny grup:*

$$0 \to \ker(\alpha) \xrightarrow{\iota} A(\overline{K}) \xrightarrow{\alpha} B(\overline{K}) \to 0$$

indukuje krótki ciąg dokładny:

$$0 \to B(K)/\alpha A(K) \xrightarrow{\delta} H^1(G, \ker(\alpha)) \xrightarrow{\iota} H^1(G, A(\overline{K}))[\alpha] \to 0.$$

Wybieramy reprezenanta $x \in B(K)$ klasy w $B(K)/\alpha A(K)$ oraz $y \in A(\overline{K})$ takie, że $\alpha(y) = x$. Wówczas:

$$\delta(x) : G \to \ker(\alpha)$$

$$\delta(x)(\sigma) = y^\sigma - y.$$

W szczególności odwzorowanie jest poprawnie określone (nie zależy od wyboru y ani reprezenanta ustalonej klasy w $B(K)/\alpha A(K)$).

Dowód. Dowód wynika z funktorialnych własności kohomologii grup oraz istnienia długiego ciągu dokładnego dla kohomologii, patrz [Wei94, Chapter 6] oraz [HS00, C.4]. □

Ograniczając się ponownie do ciał liczbowych dla waluacji $v \in M_K$ ustalamy jej rozszerzenie do waluacji na $\overline{K}$ i ustalamy zanurzenie $\overline{K} \subset \overline{K}_v$, które indukuje zanurzenie grup

$$G_v = \mathrm{Gal}(\overline{K}_v/K_v) \subset \mathrm{Gal}(\overline{K}/K)$$

oraz $A(\overline{K}) \subset A(\overline{K}_v)$ dla rozmaitości A nad ciałem K. Analogicznie do Twierdzenia 2.4.1 dostajemy ciągi dokładne dla grup G_v, które implikują istnienie diagramu przemiennego:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & B(K)/\alpha A(K) & \xrightarrow{\delta} & H^1(G, \ker(\alpha)) & \longrightarrow & H^1(G, A(\overline{K}))[\alpha] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \prod_{v \in M_K} B(K_v)/\alpha A(K_v) & \xrightarrow{\delta_v} & \prod_{v \in M_K} H^1(G_v, \ker(\alpha)) & \to & \prod_{v \in M_K} H^1(G_v, A(\overline{K}_v))[\alpha] & \to & 0
\end{array}$$

Definicja 2.4.2 (Grupa Selmera, grupa Szafarewicza-Tate'a)**.** Niech $\alpha : A \to B$ będzie izogenią nad K (ciało liczbowe) dwóch rozmaitości abelowych A i B. **Grupą Selmera** rozmaitości A stowarzyszoną z α nazywamy:

$$Sel^{(\alpha)}(A/K) := \bigcap_v \ker\left\{H^1(G, \ker(\alpha)) \to H^1(G_v, A(\overline{K}_v))[\alpha]\right\}.$$

Z kolei **grupą Szafarewicza-Tate'a** rozmaitości A jest:

$$Ш(A/K) := \bigcap_v \ker\left\{H^1(G, A(\overline{K})) \to H^1(G_v, A(\overline{K}_v))\right\}.$$

Powyższy diagram przemienny oraz definicja grup $Sel^{(\alpha)}$ oraz Ш pozwalają określić następujący ciąg dokładny:

$$0 \to B(K)/\alpha A(K) \to Sel^{(\alpha)}(A/K) \to Ш(A/K)[\alpha] \to 0. \tag{2.20}$$

Definicja 2.4.3 (Nierozgałęziona klasa)**.** Niech K będzie ciałem i niech M będzie $G_{\overline{K}/K} = Gal(\overline{K}/K)$-modułem. Niech $v \in M_K^0$ będzie skończonym miejscem ciała K, a $I_v \subset G_{\overline{K}/K}$ grupą inercji dla v. Mówimy, że klasa $\xi \in H^1(G_{\overline{K}/K}, M)$ jest **nierozgałęziona w** v jeśli jej obcięcie do $H^1(I_v, M)$ jest klasą trywialną. Ponadto grupa I_v jest określona tylko z dokładnością do sprzężenia.

Definicja 2.4.4 (Grupa klas nierozgałęzionych)**.** Niech M będzie $G_{\overline{K}/K}$-modułem, a S niech będzie skończonym zbiorem miejsc zawierającym wszystkie miejsca w nieskończoności M_K^∞. Wówczas:

$$H_S^1(G_{\overline{K}/K}, M) = \{\phi \in H^1(G_{\overline{K}/K}, M) : \phi \text{ jest nierozgał. dla dow. } v \notin S\}.$$

Lemat 2.4.5 ([HS00, Prop. C.4.2])**.** *Niech M będzie skończonym $G_{\overline{K}/K}$ modułem oraz S będzie skończonym zbiorem miejsc zawierającym M_K^∞. Wówczas grupa*

$$H_S^1(G_{\overline{K}/K}, M)$$

jest skończona.

Wniosek 2.4.6 ([HS00, Prop. C.4.2])**.** *Niech $\alpha : A \to B$ będzie izogenią rozmaitości abelowych nad K. Niech S będzie skończonym zbiorem miejsc zawierającym M_K^∞ oraz miejsca złej redukcji dla A i B, a także miejsca dzielące stopień $deg(\alpha)$. Wówczas grupa Selmera*

$$Sel^{(\alpha)}(A/K) \subset H_S^1(G_{\overline{K}/K}, \ker(\alpha))$$

jest skończona.

Przestrzenie jednorodne

Grupę Selmera oraz Ш można zintepretować w terminach geometrycznych. Pokażemy, że w istocie grupa $H^1(Gal(\overline{K}/K), A(\overline{K}))$ jest w bijekcji ze zbiorem klas równoważności rozmaitości A' izomorficznych nad $\overline{K}$ z A.

Definicja 2.4.7 (Główna przestrzeń jednorodna, A-torsor)**.** Niech A będzie rozmaitością abelową nad ciałem K. **Główną przestrzenią jednorodną** dla A/K nazywamy rozmaitość X/K z K-morfizmem:

$$\mu : X \times A \to X,$$

który określa na zbiorze $X(\overline{K})$ działanie przechodnie (tzn. dla dowolnych $x, y \in X(\overline{K})$ istnieje $g \in A(\overline{K})$ takie, że $\mu(x, g) = y$) oraz wolne ($\mu(x, g) = x$ wtedy i tylko wtedy, gdy $g = 0$). Ponadto morfizm μ spełnia własności:

(i) $\mu(x, 0) = x$ dla wszystkich $x \in X(\overline{K})$

(ii) $\mu(x, a + b) = \mu(\mu(x, a), b)$ dla $a, b \in A(\overline{K})$, $x \in X(\overline{K})$

(iii) Odwzorowanie $a \mapsto \mu(x, a)$ jest izomorfizmem nad $K(x)$ dla dowolnie ustalonego $x \in X(\overline{K})$.

Własności tego działania pozwalają określić odwzorowanie "odejmowania"

$$\nu : X \times X \to A \tag{2.21}$$

spełniające warunek $\mu(y, \nu(x, y)) = x$. Z faktu, że odejmowanie na rozmaitości abelowej jest morfizmem oraz własności (iii) z Definicji 2.4.7 wynika, że odwzorowanie ν jest morfizmem (patrz [HS00, C.5], [Sil86, Prop. 3.2]).

Dwie główne przestrzenie jednorodne (X, μ) oraz (X', μ') (dla rozmaitości abelowej A/K) są **izomorficzne nad K** jeśli istnieje K-izomorfizm $i : X \to X'$, który jest zgodny z μ, μ':

$$\begin{array}{ccc} X \times A & \xrightarrow{\mu} & X \\ {\scriptstyle i \times id_A}\downarrow & & \downarrow{\scriptstyle i} \\ X' \times A & \xrightarrow{\mu'} & X' \end{array}$$

Rysunek 2.1: Izomorfizm A-torsorów

Twierdzenie 2.4.8 ([HS00, Prop. C.5.3],[Sil86, Th. 3.6])**.** *Istnieje bijekcja pomiędzy zbiorem klas K-izomorfizmów głównych przestrzeni jednorodnych (w sensie Rysunku 2.1) oraz grupy $H^1(Gal(\overline{K}/K), A(\overline{K}))$:*

$$\Phi : Princ(A/K) \to H^1(Gal(\overline{K}/K), A(\overline{K})),$$
$$\Phi : [X] \mapsto [\sigma \mapsto \nu(\sigma(x), x)].$$

Odwzorowanie Φ nie zależy od wyboru reprezentanta klasy $[X]$ A-torsorów oraz wyboru $x \in X(\overline{K})$.

Przykład 2.4.9 ([Sil86, Example 3.7])**.** Niech K będzie ciałem i $\mathrm{char}(K) \neq 2$ oraz $K(\sqrt{d})/K$ będzie rozszerzeniem kwadratowym. Niech dana będzie krzywa eliptyczna E/K i punkt rzędu dwa $T \in E(K)$. Definiujemy 1-kocykl:

$$\xi : Gal(\overline{K}/K) \to E$$

$$\xi(\sigma) = \begin{cases} O & , \sigma(\sqrt{d}) = \sqrt{d} \\ T & , \sigma(\sqrt{d}) = -\sqrt{d} \end{cases} . \tag{2.22}$$

Skoro $T \in E(K)$, to możemy wybrać model Weierstrassa krzywej E postaci:

$$E : y^2 = x^3 + ax^2 + bx,$$

gdzie punktowi T odpowiada punkt 2-torsyjny $(0, 0)$. Niech dana będzie krzywa rzutowa $C \subset \mathbb{P}^3$, której część afiniczna jest izomorficzna z:

$$C_{\mathrm{aff}} : dw^2 = d^2 - 2adz^2 + (a^2 - 4b)z^4,$$

a punkty w nieskończoności dane są wzorami : $[0, 0, \pm\sqrt{\frac{a^2-4b}{d}}, 1]$. Krzywa C jest nieosobliwa dokładnie wtedy, gdy jej część afiniczna C_{aff} ma parami różne

pierwiastki (wielomian zmiennej z występujący po prawej stronie), co zachodzi dokładnie wtedy, gdy krzywa E jest nieosobliwa. Istnieje odwzorowanie biwymierne nad $K(\sqrt{d})$:

$$\phi : E \to C$$

$$\phi(x,y) = \left(\frac{\sqrt{d}y}{x^2+ax+b}, \frac{\sqrt{d}(x^2-b)}{x^2+ax+b} \right).$$

Odwzorowanie do niego odwrotne dane jest wzorem:

$$\phi^{-1} : C \to E$$

$$\phi^{-1}(z,w) = \left(\frac{\sqrt{d}w - az^2 + d}{2z^2}, \frac{dw - a\sqrt{d}z^2 + d\sqrt{d}}{2z^3} \right).$$

Na mocy [Sil86, II,Cor.2.4.1] odwzorowanie ϕ jest izomorfizmem, bo krzywe C i E są nieosobliwe.

Na koniec należy pokazać, że istotnie znaleziona krzywa odpowiada skonstruowanemu wcześniej kocyklowi ξ. Odwzorowanie:

$$\mu : C \times E \to C$$

$$\mu(p,P) = \phi(\phi^{-1}(p) + P)$$

spełnia warunki Definicji 2.4.7. Na mocy Twierdzenia 2.4.8 możemy wybrać dowolny punkt $p \in C$ i wówczas kocykl:

$$\sigma \mapsto \nu(p^\sigma, p) = \phi^{-1}(p^\sigma) - \phi^{-1}(p)$$

jest określony na mocy definicji μ oraz odwzorowania ν określonego w (2.21). Biorąc na przykład $p = (0, \sqrt{d})$ sprawdzamy, że:

$$\phi^{-1}(0, -\sqrt{d}) = (0,0)$$

$$\phi^{-1}(0, \sqrt{d}) = \mathcal{O}.$$

Jeśli zachodzi $\sigma(\sqrt{d}) = \sqrt{d}$, to $\nu(p^\sigma, p) = \mathcal{O}$. W przeciwnym przypadku, gdy $\sigma(\sqrt{d}) = -\sqrt{d}$, to $\nu(p^\sigma, p) = T$. Zatem skonstruowany kocykl dokładnie odpowiada kocyklowie ξ zdefiniowanemu na początku przykładu, czyli z dokładnością do izomorfizmu głównych przestrzeni jednorodnych C odpowiada kocyklowi ξ w sensie bijekcji z Twierdzenia 2.4.8.

2.5 Hipoteza Bircha-Swinnertona-Dyera

W poniższym paragrafie przedstawimy związek między rangą grupy $A(K)$ punktów K-wymiernych na rozmaitości abelowej A nad ciałem liczbowym a rzędem znikania pewnej funkcji holomorficznej, która "koduje" w pewnym sensie informację o arytmetyce punktów wymiernych na rozmaitości A. Związek ten poza nielicznymi udowodnionymi przypadkami jest wciąż przedmiotem intensywnych badań.

Jako pierwsi istnienie takiego związku między ranga grupy $E(\mathbb{Q})$ krzywej eliptycznej $E/\mathbb{Q}$ oraz rzędem znikania L-funkcji $L(E/\mathbb{Q})$ określonej poniżej

określili Birch i Swinnerton-Dyer w pracy [BSD65]. Przyczynkiem do sformułowania hipotezy była następująca prosta obserwacja: jeśli dana jest krzywa eliptyczna $E/\mathbb{Q}$, to istnienie nieskończenie wielu punktów wymiernych w $E(\mathbb{Q})$ powinno powodować, że dla (prawie) dowolnie wybranej liczby pierwszej p liczba punktów w $\tilde{E}(\mathbb{F}_p)$ przy założeniu, że krzywa E (a dokładniej równanie Weierstrassa ją definiujące) dobrze redukuje się modulo p, musi być relatywnie duża w stosunku do liczby elementów ciała $\mathbb{F}_p$. Sugeruje to rozważenie następującej funkcji:

$$f(x) = \prod_{\substack{p \leq x \\ E \text{ ma dobrą} \\ \text{red. w } p}} \frac{N_p}{p},$$

gdzie $N_p = \#E(\mathbb{F}_p)$ jest liczbą elementów w grupie nad $\mathbb{F}_p$. Obliczenia poczynione w pracy [BSD65] sugerują, że jeśli r jest rangą grupy $E(\mathbb{Q})$, to zachodzi równość.

Hipoteza 2.5.1 (Hipoteza Bircha-Swinnertona-Dyera, sformułowanie I)**.**

$$\lim_{x \to \infty} \frac{f(x)}{\log(x)^r} = C \in \mathbb{R}$$

Stała C jest pewnym nieznanym czynnikiem skalującym.

Co ciekawe, w pracy [BSD65] zasugerowany jest związek (formalny) między funkcją $f(x)$ a funkcją :

$$Z_{E,p}(u) = \exp\left(\sum_{i=1}^{\infty} \frac{N_{E,p^i} u^i}{i}\right)$$

określoną przez E. Artina i A. Weila. Liczba N_{E,p^i} określa liczbę punktów na zredukowanej krzywej $\tilde{E}$ nad ciałem $\mathbb{F}_{p^i}$. Można pokazać, że tak określona funkcja jest zbieżna w pewnym dysku analitycznym wokół $u = 0$. Co więcej, ma ona następującą równoważną postać:

$$Z_{E,p}(u) = \frac{1 - (N_p - p - 1)u + pu^2}{(1-u)(1-pu)}.$$

Podstawiając za $u = p^{-s}$, gdzie $s \in \mathbb{C}$ otrzymamy funkcję:

$$\zeta_{E,p}(s) = Z_{E,p}(p^{-s})$$

i biorąc iloczyn po wszystkich p dobrej redukcji dla E otrzymamy:

$$\zeta_E = \prod_p \zeta_{E,p}(s) = \frac{\zeta(s)\zeta(s-1)}{L_E(s)}.$$

Funkcja $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ jest zetą Riemanna. Funkcja $L_E(s)$ zadana jest wzorem:

$$L_E(s) = \prod_p (1 + (N_p - p - 1)p^{-s} + p^{1-2s})^{-1}.$$

Zbieżność tego iloczynu w ogólności zachodzi tylko dla $Re(s) > \frac{3}{2}$, a wynika to z uzyskanego przez H. Hasse oszacowania $|N_p - p - 1| \leq 2\sqrt{p}$ oraz z faktu, że

jeśli $\sum_n |b_n|$ jest zbieżny, to $\prod_n (1+b_n)$ jest zbieżny. Formalnie, gdyby iloczyn miał sens dla $s=1$ otrzymalibyśmy:

$$L_E(s) = \prod_p \left(\frac{N_p}{p}\right)^{-1},$$

gdzie iloczyn jest wzięty po liczbach pierwszych p dobrej redukcji dla E.

Powyższa heurystyka oraz dalsze obliczenia pozwoliły postawić następującą hipotezę.

Hipoteza 2.5.2 (Hipoteza Bircha-Swinnertona-Dyera, sformułowanie II)**.** *Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną oraz niech $r = ranga(E(\mathbb{Q}))$. Jeśli założymy, że funkcja $L_E(s)$ posiada przedłużenie analityczne na całe $\mathbb{C}$, to wówczas:*

$$ord_{s=1} L_E(s) = r.$$

Można pokazać (patrz [KM05]), że sformułowanie I i II są ze sobą równoważne.

Teraz podamy przeformułowanie powyższej hipotezy II dla rozmaitości abelowych, które pochodzi od Tate'a.

Niech dana będzie pewna rozmaitość abelowa A wymiaru g nad ciałem liczb wymiernych $\mathbb{Q}$ oraz pewna liczba pierwsza l. Ciąg grup

$$A[l^k] = \left\{P \in A(\overline{\mathbb{Q}}) : [l^k]P = \mathcal{O}\right\}$$

definiuje system odwrotny:

$$A[l^{i+1}] \to A[l^i] : P \mapsto [l]P,$$

którego granicę odwrotną

$$T_l(A) = \lim_{\leftarrow} A[l^k]$$

nazywamy **modułem Tate'a** rozmaitości abelowej A na liczbie pierwszej l. Twierdzenie 4.2.21 implikuje, że $A[l^k] \cong (\mathbb{Z}/l^k\mathbb{Z})^{2g}$. Stąd otrzymujemy izomorfizm:

$$T_l(A) = \lim_{\leftarrow} A[l^k] \cong \lim_{\leftarrow} (\mathbb{Z}/l^k\mathbb{Z})^{2g} \cong \mathbb{Z}_l^{2g}.$$

Dodawanie na rozmaitości abelowej A jest określone nad $\mathbb{Q}$, zatem grupa Galois $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ w naturalny sposób działa na elementach z $A[l^k]$. Indukuje to naturalne działanie również na module Tate'a. Ponadto biorąc iloczyn tensorowy z $\otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ dostajemy przestrzeń liniową:

$$V_l(A) = T_l(A) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l.$$

Element $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ działa na $((P_i)_{i\in\mathbb{N}}) \otimes x) \in V_l$ w następujący sposób:

$$\sigma((P_i)_{i\in\mathbb{N}} \otimes x) = (\sigma(P_i))_{i\in\mathbb{N}} \otimes x.$$

Otrzymamy w ten sposób ciągłą (ze względu na pro-skończoną topologię na $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ oraz indukowaną z $\mathbb{Q}_l$ topologię na $V_l(A)$) reprezentację

$$\rho_l : G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{Q}_l}(V_l(A)) \cong \mathrm{GL}_{2g}(\mathbb{Q}_l).$$

Krótki ciąg dokładny:

$$1 \to I_p \to D_p \to \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \to 1$$

dla ustalonej liczby pierwszej p daje nam rozkład grupy dekompozycji (dla ustalonego $\mathfrak{p}$ spełniającego $\mathfrak{p} \cap \mathbb{Z} = (p)$):

$$D_p = \{\sigma \in G_{\mathbb{Q}} : \sigma(\mathfrak{p}) = \mathfrak{p}\}.$$

Generator topologiczny grupy $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ oznaczany jako Frob_p działa następująco:

$$\mathrm{Frob}_p \mid_{\mathbb{F}_{p^k}} : \alpha \mapsto \alpha^p.$$

Istnieje zatem określony z dokładnością do wyboru ideału $\mathfrak{p}$ i z dokładnością do elementu z I_p automorfizm $\mathrm{Frob}_p \in G_{\mathbb{Q}}$, który przez reprezentację ρ_l działa na $V_l(A)^{I_p} = \{v \in V_l(A) : \rho_l(\sigma)(v) = v \text{ dla } \sigma \in I_p\}$ poprzez określony z dokładnością do sprzężenia element $\rho_l(\mathrm{Frob}_p) \in \mathrm{GL}_{2g}(\mathbb{Q}_l)$.

Niech l będzie ustaloną liczbą pierwszą. Wielomian charakterystyczny (dla ustalonego pierwszego $p \neq l$) elementu Frobeniusa $Frob_p$ ma postać:

$$\Phi_p(x) := \det\left(I_{2g} - \rho_l(\mathrm{Frob}_p) \mid_{V_l(A)^{I_p}} x\right).$$

Wielomian charakterystyczny jest dobrze określony dla elementów zadanych z dokładnością do sprzężenia. Zatem definicja powyżej jest jednoznaczna. Co więcej, André Weil pokazał, że wielomian charakterystyczny Φ_p nie zależy od wyboru liczby pierwszej $l \neq p$.

Definicja 2.5.3 (L-funkcja reprezentacji)**. L-funkcją stowarzyszoną z rozmaitością abelową** $A/\mathbb{Q}$ nazywamy funkcję postaci:

$$L(A/\mathbb{Q}, s) = \prod_p (\Phi_p(p^{-s}))^{-1}$$

Uwaga 2.5.4. Jeśli rozmaitość A ma dobrą redukcję w p, to:

$$\Phi_p(x) = \prod_{i=1}^{2g}(1 - \alpha_i x),$$

gdzie elementy $\alpha_i \in \overline{\mathbb{Q}}$ są co do modułu równe $|\alpha_i| = \sqrt{p}$. To pozwala oszacować iloczyn $L(A/\mathbb{Q}, s)$:

$$|L(A/\mathbb{Q}, s)| \leq \left(\prod_p \frac{1}{|1 - p^{1/2-\mathrm{Re}(s)}|}\right)^{2g} \leq \left(\zeta\left(\mathrm{Re}(s) - \frac{1}{2}\right)\right)^{2g}$$

Iloczyn $L(A/\mathbb{Q}, s)$ jest na mocy powyższych nierówności zbieżny dla $\mathrm{Re}(s) > \frac{3}{2}$ i jest funkcją holomorficzną.

Hipoteza 2.5.5. *L-funkcja $L(A/\mathbb{Q}, s)$ posiada przedłużenie analityczne na całą płaszczyznę $\mathbb{C}$. Ponadto istnieje liczba naturalna N (tak zwany **przewodnik**), podzielna przez wszystkie liczby pierwsze złej redukcji dla A i taka, że funkcja:*

$$\Lambda(A/\mathbb{Q}, s) = N^{s/2}((2\pi)^{-s}\Gamma(s))^{2g}L(A/\mathbb{Q}, s)$$

spełnia równanie funkcyjne:

$$\Lambda(A/\mathbb{Q}, 2-s) = \varepsilon\Lambda(A/\mathbb{Q}, s)$$

dla pewnego $\varepsilon \in \{-1, 1\}$.

Hipoteza jest prawdziwa dla krzywych eliptycznych nad $\mathbb{Q}$ oraz dla pewnych klas rozmaitości abelowych wyższych wymiarów (patrz [HS00, Conj.F.4.1.5]).

Możemy teraz sformułować ogólną postać hipotez I i II dla rozmaitości abelowych nad $\mathbb{Q}$.

Hipoteza 2.5.6 (Hipoteza Bircha-Swinnertona-Dyera, sformułowanie III)**.** *Niech* $A/\mathbb{Q}$ *będzie rozmaitością abelową. Jeśli* $L(A/\mathbb{Q}, s)$ *posiada przedłużenie analityczne do* $\mathbb{C}$*, to:*

$$ranga(A(\mathbb{Q})) = ord_{s=1}L(A/\mathbb{Q}, s).$$

Ponadto wielkość:

$$L^*(A/\mathbb{Q}, 1) := \lim_{s\to 1} \frac{L(A/\mathbb{Q}, s)}{(s-1)^{ranga(A(\mathbb{Q}))}}$$

wyraża się następującym wzorem:

$$L^*(A/\mathbb{Q}, 1) = \Omega_A \prod_p c_p \frac{\#Ш(A/\mathbb{Q}) \mid Reg(A/\mathbb{Q}) \mid}{\#A(\mathbb{Q})_{tors} \cdot \#\hat{A}(\mathbb{Q})_{tors}}.$$

(i) Wartość $\Omega_A = \left|\int_{A(\mathbb{R})} \eta_A\right|$*, gdzie* η_A *jest formą różniczkową stopnia* $\dim(A)$ *określoną w taki sposób, że ma skończoną niezerową redukcję na każdym włóknie modelu Nérona dla* A*.*

(ii) Liczby $c_p = [A(\mathbb{Q}_p) : A^0(\mathbb{Q}_p)]$ *są różne od jedynki tylko dla liczb* p *złej redukcji* A*, ponadto* $A^0(\mathbb{Q}_p)$ *jest podgrupą w* $A(\mathbb{Q}_p)$ *elementów, które przy redukcji mapują się do składowej spójności identyczności modelu Nérona* $A/\mathbb{Q}_p$*.*

(iii) Liczba $\#Ш(A/\mathbb{Q})$ *oznacza liczbę elementów w grupie* Ш *określonej w Definicji 2.4.2.*

(iv) Liczby $\#A(\mathbb{Q})_{tors}$ *i* $\#\hat{A}(\mathbb{Q})_{tors}$ *określają ilość elementów w grupie punktów torsyjnych na rozmaitości* A *i dualnej do niej rozmaitości* $\hat{A}$*.*

(v) Wartość $|Reg(A/\mathbb{Q})|$ *jest regulatorem stowarzyszonym z dywizorem Poincarégo* $\mathcal{P}$ *(patrz [HS00, Thm.7.3.4]), szerokim i symetrycznym na rozmaitości abelowej* $A\times\hat{A}$*. Dokładniej, istnieje wysokość kanoniczna* $\hat{h}_{A\times\hat{A},\mathcal{P}} : (A\times\hat{A})(\overline{\mathbb{Q}}) \to \mathbb{R}$ *i stowarzyszona z nią forma dwuliniowa* $\langle\cdot,\cdot\rangle_{\mathcal{P}}$*. Część beztorsyjna w* $A(\mathbb{Q})$ *generowana jest przez punkty* $P_1, \ldots, P_r$*, z kolei generatory części wolnej* $\hat{A}(\mathbb{Q})$ *są postaci* $P_1', \ldots, P_r'$ *(rozmaitości* A *i* $\hat{A}$ *są izogeniczne przez izogenię* $\lambda_D : A \to \hat{A}$ *stowarzyszoną z dowolnym szerokim dywizorem* $D \in Div(A)$*). Wówczas możemy określić następujące dwie liczby:*

$$Reg_D(A/\mathbb{Q}) = \det \mid (\langle P_i, P_j\rangle_D)_{1\le i,j\le r} \mid,$$

gdzie $\langle \cdot, \cdot \rangle_D$ *pochodzi od wysokości kanonicznej* $\hat{h}_{A,D}$ *oraz wielkość*

$$Reg(A/\mathbb{Q}) = \det \mid (\hat{h}_{A\times\hat{A},\mathcal{P}}(P_i, P_j^{'})_{1\leq i,j\leq r}) \mid .$$

Zachodzi między nimi związek:

$$Reg_D(A/\mathbb{Q}) = [\hat{A}(\mathbb{Q}) : \lambda_D(A(\mathbb{Q}))]Reg(A/\mathbb{Q}).$$

W szczególności widać, że wartość $L^*(A/\mathbb{Q}, 1)$ *została wybrana tak, aby nie zależała od wyboru szczególnej izogenii* λ_D *zależnej od szerokiego dywizora* D*. Z definicji jeśli ranga jest równa zero, to przyjmujemy, że wszystkie wyżej zdefiniowane regulatory są równe* 1*.*

W szczególności jeśli rozważamy hipotezę III w przypadku, gdy rozmaitość jest krzywą eliptyczną $E/\mathbb{Q}$, to $\hat{E}$ jest izomorficzna z E i w mianowniku wyrażenia $L^*(E/\mathbb{Q}, 1)$ pojawia się kwadrat $\#E(\mathbb{Q})_{tors}$.

Twierdzenie o istnieniu przedłużenia analitycznego (jednoznacznego) funkcji $L(E/\mathbb{Q}, s)$ (Wiles, Taylor, Conrad, Breuil, Diamond) pozwala szukać wzorów na rozwinięcie $L(E/\mathbb{Q}, s)$ w pewien szereg wokół 1. Z jednej strony mamy wzór dla $Re(s) > \frac{3}{2}$:

$$L(E/\mathbb{Q}, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_{p|\Delta} \frac{1}{1 - a_p p^{-s}} \prod_{p\nmid\Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}.$$

Ciąg $\{a_n\}$ określony jest przez rozwinięcie iloczynu (niech $a_p := p + 1 - N_p$): w szereg Dirichleta dla $Re(s) > \frac{3}{2}$. Funkcje $L_E(s)$ i $L(E/\mathbb{Q}, s)$ różnią się o czynniki pochodzące od $p \mid \Delta$, czynników dzielących wyróżnik krzywej (miejsc złej redukcji).

Zachodzi ponadto następujące twierdzenie.

Twierdzenie 2.5.7 (Lavrik)**.** *Niech* $E/\mathbb{Q}$ *będzie krzywą eliptyczną. Dla dowolnej liczby zespolonej* $s \in \mathbb{C}$ *istnieje rozwinięcie L-funkcji stowarzyszonej z* E*:*

$$L(E/\mathbb{Q}, s) = N^{-s/2}(2\pi)^s\Gamma(s)^{-1} \cdot \sum_{n=1}^{\infty}(a_n(F_n(s-1) + \varepsilon F_n(1-s))).$$

Liczba naturalna N *jest przewodnikiem krzywej eliptycznej określonym w Hipotezie 2.5.5. Ciąg* $\{a_n\}$ *określony jest powyżej,* ε *jest znakiem równania funkcyjnego* $\Lambda(2-s) = \varepsilon\Lambda(s)$*, natomiast funkcje* F_n *dane są wzorami:*

$$F_n(t) = \Gamma\left(t+1, \frac{2\pi n}{\sqrt{N}}\right)\left(\frac{\sqrt{N}}{2\pi n}\right)^{t+1},$$

$$\Gamma(z, \alpha) = \int_{\alpha}^{\infty} t^{z-1}e^{-t}dt,$$

$$\Gamma(z) = \Gamma(z, 0).$$

Przykład 2.5.8. Dana jest krzywa eliptyczna

$$E : y^2 = x^3 + 1$$

nad ciałem $\mathbb{Q}$. Izomorfizm $(x, y) \mapsto (x - 1, y)$ przekształca ją do postaci $y^2 = x^3 - 3x^2 + 3x$ i stosując metodę z Twierdzenia 3.1.1 można udowodnić, że ranga grupy $E(\mathbb{Q})$ jest równa zero, czyli $E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tors}}$. Ponadto Twierdzenie 2.2.23 implikuje, że $E(\mathbb{Q})_{\text{tors}} = \langle(2, 3)\rangle \cong \mathbb{Z}/6\mathbb{Z}$. Wyznaczamy następnie wartość liczb Tamagawy:

$$c_p = \begin{cases} 3 & p = 2 \\ 2 & p = 3 \\ 1 & \text{w p.p.} \end{cases}.$$

Regulator $Reg(E/\mathbb{Q}) = 1$ z definicji (ranga jest równa 0).

Forma Nérona przyjmuje dla $E : y^2 = x^3 + 1$ postać $\omega = \frac{dx}{2y}$. Zbiór $E(\mathbb{R}) = \{(x, y) \in \mathbb{R}^2 : y^2 = x^3 + 1\}$ ma jedną składową, po której całkujemy formę ω:

$$\Omega_E = \int_{E(\mathbb{R})} \omega = \int_{\infty}^{-1} \frac{dx}{-2\sqrt{x^3 + 1}} + \int_{-1}^{\infty} \frac{dx}{2\sqrt{x^3 + 1}} \approx 4.206546315976.$$

Obliczenie wartości $L(E, 1)$ za pomocą formuły Lavrika pozwala nam wyznaczyć hipotetyczny rząd grupy $Ш(E/\mathbb{Q}) = 1$:

$$L(E, 1) \approx 0.701091052662727$$

$$\#Sha(E/\mathbb{Q}) = \frac{L(E, 1)E(\mathbb{Q})^2_{tors}}{\Omega_E c_2 c_3 |\text{Reg}(E/\mathbb{Q})|} = 1.$$

Wynik ten jest istotnym wzmocnieniem Twierdzenia 2.4.6 zastosowanego do krótkiego ciągu dokładnego 2.20, gdzie pokazaliśmy tylko, że część $Ш(E/\mathbb{Q})[\alpha]$ należąca do jądra pewnej izogenii $\alpha : E \to E'$ jest skończenie generowana. Co więcej wyniki Casselsa i Tate'a sugerują, że nie tylko $Ш(E/\mathbb{Q})$ jest skończone, ale również rząd grupy jest zawsze kwadratem liczby całkowitej (poza 2-torsją).

Odnotujmy jeszcze dwa interesujące szczególne przypadki, gdy hipoteza Bircha-Swinnertona-Dyera jest prawdziwa lub, gdy potrafimy efektywnie obliczyć wartośc L-funkcji w jedynce.

Twierdzenie 2.5.9 (Tunell)**.** *Niech $E_n : y^2 = x^3 - n^2 x$ będzie krzywą eliptyczną nad $\mathbb{Q}$ dla ustalonego $n \in \mathbb{Z}$, wolnego od kwadratów. Wówczas:*

$$L(E_n/\mathbb{Q}, 1) = \frac{(r - 2s)^2 a\Omega}{16\sqrt{n}},$$

gdzie

$$a = \begin{cases} 1 & 2 \nmid n \\ 2 & 2 \mid n \end{cases}$$

oraz

$$r = \#\{(x, y, z) \in \mathbb{Z}^3 \mid x^2 + 2ay^2 + 8z^2 = n\},$$
$$s = \#\{(x, y, z) \in \mathbb{Z}^3 \mid x^2 + 2ay^2 + 32z^2 = n\},$$
$$\Omega = \int_1^{\infty} \frac{dx}{\sqrt{x^3 - x}} \approx 2.6220575543.$$

Twierdzenie 2.5.10 (Kolyvagin, 1990)**.** *Niech $E/\mathbb{Q}$ będzie krzywą eliptyczną. Wówczas jeśli*

$$ord_{s=1}L(E/\mathbb{Q}, s) \leq 1,$$

to zachodzi równość

$$ranga(E(\mathbb{Q})) = ord_{s=1}L(E/\mathbb{Q}, s).$$

3

Przykłady obliczania rang

W tym rozdziale przedstawimy przykłady obliczania rangi grupy Mordella-Weila rozmaitości abelowych i ich rodzin, które określone są nad ciałami liczbowymi. Część opisanych tutaj wyników pochodzi z pracy [Nas10]

3.1 Spadek metodą 2-izogenii

Bazując na obliczeniach przeprowadzonych w Przykładzie 2.4.9 pokażemy jak efektywnie obliczyć grupę Selmera $S^{(\phi)}$, gdzie $\phi : E \to E'$ jest izogenią stopnia 2 dla krzywych eliptycznych E, E' nad ciałem K:

$$E : y^2 = x^3 + ax^2 + bx$$

$$E' : Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X.$$

Morfizm ϕ dany jest wzorem:

$$\phi(x, y) = \left(\frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2} \right).$$

Ponadto istnieje morfizm $\widehat{\phi} : E' \to E$:

$$\widehat{\phi}(X, Y) = \left(\frac{Y^2}{4X^2}, \frac{Y((a^2 - 4b) - X^2)}{8X^2} \right),$$

który spełnia relacje $\phi \circ \widehat{\phi} = [2]$ oraz $\widehat{\phi} \circ \phi = [2]$, dając mnożenie przez 2 na krzywej E i E', odpowiednio. Sprawdzamy bezpośrednio, że $E[\phi] = \ker \phi = \{\mathcal{O}, (0, 0)\}$ i podobnie dla $\widehat{\phi}$ i E'.

Dla ustalonego zbioru waluacji S definiujemy grupę $K(S, 2) \subset K^\times / K^{\times 2}$ składającą się z elementów b, dla których $2 | ord_v(b)$ dla wszystkich $v \notin S$.

Twierdzenie 3.1.1 ([Sil86, Prop.4.9]). *Załóżmy, że zdefiniowane powyżej krzywe E oraz E' są określone nad ciałem doskonałym K. Niech $S = M_K^\infty \cup \{| \cdot |_\mathfrak{p} : \mathfrak{p} | (2b(a^2 - 4b))\}$ będzie zbiorem waluacji w nieskończoności oraz waluacji dyskretnych pochodzących od ideałów pierwszych w $\mathcal{O}_K$ dzielących wyróżnik $\Delta(E) = 16b^2(a^2 - 4b)$. Wówczas mamy krótki ciąg dokładny:*

$$0 \to E'(K)/\phi(E(K)) \xrightarrow{\delta} K(S, 2) \xrightarrow{c} Princ(E/K)[\phi], \tag{3.1}$$

gdzie:

$$\delta(P) = \begin{cases} 1 & P = \mathcal{O} \\ a^2 - 4b & P = (0,0) \\ X & P = (X,Y) \neq \mathcal{O}, (0,0) \end{cases},$$

$$c(d) = [C_d],$$

gdzie $[C_d]$ *jest klasą równoważności* K*-izomorficznych* E*-torsorów oraz:*

$$C_{d,aff} : dw^2 = d^2 - 2adz^2 + (a^2 - 4b)z^4.$$

Wówczas:

$$S^{(\phi)}(E/K) \cong \{d \in K(S,2) : C_{d,aff}(K_v) \neq \emptyset \text{ dla wszystkich } v \notin S\}.$$

Ponadto odwzorowanie:

$$\psi : C_{d,aff} \to E'$$

$$\psi(z,w) = \left(\frac{d}{z^2}, \frac{-dw}{z^3}\right)$$

dla $P \in C_{d,aff}(K)$ *spełnia warunek:*

$$\delta(\psi(P)) \equiv d (mod\ K^{*2}).$$

Dowód. Na początek zauważmy, że dana izogenia $\phi : E \to E'$ ma jądro $E[\phi] = \{\mathcal{O}, (0,0)\}$, które można identyfikować z dwuelementową grupą pierwiastków μ_2 z jedności stopnia 2. Niech $G = Gal(\overline{K}/K)$. Wówczas:

$$H^1(G, E[\phi]) \cong H^1(G, \mu_2)$$

oraz z krótkiego ciągu dokładnego:

$$1 \to \mu_2 \to \overline{K}^\times \xrightarrow{2} \overline{K}^\times \to 1$$

obliczając funktor kohomologii $H^\cdot(G, -)$ dostajemy długi ciąg dokładny. Na mocy 90. twierdzenia Hilberta (patrz [Wei94, Chapt.6]) $H^1(G_{\overline{K}/K}, \overline{K}^\times) = 0$. Zatem otrzymujemy krótki ciąg dokładny:

$$1 \to \mu_2 \to K^\times \xrightarrow{2} K^\times \xrightarrow{\delta} H^1(G_{\overline{K}/K}, \mu_2) \to 1.$$

Homomorfizm łączący δ dany jest wzorem:

$$\delta(x) = \{\sigma \mapsto \frac{\sigma(y)}{y}\}$$

dla dowolnie wybranego $y \in \overline{K}^\times$ takiego, że $x = y^2$.

Stosując ciąg dokładny (2.20) dla $\phi : E \to E'$ oraz korzystając z Wniosku 2.4.6 mamy, że:

$$S^{(\phi)}(E/K) \subset H^1_S(G_{\overline{K}/K}, E[\phi])$$

dla $S = M_K^\infty \cup \{|\cdot|_\mathfrak{p} : \mathfrak{p}|(2b(a^2 - 4b))\}$. Ponadto ze względu na izomorfizmy:

$$H^1(G, E[\phi]) \cong H^1(G, \mu_2) \cong K^\times / K^{\times 2}$$

($d \in K^\times/K^{\times 2}$ reprezentuje kocykl $\sigma \mapsto \frac{\sigma(\sqrt{d})}{\sqrt{d}}$ należący do grupy $H^1_S(G, E[\phi])$), Lemat 2.2.26 implikuje, że $d \in K(S,2)$. Mamy zatem izomorfizm:

$$H^1_S(G_{\overline{K}/K}, E[\phi]) \cong K(S,2).$$

W takim razie jeśli $d \in K(S,2)$, to odpowiada mu kocykl z Przykładu 2.4.9:

$$\xi(\sigma) = \begin{cases} O & ,\sigma(\sqrt{d}) = \sqrt{d} \\ T & ,\sigma(\sqrt{d}) = -\sqrt{d} \end{cases}. \tag{3.2}$$

Kocykl ξ na mocy Przykładu 2.4.9 jest (w sensie Twierdzenia 2.4.8) stowarzyszony z przestrzenią jednorodną C_d/K:

$$C_d : dw^2 = d^2 - 2adz^2 + (a^2 - 4b)z^4.$$

Zatem elementy $Sel^{(\phi)}(E/K)$ odpowiadają tym wartościom $d \in K(S,2)$, dla których $C_d(K_v) \neq \emptyset$ dla dowolnego $v \in S$.

Wyznaczymy teraz jawnie homomorfizm:

$$\delta : E'(K)/\phi(E(K)) \to H^1(G_{\overline{K}/K}, E[\phi]) \cong K^\times/K^{\times 2}.$$

Zgodnie z Twierdzeniem 2.4.1 możemy wybrać dla ustalonego $P \in E'(K)$ reprezentanta klasy w $E'(K)/\phi(E(K))$; dowolne $Q \in E(\overline{K})$ takie, że $\phi(Q) = P$. Rozważymy trzy oddzielne przypadki.

(i) $P = \mathcal{O}$

Wówczas biorąc $Q = \mathcal{O}$ mamy $\phi(Q) = P$ i $\delta(P)(\sigma) = \sigma(Q) - Q = \mathcal{O}$ reprezentuje klasę trywialną, której odpowiada $1 \in K^*/K^{*2}$.

(ii) $P = (0,0)$

Wybieramy $Q = \left(\frac{-a+\sqrt{a^2-4b}}{2}, 0\right)$. Jeśli $\sqrt{a^2-4b} \in K$, to $\delta(P)$ jest ponownie klasą trywialną. Jeśli natomiast $K(\sqrt{a^2-4b})/K$ jest rozszerzeniem kwadratowym, to:

$$\sigma(Q) = \begin{cases} \left(\frac{-a+\sqrt{a^2-4b}}{2}, 0\right) = Q & ,\sigma(\sqrt{a^2-4b}) = \sqrt{a^2-4b} \\ \left(\frac{-a-\sqrt{a^2-4b}}{2}, 0\right) = Q + (0,0) & ,\sigma(\sqrt{a^2-4b}) = -\sqrt{a^2-4b} \end{cases}.$$

Skoro $Q + Q = \mathcal{O}$, to:

$$\sigma(Q) - Q = \begin{cases} Q - Q = \mathcal{O} & ,\sigma(\sqrt{a^2-4b}) = \sqrt{a^2-4b} \\ Q + (0,0) - Q = (0,0) & ,\sigma(\sqrt{a^2-4b}) = -\sqrt{a^2-4b} \end{cases}.$$

Przez utożsamienie $H^1(G_{\overline{K}/K}, E[\phi]) \cong K^\times/K^{\times 2}$ dostajemy, że:

$$\delta((0,0)) = a^2 - 4b.$$

(iii) $P = (X, Y) \neq \mathcal{O}, (0, 0)$

Z równości $\phi(x, y) = \left(\frac{y^2}{x^2}, \frac{y(b-x^2)}{x^2}\right) = (X, Y)$ oraz z założenia $x \neq 0$ (bo $P \neq \mathcal{O}$) dostajemy punkt:

$$Q = \left(x, \frac{Yx^2}{b - x^2}\right), \text{ gdzie } x = \frac{(X - a) + \sqrt{\Delta}}{2}$$

oraz $\Delta = (a - X)^2 - 4b$. Jeśli $K(\sqrt{\Delta}) = K$, to $\delta(P) = 1 \in K^\times / K^{\times 2}$. Z kolei, gdy $[K(\sqrt{\Delta}) : K] = 2$, to podobnie jak w (ii):

$$\sigma(Q) - Q = \begin{cases} \mathcal{O} & , \sigma(\sqrt{\Delta}) = \sqrt{\Delta} \\ (0, 0) & , \sigma(\sqrt{\Delta}) = -\sqrt{\Delta} \end{cases} .$$

Skoro punkt $(X, Y) \in E'(K)$, to $\frac{Y^2}{X} = \Delta$, a zatem:

$$\Delta \equiv X \pmod{K^{\times 2}}.$$

Otrzymujemy przyporządkowanie $\delta((X, Y)) = X$.

Dla zakończenia dowodu wystarczy pokazać, że ciąg (3.1) jest dokładny.

Dokładność w miejscu $K(S, 2)$. Jeśli $c(d)$ jest klasą trywialną w

$$H^1(G_{\overline{K}/K}, E[\phi]),$$

to na krzywej C_d istnieje K-wymierny punkt P i wówczas odwzorowanie ψ z tezy twierdzenia daje:

$$\delta(\psi(P)) \equiv d \pmod{K^{\times 2}}.$$

Zatem $\ker(c) \subset \mathrm{im}(\delta)$. Na odwrót jeśli:

(i) $d \equiv \delta(\mathcal{O}) \equiv 1 \pmod{K^{\times 2}}$, to $d = k^2$ dla pewnego $k \in K^\times$ i punkt $(0, k) \in C_d(K)$,

(ii) $d \equiv \delta((0, 0)) \equiv a^2 - 4b \pmod{K^{\times 2}}$, wtedy oba punkty w nieskończoności $[0, 0, \pm\sqrt{\frac{a^2-4b}{d}}, 1]$ należą do $C_d(K)$,

(iii) $d \equiv \delta((X, Y)) \equiv X \pmod{K^{\times 2}}$, wówczas punkt $(1, \frac{Y}{X}) \in C_d(K)$.

Dokładność w miejscu $E'(K)/\phi(E(K))$ sprowadza się do pokazania injektywności odwzorowania δ. Jeżeli zachodzi równość $\delta(P) \equiv 1 \pmod{K^{\times 2}}$ dla pewnego $P \in E'(K)$, to wystarczy pokazać, że wówczas $P \in \phi(E(K))$:

(i) $P = \mathcal{O}$. Skoro ϕ jest izogenią, a w szczególności homomorfizmem grup, to $\phi(\mathcal{O}) = \mathcal{O}$.

(ii) $P = (0, 0)$. Wtedy $a^2 - 4b = k^2$ dla pewnego $k \in K^\times$. Zatem istnieje K-wymierny niezerowy pierwiastek x_0 równania $x^2 + ax + b$ i zachodzi równość $\phi((x_0, 0)) = (0, 0)$.

(iii) $P = (X, Y) \neq \mathcal{O}, (0, 0)$. Wówczas $X = k^2$ i otrzymujemy równość:

$$\phi\left(\frac{Y + k(k^2 - a)}{2k}, \frac{Y + k(k^2 - a)}{2}\right) = (X, Y).$$

□

Zanim omówimy konkretny przykład, do którego można zastosować powyższe twierdzenie, warto zauważyć, że relacje $\phi \circ \widehat{\phi} = [2]$ oraz $\widehat{\phi} \circ \phi = [2]$ implikują istnienie następującego ciągu dokładnego:

$$0 \to \frac{E'(K)[\widehat{\phi}]}{\phi(E(K)[2])} \to \frac{E'(K)}{\phi(E(K))} \xrightarrow{\widehat{\phi}} \frac{E(K)}{2E(K)} \to \frac{E(K)}{\widehat{\phi}(E'(K))} \to 0. \tag{3.3}$$

Stosując Twierdzenie 3.1.1 do obu izogenii w pewnych przypadkach możemy próbować wyznaczyć generatory grupy $E(K)/2E(K)$.

Przykład 3.1.2. Niech ciało $K = \mathbb{Q}$ oraz niech dane będą dwie izogeniczne krzywe:

$$E : y^2 = x^3 + 11x^2 + 17x,$$

$$E' : Y^2 = X^3 - 22X^2 + 53X,$$

a także izogenie $\phi : E \to E'$, $\phi(x, y) = (y^2/x^2, y(17 - x^2)/x^2)$ oraz $\widehat{\phi} : E' \to E$, $\widehat{\phi}(X, Y) = (Y^2/(4X^2), Y(53 - X^2)/(8X^2))$, które spełniają relacje $\phi \circ \widehat{\phi} = [2]$ oraz $\widehat{\phi} \circ \phi = [2]$. Wówczas zbior S określony w Twierdzeniu 3.1.1 jest postaci:

$$S = M_{\mathbb{Q}}^{\infty} \cup \{|\cdot|_2, |\cdot|_{17}, |\cdot|_{53}\},$$

gdzie $M_{\mathbb{Q}}^{\infty}$ zawiera zwykłą wartość bezwzględną na $\mathbb{Q}$ oraz normy $|\cdot|_p$ są standardowymi normami p-adycznymi na $\mathbb{Q}$ (patrz Twierdzenie 2.1.1). Grupa $\mathbb{Q}(S, 2) = \{\pm 1, \pm 2, \pm 17, \pm 53\}$ zawiera podgrupy $Sel^{(\phi)}(E/\mathbb{Q})$ i $Sel^{(\widehat{\phi})}(E/\mathbb{Q})$, które musimy wyznaczyć. Rozważamy przypadki:

(1) $Sel^{(\phi)}(E/\mathbb{Q}) \cong \{1, 53\}$

Niech $d = -1$:

Krzywa $C_{-1} : -w^2 = 1 + 22z^2 + 53z^4$ nie ma punktów rzeczywistych, zatem $C_{-1}(\mathbb{R}) = \emptyset$, co pociąga $-1 \notin Sel^{(\phi)}(E/\mathbb{Q})$. Ponadto łatwo sprawdzić, że zbiory $C_{-2}(\mathbb{R}), C_{-17}(\mathbb{R}), C_{-53}(\mathbb{R})$ są również puste, a zatem

$$-2, -17, -53 \notin Sel^{(\phi)}(E/\mathbb{Q}).$$

Niech $d = 2$:

Krzywa $C_2 : 2w^2 = 4 - 44z^2 + 53z^4$ nie ma punktów w ciele 2-adycznym $\mathbb{Q}_2$. Jeśli $z \notin \mathbb{Z}_2$, to:

$$\mathrm{ord}_2(2w^2) \equiv 1 (\mathrm{mod}\ 2)$$

$$\mathrm{ord}_2(4 - 44z^2 + 53z^4) \equiv 0 (\mathrm{mod}\ 2),$$

co jest niemożliwe. Stąd $z \in \mathbb{Z}_2$. Gdyby $w \notin \mathbb{Z}_2$ to $\mathrm{ord}_2(2w^2) < 1$ oraz $\mathrm{ord}_2(2w^2) \geq 0$. Sprzeczność. Stąd mamy $C_2(\mathbb{Q}_2) = C_2(\mathbb{Z}_2)$. Dostajemy kongruencje:

$$z^4 \equiv 0 (\mathrm{mod}\ 2\mathbb{Z}_2) \Rightarrow z \equiv 0 (\mathrm{mod}\ 2\mathbb{Z}_2),$$

$$z \equiv (\mathrm{mod}\ 2\mathbb{Z}_2 \Rightarrow w \equiv 0 (\mathrm{mod}\ 2\mathbb{Z}_2).$$

Istnieją zatem $w_0, z_0 \in \mathbb{Z}_2$ takie, że $w = 2w_0$ i $z = 2z_0$, co daje:

$$8w_0^2 = 4 - 44 \cdot 4z_0^2 + 53 \cdot 16z_0^4$$

$$2w_0^2 = 1 - 44z_0^2 + 53 \cdot 4z_0^4$$
$$0 \equiv 1 (\text{mod } 2\mathbb{Z}_2).$$

Sprzeczność pociąga, że $2 \notin \text{Sel}^{(\phi)}(E/\mathbb{Q})$.

Niech $d = 17$:

Krzywa $C_{17} : 17w^2 = 289 - 374z^2 + 53z^4$ nie ma punktów w $\mathbb{Q}_{17}$. Podobnie jak dla $d = 2$ pokazujemy, że $C_{17}(\mathbb{Q}_{17}) = C_{17}(\mathbb{Z}_{17})$. Redukując modulo $17\mathbb{Z}_{17}$ otrzymamy $z, w \equiv 0 (\text{mod } 17\mathbb{Z}_{17})$ i biorąc $z_0, w_0 \in \mathbb{Z}_{17}$ takie, że $w = 17w_0$ oraz $z = 17z_0$ po wstawieniu do równania i skróceniu przez 17^2 dostajemy $0 \equiv 1 (\text{mod } 17\mathbb{Z}_{17})$, a stąd $17 \notin \text{Sel}^{(\phi)}(E/\mathbb{Q})$.

Niech $d = 53$:

Krzywa $C_{53} : 53w^2 = 53^2 - 2 \cdot 11 \cdot 53z^2 + 53z^4$ posiada punkt $(z, w) = (\frac{1}{3}, \frac{64}{9}) \in C_{53}(\mathbb{Q})$. Odwzorowanie ψ z Twierdzenia 3.1.1 daje nam punkt:

$$\psi\left(\frac{1}{3}, \frac{64}{9}\right) = (477, -10176) \in E'(\mathbb{Q}).$$

Ostatecznie dostajemy, że $\text{Sel}^{(\phi)}(E/\mathbb{Q}) \cong E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \cong \mathbb{Z}/2\mathbb{Z}$.

(2) $Sel^{(\widehat{\phi})}(E'/\mathbb{Q}) \cong \{\pm 1, \pm 17\}$. Stosujemy teraz Twierdzenie 3.1.1 do izogenii $\widehat{\phi} : E' \to E$ i przestrzenie jednorodne oznaczać będziemy C'_d. Dane jest również odwzorowanie:

$$\psi' : C'_d \to E, \ , \psi'(z, w) = \left(\frac{d}{4z^2}, \frac{-dw}{8z^3}\right).$$

Niech $d = -1$:

Dany jest punkt $(\frac{1}{6}, \frac{1}{9}) \in C_{-1}(\mathbb{R})$. Stąd $-1 \in Sel^{(\widehat{\phi})}(E'/\mathbb{Q})$ oraz $\psi'(\frac{1}{6}, \frac{1}{9}) = (-9, 3) \in E(\mathbb{Q})$.

Niech $d = 2$:

Argumentacja identyczna jak w przykładzie dla $\text{Sel}^{(\phi)}(E/\mathbb{Q})$ pociąga, że $C'_d(\mathbb{Q}_2) = \emptyset$ i $2 \notin \text{Sel}^{(\widehat{\phi})}(E'/\mathbb{Q})$.

Niech $d = 17$:

Otrzymujemy punkt $(\frac{16}{3}, \frac{1073}{9}) \in C'_{17}(\mathbb{Q})$ oraz punkt

$$\psi'(\frac{16}{3}, \frac{1073}{9}) = (\frac{153}{1024}, -\frac{54723}{32768}) \in E(\mathbb{Q}).$$

Niech $d = 53$:

Argumentacja jak dla $d = 2$ daje $53 \notin \text{Sel}^{(\widehat{\phi})}(E'/\mathbb{Q})$.

Niech $d = -2, -53$:

Wystarczy skorzystać ze struktury grupowej w $\mathbb{Q}(S, 2)$ i skoro $-1 \in \text{Sel}^{(\widehat{\phi})}(E'/\mathbb{Q})$ i $2 \notin \text{Sel}^{(\widehat{\phi})}(E'/\mathbb{Q})$, to $-2 \notin \text{Sel}^{(\widehat{\phi})}(E'/\mathbb{Q})$. Podobnie dla $d = -53$.

Otrzymujemy zatem izomorfizmy:

$$E(\mathbb{Q})/\widehat{\phi}(E'(\mathbb{Q})) \cong \text{Sel}^{(\widehat{\phi})}(E/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Skoro $E'(\mathbb{Q})[\widehat{\phi}] = \{\mathcal{O}, (0,0)\}$ oraz $\phi(E(\mathbb{Q})[2]) = \phi(\{\mathcal{O}, (0,0)\}) = \{\mathcal{O}\}$ to w terminach abstrakcyjnych grup ciąg dokładny (3.3) przyjmuje postać:

$$0 \to \mathbb{Z}/2\mathbb{Z} \xrightarrow{a \mapsto a} \mathbb{Z}/2\mathbb{Z} \xrightarrow{a \mapsto 0} E(\mathbb{Q})/2E(\mathbb{Q}) \xrightarrow{a \mapsto a} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \to 0.$$

Twierdzenie 2.2.23 pozwala nam efektywnie obliczyć strukturę grupy $E(\mathbb{Q})_{tors}$. Krzywa E ma dobrą redukcję dla $p = 3, 5$ i $p = 19$. Ponadto:

$$\begin{aligned}
\tilde{E}(\mathbb{F}_3) &= \langle (0,0) \rangle \cong \mathbb{Z}/2\mathbb{Z} \\
\tilde{E}(\mathbb{F}_5) &= \langle (2,1) \rangle \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \\
\tilde{E}(\mathbb{F}_{19}) &= \langle (12,1) \rangle \cong \mathbb{Z}/16\mathbb{Z}.
\end{aligned}$$

Twierdzenie 2.2.23 pociąga:

$$E(\mathbb{Q})[3^r] \hookrightarrow \tilde{E}(\mathbb{F}_{19}) \Rightarrow E(\mathbb{Q})[3^r] = 0 \text{ dla dowolnego } r \geq 1,$$

$$E(\mathbb{Q})[5^r] \hookrightarrow \tilde{E}(\mathbb{F}_3) \Rightarrow E(\mathbb{Q})[5^r] = 0 \text{ dla dowolnego } r \geq 1.$$

Ponadto jeśli $3, 5 \nmid m$, to $E(\mathbb{Q})[m] \hookrightarrow \tilde{E}(\mathbb{F}_3)$ oraz $E(\mathbb{Q})[m] \hookrightarrow \tilde{E}(\mathbb{F}_5)$ i wtedy $|E(\mathbb{Q})[m]| \mid 2$. Stąd dostajemy:

$$E(\mathbb{Q})_{tors} = E(\mathbb{Q})[2] = \{\mathcal{O}, (0,0)\}.$$

Otrzymujemy ostatecznie:

$$E(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

3.2 Rangi w rodzinach krzywych eliptycznych

Rodzina parametryzowana krzywą eliptyczną

W poniższym przykładzie rozważać będziemy rodzinę krzywych eliptycznych

$$E_t : y^2 + txy = x^3 + tx^2 - x + 1$$

określonych nad ciałem liczb wymiernych $\mathbb{Q}$ z parametrem $t \in \mathbb{Q}$. Przedstawimy szkic dowodu następującego twierdzenia.

Twierdzenie 3.2.1 ([Nas10]). *Niech dana będzie krzywa eliptyczna nad $\mathbb{Q}$ postaci:*

$$E_{(u^2-u-3)} : y^2 + (u^2 - u - 3)xy = x^3 + (u^2 - u - 3)x^2 - x + 1.$$

Istnieje nieskończony podzbiór $S \subset \mathbb{Q}$ taki, że jeśli $u \in S$, to grupa Mordella-Weila punktów wymiernych $E_{(u^2-u-3)}(\mathbb{Q})$ zawiera podgrupę rangi 4 rozpiętą przez punkty:

$$(0,1), (1,1), (u, u+1), \left(\frac{1}{9}, \frac{1}{54}(9 + 3u - 3u^2 + v)\right),$$

gdzie punkt (u, v) leży na krzywej:

$$2569 + 18u - 9u^2 - 18u^3 + 9u^4 = v^2.$$

Ponadto, istnieje przekształcenie biwymierne ostatniej krzywej do postaci:

$$y_0^2 = x_0^3 - 92835x_0 + 1389150.$$

Grupa punktów $\mathbb{Q}$-wymiernych tej krzywej ma rangę 2. Ponadto dla $u_1, u_2 \in S$, $u_1 \neq u_2$ krzywe $E_{(u_1^2-u_1-3)}$ i $E_{(u_2^2-u_2-3)}$ nie są ze sobą izomorficzne nad $\overline{\mathbb{Q}}$.

Twierdzenie podaje dolne ogranicznie na rangę grupy wskazanych krzywych. Można jednak wskazać przykłady, dla których ranga jest istotnie wyższa.

Przykład 3.2.2. Dla $u = 16$ możemy pokazać korzystając z programu `mwrank` [Cre97], że grupa punktów wymiernych krzywej $E_{239} : y^2 + 239xy = x^3 + 239x^2 - x + 1$ nad $\mathbb{Q}$ ma rangę 5 i rozpinają ją punkty:

$$(0,1), (1,1), (16,17), (-\frac{14}{15}, \frac{16661}{125}), (\frac{52}{81}, \frac{469}{729}).$$

W celu udowodnienia Twierdzenia 3.2.1 cytujemy zasadnicze twierdzenie, na którym oparta jest główna część dowodu.

Twierdzenie 3.2.3 ([Fal83])**.** *Niech K będzie ciałem liczbowym oraz C gładką krzywą nad K, genusu $g \geq 2$. Wówczas zbiór punktów K-wymiernych $C(K)$ jest skończony.*

Warunek gładkości nie jest istotnie ograniczający w świetle poniższego twierdzenia.

Twierdzenie 3.2.4 ([Har06, I Cor. 6.11])**.** *Niech C będzie krzywą nad ciałem K algebraicznie domkniętym. Wówczas istnieje krzywa C' gładka, biwymiernie równoważna z krzywą C.*

W szczególności, jeśli C jest krzywą określoną nad ciałem liczbowym K, to istnieje skończone rozszerzenie L/K oraz określony nad L izomorfizm pewnego otwartego podzbioru w C na otwarty podzbiór C' dla pewnej krzywej gładkiej C' określonej nad L. Stąd na mocy Twierdzenia 3.2.3 na krzywej C (posiadającej punkty osobliwe) zbiór $C(K)$ jest skończony.

Łatwo można teraz pokazać, że na krzywej $E_{(u^2-u-3)}$ dla prawie wszystkich (tzn. wszystkich poza skończoną liczbą) $u \in \mathbb{Q}$ grupa $\mathbb{Q}$-wymiernych punktów dwutorsyjnych jest trywialna.

Lemat 3.2.5 ([Nas10])**.** *Niech $P = (x, y) \in E_{(u^2-u-3)}(\mathbb{Q})$. Jeśli $2P = \mathcal{O}$, to:*

$$1 - x + \frac{1}{4}(4(-3 - u + u^2) + (-3 - u + u^2)^2)x^2 + x^3 = 0.$$

Powyższa krzywa jest biwymiernie równoważna (nad $\mathbb{Q}$) z krzywą:

$$y_0^2 = -55 + 192x_0 - 114x_0^2 + 68x_0^3 - 15x_0^4 + 4x_0^5$$

genusu 2. W szczególności, dla prawie wszystkich $u \in \mathbb{Q}$ mamy $E_{(u^2-u-3)}(\mathbb{Q})[2] = \{\mathcal{O}\}$.

W dowodzie wykorzystamy następujący elementarny fakt.

Lemat 3.2.6. *Niech M będzie lewym $\mathbb{Z}$-modułem. Niech dany będzie element $b \in M$ oraz liniowo niezależne elementy $a_1, \ldots, a_k \in M$ takie, że klasy $[a_1], \ldots, [a_k] \in M/2M$ są liniowo niezależne nad $\mathbb{F}_2$. Jeśli $[b]$ nie należy do podmodułu $\langle [a_1], \ldots, [a_k] \rangle$ generowanego przez klasy $[a_1], \ldots, [a_k]$ oraz $M[2] = 0$, wówczas $b, a_1, \ldots, a_k$ są liniowo niezależne nad $\mathbb{Z}$ w M.*

Dowód. Przypuśćmy, że istnieje zależność liniowa:

$$\beta b + \alpha_1 a_1 + \ldots + \alpha_k a_k = 0,$$

taka, że nie wszytkie współczynniki są zerami. Bez utraty ogólności możemy założyć, że β jest najmniejszą dodatnią liczbą spełniającą pewną nietrywialną zależnośc liniową jak wyżej. Wówczas jeśli β jest nieparzyste, to $[\beta b] = [b]$, co daje sprzeczność z założeniem $b \notin \langle [a_1], \ldots, [a_k] \rangle$.

Jeśli z kolei β jest parzyste, to $[\beta b] = [0] = \overline{\alpha_1}[a_1] + \ldots + \overline{\alpha_k}[a_k]$, gdzie $\bar{\cdot}$ oznacza branie reszty modulo 2. Elementy $[a_i]$ są liniowo niezależne nad $\mathbb{F}_2$, stąd $\overline{\alpha_i} = \overline{0}$, czyli możemy znaleźć elementy β' oraz α_i' spełniające $2\beta' = \beta$ oraz $2\alpha_i' = \alpha_i$ i wówczas zachodzi nietrywialna relacja:

$$\beta' b = \alpha_1' a_i + \ldots + \alpha_k' a_k,$$

co przeczy minimalności β. □

Zauważmy, że z powyższego lematu oraz z Lematu 3.2.5 wynika prosta metoda sprawdzenia warunku z Twierdzenia 3.2.1 (przy użyciu Twierdzenia 3.2.3). Dane są punkty:

$$P_1 = (0,1), P_2 = (1,1), P_3 = (u, u+1), P_4 = \left(\frac{1}{9}, \frac{1}{54}(9 + 3u - 3u^2 + v)\right)$$

Jeśli dla krzywej $E_{(u^2-u-3)}$ i ustalonego $u \in \mathbb{Q}$ zachodzi $E_{(u^2-u-3)}(\mathbb{Q})[2] = \{\mathcal{O}\}$ (a na mocy Lematu 3.2.5 warunek ten zachodzi dla prawie wszystkich u), to aby udowodnić liniową niezależność punktów P_1, P_2, P_3 i P_4 wystarczy pokazać, że:

$$\epsilon_1 P_1 + \epsilon_2 P_2 + \epsilon_3 P_3 + \epsilon_4 P_4 \notin 2E_{(u^2-u-3)}(\mathbb{Q}) \tag{3.4}$$

dla $\epsilon_i \in \{0, 1\}$ (bez kombinacji trywialnej $\epsilon_i = 0$ dla $i = 1, \ldots, 4$).

Lewa strona należy do $E_{(u^2-u-3)}(\mathbb{Q})$ wtedy i tylko wtedy, gdy

$$\sqrt{2569 + 18u - 9u^2 - 18u^3 + 9u^4}$$

jest liczbą całkowitą.

Niech punkt $(x, y) \in E_{u^2-u-3}$. Ze wzorów na podwojenie punktu na krzywej eliptycznej dostajemy:

$$x(2P) = \frac{4 - 2u + u^2 + 2u^3 - u^4 - 8x + 2x^2 + x^4}{4 - 4x + (-3 + 2u - u^2 - 2u^3 + u^4)x^2 + 4x^3}.$$

Warunek (3.4) dla ustalonej czwórki $(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4)$ określa pewne równanie wielomianowe (po wyrugowaniu mianowników i pierwiastka pochodzącego z czwartego punktu):

$$f_{(\epsilon_1,\epsilon_2,\epsilon_3,\epsilon_4)}(x, u) = 0.$$

Ponadto sprawdzenie, że dwie krzywe E_{u_1}, E_{u_2} nie są izomorficzne nad $\overline{\mathbb{Q}}$ sprowadza się do pokazania, że mają one różne $j - niezmienniki$, tzn. do warunku:

$$j(E_{u_1}) \neq j(E_{u_2}),$$

gdzie:

$$j(E_u) = -\frac{(48 + u^2(4+u)^2)^3}{(2+u)^2(92 + (-1+u)u(4+u)(5+u))}.$$

Dowód Twierdzenia 3.2.1. W świetle powyższej dyskusji wystarczy pokazać, że dla dowolnej czwórki $(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4) \neq (0,0,0,0)$ krzywa zadana równaniem

$$f_{(\epsilon_1,\epsilon_2,\epsilon_3,\epsilon_4)}(x,u) = 0 \tag{3.5}$$

ma skończenie wiele punktów $\mathbb{Q}$-wymiernych oraz, że równość

$$j(E_{u_1}) = j(E_{u_2}) \tag{3.6}$$

zachodzi tylko dla skończenie wielu par $u_1, u_2 \in \mathbb{Q}$.

Na mocy Twierdzenia 3.2.3 wystarczy pokazać, że krzywe zadane równaniami (3.5) oraz (3.6) mają genus większy niż 1.

Dla przykładu (szczegóły w [Nas10])) podajemy równania odpowiadajace takim krzywym oraz podajemy ich genus:

$$\begin{aligned} C_{(0,0,0,1)} : 40 - 18u + 9u^2 + 18u^3 - 9u^4 - 76x + \\ 15x^2 + 2ux^2 - u^2x^2 - 2u^3x^2 + u^4x^2 + 4x^3 + 9x^4 = 0 \end{aligned}$$

$$genus(C_{(0,0,0,1)}) = 5$$

$$\begin{aligned} C_{(1,0,0,1)} : 9(9u^4 - 18u^3 - 9u^2 + 18u + 2569)(u^4x^2 - 2u^3x^2 - u^2x^2 \\ + 2ux^2 + 4x^3 - 3x^2 - 4x + 4)^2 - (153u^4x^2 \\ + u^4 - 306u^3x^2 - 2u^3 - 153u^2x^2 - u^2 \\ + 306ux^2 + 2u - x^4 + 612x^3 - 461x^2 - 604x + 608)^2 = 0 \end{aligned}$$

$$genus(C_{(1,0,0,1)}) = 9$$

Z kolei krzywa powstająca przez wyrugowanie mianowników w równaniu (3.6) ma genus 11. Zatem specjalizując parametr $u \mapsto u^2 - u - 3$ na mocy Twierdzenia 3.2.3 nadal będzie tylko skończenie wiele parametrów wymiernych spełniających równanie (3.6). Jedyny przypadek, który nie daje krzywej genusu wyższego niż jeden odpowiada czwórce $(1,0,0,0)$. Biorąc równanie odpowiadające tej czwórce:

$$C_{(1,0,0,0)} : 4 - 2u + u^2 + 2u^3 - u^4 - 8x + 2x^2 + x^4 = 0,$$

łatwo dostajemy reparametryzację równania do postaci Weierstrassa krzywej eliptycznej:

$$F : y_0^2 = x_0^3 + \frac{359}{3}x_0 + \frac{3130}{27}.$$

Grupa $F(\mathbb{Q})$ jest generowana przez punkt nieskończonego rzędu:

$$\left(\frac{53}{3}, 88\right).$$

Skoro krzywe $C_{(1,0,0,0)}$ i F są biwymierne, to nasza metoda sugeruje, że należy odrzucić nieskończony zbiór parametrów u w tezie twierdzenia. Należy jednak wziąć pod uwagę warunek:

$$\sqrt{2569 + 18u - 9u^2 - 18u^3 + 9u^4} \in \mathbb{Z}.$$

Dla uproszczenia obliczeń rozważmy ponownie ogólną krzywą eliptyczną rodziny $E_t : y^2 + txy = x^3 + tx^2 - x + 1$ dla ustalonego t oraz załóżmy, że istnieje punkt $P \in E_t(\mathbb{Q})$ taki, że $x(P) = \frac{1}{9}$. Otrzymamy następujący równoważny układ równań:

$$\begin{aligned} s^2 &= 2596 + 36t + 9t^2 \\ 0 &= 1 - 4t - t^2 - 8x + 2x^2 + x^4. \end{aligned} \tag{3.7}$$

Pierwsze równanie definiuje pewną (niepustą) kwadrykę nad $\mathbb{Q}$. Możemy napisać jej wymierną parametryzację:

$$\begin{aligned} t &= \frac{2596 - f^2}{6f - 36} \\ s &= \frac{f^2 - 12f + 2596}{2f - 12}. \end{aligned}$$

Wstawiając parametryzację t do równania (3.7) otrzymamy krzywą genusu 3. Stosując ponownie Twierdzenie 3.2.3 i biorąc specjalizację $t \mapsto u^2 - u - 3$ dostajemy, że na krzywej $C_{(1,0,0,0)}$ jest skończenie wiele punktów $\mathbb{Q}$-wymiernych przy założeniu, że na krzywej eliptycznej $E_{(u^2-u-3)}$ istnieje punkt wymierny o pierwszej współrzędnej równej $\frac{1}{9}$.

To kończy dowód twierdzenia. □

Praktyczna metoda generowania krzywych o randze co najmniej 4 w rodzinie $E_{(u^2-u-3)}$ opiera się na przekształceniu równania:

$$C_2 : 2569 + 18u - 9u^2 - 18u^3 + 9u^4 = v^2$$

z tezy Twierdzenia 3.2.1 do skróconej postaci Weierstrassa:

$$C_1 : y_0^2 = x_0^3 - 92835x_0 + 1389150.$$

Istnieje odwzorowanie wymierne (morfizm rozmaitości algebraicznych na ustalonych podzbiorach otwartych):

$$\begin{aligned} \phi &: C_1 \to C_2 \\ \phi(x_0, y_0) &= (u, v), \end{aligned}$$

gdzie

$$\begin{aligned} u &= \frac{565605 + x_0(-948 + 7x_0) + 266y_0}{(-1551 + x_0)(45 + x_0)} \\ v &= \frac{-1418250637125 + 460545750x_0 - 917966790y_0 + 2108340x_0y_0 + 9594x_0^2y_0}{(-1551 + x_0)^2(45 + x_0)^2}. \end{aligned}$$

Grupa $C_1(\mathbb{Q}) \cong \mathbb{Z}^2 \oplus \mathbb{Z}/2$. Część wolna generowana jest przez punkty $P_1 = (-309, 756)$, $P_2 = (-45, 2340)$, a część torsyjna przez punkt $T = (15, 0)$.

Odwzorowanie biwymierne ϕ indukuje izomorfizm $C_1\setminus\{(-45,2340),(1551,59904)\}$ na $C_2\setminus\{\infty_{C_2}\}$ (gdzie ∞_{C_2} jest punktem w nieskończoności w domknięciu rzutowym C_2). Otrzymujemy zatem odwzorowanie:

$$\upsilon : \{0,1\}\times\mathbb{Z}^2 \to \mathbb{Q}$$

$$\upsilon : (\alpha,\beta_1,\beta_2) \mapsto u(\alpha T+\beta_1 P_1+\beta_2 P_2).$$

Z Twierdzenia 3.2.1 wynika, że poza skończoną liczbą elementów w obrazie $\mathrm{Im}(\upsilon)$ grupa $E_{(u^2-u-3)}(\mathbb{Q})$ ma rangę co najmniej 4 dla $u=\upsilon(\alpha,\beta_1,\beta_2)$.

Rodzina Mestre parametryzowana prostą rzutową

W tej części pracy opiszemy pochodzącą z [Mes91] konstrukcję krzywej eliptycznej E nad ciałem $\mathbb{Q}(t)$, która posiada 11 liniowo niezależnych punktów. Poprzez morfizm $(x,y,t)\mapsto t : E\to\mathbb{P}^1$ możemy traktować E jako rodzinę krzywych nad ciałem $\mathbb{Q}$, spośród których tylko skończenie wiele jest krzywymi osobliwymi.

Lemat 3.2.7. *Niech k będzie ciałem charakterystyki różnej od 3 i niech dany będzie $p\in k[x]$ wielomian unormowany stopnia 12. Istnieje jednoznacznie określona trójka wielomianów (g,r_1,r_2) w $k[x]$ spełniających równanie:*

$$p = g^3 + r_1 g + r_2. \tag{3.8}$$

Wielomian g jest stopnia 4 i jest unormowany. Ponadto zachodzą nierówności:

$$deg(r_1)\le 3, \quad deg(r_2)\le 3.$$

Dowód. Niech dany będzie wielomian $p(x)=x^{12}+p_1x^{11}+\ldots p_{11}x^1+p_{12}$ oraz niech $g(x)=x^4+s_1x^3+s_2x^2+s_3x+s_4$. Przez porównanie współczynników przy x^k dla $k=11,10,9$ i 8 w równaniu (3.8) dostajemy układ równań:

$$\begin{aligned}
p_1 &= 3s_1\\
p_2 &= 3s_1^2+3s_2\\
p_3 &= s_1^3+6s_1s_2+3s_3\\
p_4 &= 3s_1^2s_2+3s_2^2+6s_1s_3+3s_4.
\end{aligned}$$

Przez eliminację zmiennych w kolejnych równaniach otrzymujemy jawną postać wielomianu g:

$$\begin{aligned}
g(x) = &-\frac{10p_1^4}{243}+\frac{5p_1^2p_2}{27}-\frac{p_2^2}{9}-\frac{2p_1p_3}{9}+\frac{p_4}{3}+\left(\frac{5p_1^3}{81}-\frac{2p_1p_2}{9}+\frac{p_3}{3}\right)x\\
&+\left(-\frac{p_1^2}{9}+\frac{p_2}{3}\right)x^2+\frac{p_1x^3}{3}+x^4.
\end{aligned}$$

Wielomian r_1 otrzymujemy jako część wielomianową dzieląc z resztą $p-g^3$ przez g. Reszta z dzielenia jest wielomianem r_2. □

W dalszych rozważaniach interesować nas będzie współczynnik wielomianu r_1 przy najwyższej potędze:

$$s=\frac{1}{243}\left(22p_1^5-120p_1^3p_2+135p_1p_2^2+135p_1^2p_3-162p_2p_3-162p_1p_4+243p_5\right).$$

Lemat 3.2.8. *Niech* $p(x) = \prod_{i=1}^{12}(x - x_i) \in k(x_1, \ldots, x_{12})[x]$. *Wówczas współczynnik* s *(określony powyżej jako wielomian zmiennych* x_i*) zadaje rozmaitość afiniczną* $s(x_1, \ldots, x_{12}) = 0$*, która zawiera zbiór algebraiczny zadany parametrycznie:*

$$(x_1, \ldots, x_{12}) = (a, b, c, d, a, b, c, d, a, b, c, d) + t(d, d, d, c, c, c, b, b, b, a, a, a),$$

gdzie $a, b, c, d, t \in k$ *są dowolne.*

Dowód. Ze wzorów Viete'a otrzymujemy wyrażenia na współczynniki p_i wielomianu p i podstawiając do wzoru na s przez bezpośrednie sprawdzenie otrzymujemy tezę. □

W szczególności wybierzmy teraz pierwiastki

$$(x_1, \ldots, x_{12}) = (a, b, c, d, a, b, c, d, a, b, c, d) + t(d, d, d, c, c, c, b, b, b, a, a, a).$$

Równanie (3.8) implikuje:

$$0 = p(x_i) = g(x_i)^3 + r_1(x_i)g(x_i) + r_2(x_i).$$

Zatem punkty $(x_i, g(x_i))$ leżą na krzywej:

$$C : y^3 + r_1(x)y + r_2(x) = 0$$

zdefiniowanej nad $K = \mathbb{Q}(a, b, c, d, t)$. Ze względu na wybór x_i wielomian $r_1(x) \in K[x]$ ma stopień co najwyżej 2 (z definicji ma stopień co najwyżej 3, ale współczynnik przy najwyższej potędze, czyli s znika na mocy Lematu 3.2.8), co pociąga, że krzywa C/K jest stopnia trzy.

Specjalizując teraz zmienne a, b, c i d do wartości w $\mathbb{Q}$ otrzymamy krzywe stopnia trzy, na których mamy określone 12 punktów $\mathbb{Q}(t)$-wymiernych. Ujednoradniając wielomian definiujący C otrzymamy krzywą rzutową $\tilde{C}$ w $\mathbb{P}^2$ nad $\overline{\mathbb{Q}(t)}$.

Twierdzenie 3.2.9. *Kładąc* $a = -1$*,* $b = 2$*,* $c = 0$ *oraz* $d = 17$ *otrzymujemy krzywą rzutową* $\tilde{C}$ *nieosobliwą nad* $\overline{\mathbb{Q}(t)}$*. Niech dany będzie punkt*

$$P_0 = [-1, 342 + 279t - 238t^2, 1] \in \tilde{C}(\mathbb{Q}(t)).$$

Wówczas para $(\tilde{C}, P_0)$ *jest krzywą eliptyczną. Ponadto grupa* $\tilde{C}(\mathbb{Q}(t))$ *posiada* 11 *niezależnych liniowo punktów w części afinicznej* C*:*

$$\begin{array}{ll}
P_1 = \left(-1 + 17t, -2\left(288 - 3361t + 3060t^2\right)\right) & P_2 = \left(2 + 17t, -1050 - 6217t + 7650t^2\right) \\
P_3 = \left(17t, 374 + 747t - 1530t^2\right) & P_4 = \left(17, -1530 + 747t + 374t^2\right) \\
P_5 = \left(2, -2\left(-240 + 159t + 68t^2\right)\right) & P_6 = \left(2t, 2\left(-68 - 159t + 240t^2\right)\right) \\
P_7 = \left(17 + 2t, 7650 - 6217t - 1050t^2\right) & P_8 = \left(-1 + 2t, 234 - 1213t + 570t^2\right) \\
P_9 = \left(2 - t, 570 - 1213t + 234t^2\right) & P_{10} = \left(-t, -238 + 279t + 342t^2\right) \\
P_{11} = \left(17 - t, -2\left(3060 - 3361t + 288t^2\right)\right) &
\end{array}$$

Dowód. Równanie jednorodne krzywej $\tilde{C}$, którą otrzymujemy przy ustalonym wyborze a, b, c, d ma postać:

$$z^3 + a_1x^2z + a_2wxz + a_3w^2z + a_4x^3 + a_5wx^2 + a_6w^2x + a_7w^3,$$

gdzie współczynniki a_i są zadane równaniami:

$$a_1 = -4\left(42078 - 81923t + 42078t^2\right),$$
$$a_2 = -12(1+t)\left(2006 - 10711t + 2006t^2\right),$$
$$a_3 = -107508 - 1615080t + 3198533t^2 - 1615080t^3 - 107508t^4,$$
$$a_4 = -20007680(-1+t)^2(1+t),$$
$$a_5 = 4(22326468 + 75564516t - 195270611t^2 + 75564516t^3 + 22326468t^4),$$
$$a_6 = 4(1+t)(12777948 - 140544164t + 250930219t^2 - 140544164t^3 + 12777948t^4),$$
$$a_7 = -2(6052816 + 172482204t - 287040540t^2 + 184802333t^3 - 287040540t^4 + 172482204t^5 + 6052816t^6).$$

Na mocy [Har06, Prop.4.6] istnieje zanurzenie krzywej $(\tilde{C}, P_0)$ w $\mathbb{P}^2$ (indukowane przez system liniowy $|3P_0|$) do krótkiej postaci Weierstrassa:

$$y^2 = x^3 + ax + b,$$

posyłające punkt P_0 na punkt w nieskończoności.

Praktyczny algorytm realizujący to zanurzenie można znaleźć w [vH95] (implementacja algorytmu w pakiecie MAPLE). Zastosowanie tej metody do krzywej $\tilde{C}$ daje nam równanie Weierstrassa:

$$E : y^2 = x^3 + a(t)x + b(t),$$

gdzie współczynniki dane są wzorami:

$$\begin{aligned} a(t) = -\frac{16}{3}(&42216450819481621800 0 + 57674012841634266699 84t \\ &+ 10748781663416427146040t^2 - 12079032258011686828692 0t^3 \\ &+ 18215183482771857855754 5t^4 + 26907807141183189589380t^5 \\ &- 21041353330391561776940 6t^6 + 26907807141183189589380t^7 \\ &+ 18215183482771857855754 5t^8 - 12079032258011686828692 0t^9 \\ &+ 10748781663416427146040t^{10} + 57674012841634266699 84t^{11} \\ &+ 42216450819481621800 0t^{12}), \end{aligned}$$

$$\begin{aligned} b(t) = \frac{128}{27}(&88869434401755794863089139536 00t^{18} + \\ &17128016413498876398786752790240 0t^{17} + 96921679717530572622908106135384 0t^{16} \\ &- 23115949476475327541088122979273 60t^{15} - 23760837973879613334551448211146948t^{14} + \\ &81412717346835256380887447443104060t^{13} + 24484159847622319074900985578614505t^{12} \\ &- 59666493262973525070043517295261399 0t^{11} + 14817632263355382076434730146362269 65t^{10} \\ &- 19321442413027654094483869345896586 72t^9 + 14817632263355382076434730146362269 65t^8 \\ &- 59666493262973525070043517295261399 0t^7 + 24484159847622319074900985578614505t^6 \\ &+ 81412717346835256380887447443104060t^5 - 23760837973879613334551448211146948t^4 \\ &- 23115949476475327541088122979273 60t^3 + 96921679717530572622908106135384 0t^2 \\ &+ 17128016413498876398786752790240 0t + 88869434401755794863089139536 00). \end{aligned}$$

Izomorfizm krzywych $(\tilde{C}, P_0)$ i $(E, \mathcal{O})$ jest dany nad $\mathbb{Q}(t)$. Wyróżnik $\Delta(t) = -4a(t)^3 - 27b(t)^2$ równania definiującego krzywą E ma stopień 36 i jest nierozkładalny jako wielomian zmiennej t nad $\mathbb{Q}$. Morfizm $\pi : E \to \mathbb{P}^1$ zadany jako $(x, y, t) \mapsto t$ definiuje nam rodzinę krzywych nad $\mathbb{Q}$. Dla wszystkich $\alpha \in \overline{\mathbb{Q}}$ takich, że $\Delta(\alpha) \neq 0$ włókno $\pi^{-1}(\alpha)$ jest nieosobliwą krzywą eliptyczną.

Z kolei jeśli $\Delta(\beta) = 0$, to można sprawdzić (korzystając z algorytmu [SS09, 4.2]), że włókna $\pi^{-1}(\beta)$ są krzywymi singularnymi izomorficznymi (nad $\overline{\mathbb{Q}}$) z $y^2 = x^3 + x^2$ (inaczej: włókna osobliwe są typu I_1 w klasyfikacji Kodairy).

Skoro krzywe $\tilde{C}$ i E są izomorficzne nad $\mathbb{Q}(t)$, więc włókna osobliwe są tego samego typu. Można pokazać, że istnieje wysokość kanoniczna $\hat{h} : \tilde{C}(\overline{\mathbb{Q}(t)}) \to \mathbb{R}$ spełniająca te same własności, które spełnia wysokość kanoniczna dla rozmaitości abelowych nad ciałem liczbowym (patrz [BG06, 1.4.6]). Ponadto mamy odwzorowanie dwuliniowe stowarzyszone z wysokością $\hat{h}$:

$$\langle P, Q \rangle = \chi + (P.P_0) + (Q.P_0) - (P.Q),$$

$$\langle P, P \rangle = 2(\chi + (P.P_0)).$$

Liczba $\chi \in \mathbb{N}$ jest równa genusowi arytmetycznemy $\tilde{C}$ traktowanej jako powierzchnia nad $\overline{\mathbb{Q}}$. W powyższym przypadku, na podstawie [SS09, Thm.6.10] mamy $\chi = 3$. Punkty $P, Q \in \tilde{C}(\mathbb{Q}(t))$ traktujemy jako przekroje odwzorowania $\pi : \tilde{C} \to \mathbb{P}^1 : (x, z, w, t) \mapsto t$. Wówczas $(P.Q)$ jest stopniem przecięcia krzywych $P(t)$, $Q(t)$ (liczonym jako krotność ich przecięcia). Jeśli dane są dwa punkty $P_i = (\alpha + \beta t, g(\alpha + \beta t))$ oraz $P_j = (\gamma + \delta t, g(\gamma + \delta t))$, to ich indeks przecięcia może być równy tylko 1 lub 0 (brak przecięcia lub przecięcie jednokrotne, transwersalne). Stąd dostajemy następujace proste kryterium dla $i \neq j$:

$$(P_i.P_j) = \begin{cases} 0 & (\alpha - \gamma)(\beta - \delta) = 0, \\ 1 & \text{w p.p.} \end{cases}$$

Zatem punkty $P_1, \ldots, P_{11}$ są niezależne liniowo nad $\mathbb{Z}$ wtedy i tylko wtedy, gdy macierz:

$$H = (\langle P_i, P_j \rangle)_{1 \leq i,j \leq 11}$$

ma niezerowy wyznacznik. Łatwo sprawdzić, że $\det H = 2^8 \cdot 3^5 \cdot 5 \cdot 17$. □

Krzywe eliptyczne nad $\mathbb{F}_p(t)$

W tym paragrafie naszkicujemy dowód, że krzywa eliptyczna w postaci Legendre'a:

$$E : y^2 = x(x + 1)(x + t)$$

nad ciałem $\mathbb{F}_p(t)$ ($p > 2$ jest liczbą pierwszą) posiada $d-2$ liniowo niezależnych punktów w rozszerzeniu $K_d = \mathbb{F}_p(\mu_d, t^{1/d})$ (patrz [Ulm10]).

W celu konstrukcji poszukiwanych punktów specjalizujemy $d = p^f + 1$ dla $f \geq 0$ (w szczególności d jest zawsze parzyste). Wówczas rozszerzenie K_d konstruujemy poprzez dołączenie pierwiastka pierwotnego μ_d stopnia d z 1 oraz dołączając do $\mathbb{F}_p(t)$ element u spełniający relację $u^d = t$. Wówczas otrzymujemy

$$K_d = \mathbb{F}_p(t)(\mu_d, u)$$

i widać w szczególności, że rozszerzenie nie zależy od wyboru pierwiastka równania $X^d = t$.

Na krzywej E istnieje jeden oczywisty punkt:

$$P(u) = (u, u(u+1)^{d/2}) \in E(K_d).$$

Korzystamy przy tym w istotny sposob z tożsamości $(a+b)^p = a^p + b^p$ zachodzącej dla $a, b \in \mathbb{F}_p(t)$.

Ponadto łatwo sprawdzić, że punkty $P(\mu_d^i)$ dla $i = 1, \ldots, d-1$ również należą do grupy $E(K_d)$.

Twierdzenie 2.3.7 orzeka tylko, że grupa $E(K_d)$ jest skończenie generowana. Nie podaje jednak metody konstrukcji wysokości kanonicznej i dodatnio określonej, symetrycznej formy dwuliniowej na $E(K_d) \otimes \mathbb{R}$. Takie funkcje istnieją (patrz [Ulm10, 4.2], [SS09, 11.8]). Niech odwzorowanie:

$$\langle \cdot, \cdot \rangle : E(K_d) \times E(K_d) \to \mathbb{R}$$

będzie symetryczne i dodatnio określone na punktach nietorsyjnych (tzn. jeśli $\langle P, P \rangle = 0$, to $P \in E(K_d)_{tors}$)). Wówczas na przestrzeni liniowej $E(K_d) \otimes \mathbb{R}$ indukuje ono strukturę przestrzeni euklidesowej z iloczynem skalarnym $\langle \cdot, \cdot \rangle$, w której obraz inkluzji $E(K_d)/E(K_d)_{\text{tors}} \hookrightarrow E(K_d) \otimes_{\mathbb{Z}} \mathbb{R}$ określa kratę.

Twierdzenie [Ulm10, 4.4] orzeka, że dla $d = p^f + 1$ i $p > 2$ oraz $f \geq 0$ zachodzą następujące równości:

$$\langle P_i, P_j \rangle = \begin{cases} \frac{(d-1)(d-2)}{2d} & i = j, \\ \frac{1-d}{d} & 2 \mid i-j,\ i-j \neq 0, \\ 0 & 2 \nmid i-j. \end{cases}$$

W szczególności łatwo sprawdzić, że dla punktu $Q = P_0 + \ldots + P_{d-1}$ mamy $\langle Q, Q \rangle = 0$, co pociąga, że $Q \in E(K_d)_{\text{tors}}$. Podobnie sprawdzamy, że dla $R = P_0 - P_1 + \ldots + P_{d-2} - P_{d-1}$ zachodzi równość $\langle R, R \rangle = 0$ i $R \in E(K_d)_{\text{tors}}$.

Zauważmy teraz, że macierz

$$H = (\langle P_i, P_j \rangle)_{0 \leq i,j \leq d-3}$$

jest cykliczna, a jej pierwszy wiersz jest dany następująco

$$(a_0, a_1, \ldots, a_{d-5}, a_{d-4}, a_{d-3}) = \left(\frac{(d-1)(d-2)}{2d}, 0, \frac{1-d}{d}, \ldots, 0, \frac{1-d}{d}, 0 \right).$$

Niech dany będzie teraz wielomian:

$$f(x) = \frac{(d-1)(d-2)}{2d} + \frac{1-d}{d} x^2 + \ldots + \frac{1-d}{d} x^{d-4} \in \mathbb{Q}[x].$$

Wyznacznik macierzy H można obliczyć za pomocą operacji elementarnych (patrz [BG02]):

$$\det H = \prod_{i=1}^{d-2} f(\zeta_{d-2}^i),$$

gdzie ζ_{d-2} jest pierwiastkiem pierwotnym stopnia $d-2$ z 1. Zauważmy, że jeśli $\zeta = \zeta_{d-2}^i \neq \pm 1$, to:

$$1 + \zeta + \zeta^2 + \ldots + \zeta^{d-3} = 0,$$

$$1 + (-\zeta) + (-\zeta)^2 + \ldots + (-\zeta)^{d-3} = 0$$

i skoro d jest parzyste, to dodając powyższe równości stronami i dzieląc przez 2 dostajemy:

$$1 + \zeta^2 + \zeta^4 + \ldots + \zeta^{d-4} = 0.$$

Zatem dla $\zeta^{d-2} = 1$ i $\zeta \neq \pm 1$:

$$\begin{aligned} f(\zeta) &= \frac{1-d}{d}\left(-\frac{(d-2)}{2} + \zeta^2 + \zeta^4 + \ldots + \zeta^{d-4}\right) \\ &= \frac{1-d}{d}\left(-\frac{(d-2)}{2} - 1\right) = \frac{d-1}{2}. \end{aligned}$$

Z kolei dla $\zeta = \pm 1$ zachodzą równości:

$$f(\pm 1) = \frac{1-d}{d}\left(-\frac{(d-2)}{2} + \frac{d-4}{2}\right) = \frac{d-1}{d}.$$

Podstawiając do wzoru na wyznacznik macierzy H dostajemy:

$$\det H = f(1)f(-1)\prod_{\zeta \neq \pm 1} f(\zeta) = \left(\frac{d-1}{d}\right)^2 \cdot \left(\frac{d-1}{2}\right)^{d-4}.$$

W szczególności dla $d = p^f + 1$ wyznacznik $\det H \neq 0$. Stąd punkty $P_0, \ldots, P_{d-3}$ są liniowo niezależne i generują podgrupę rangi $d-2$ w $E(K_d)$.

Powyższy przykład pokazuje, że nad ciałami skończenie generowanymi dodatniej charakterystyki można efektywnie konstruować krzywe eliptyczne z grupą punktów wymiernych dowolnie wysokiej rangi. Własność ta jest w silnym kontraście z sytuacją dla krzywych eliptycznych nad ciałami liczbowymi. Aktualny rekord rangi jaki ma miejsce należy do Elkiesa, który podał:

$$\begin{aligned} &E : y^2 + xy + y = x^3 - x^2 \\ &- 20067762415575526585033208209338542750930230312178956502x \qquad (3.9) \\ &+ 3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9. \end{aligned}$$

Grupa $E(\mathbb{Q})$ zawiera 28 liniowo niezależnych punktów

$$\begin{aligned} P_1 &= (-212415009125438107329213746 3, 259854492051899599030515511070780628911531), \\ P_2 &= (233450986603470175688475453 7, 188720041954944691808683165528036279315 31), \\ P_3 &= (-167173605406236906387903866 3, 251709377261144287808506947241319126049131), \\ P_4 &= (213913026013915666649298213 7, 366395091714397292024214596929412975275 31), \\ P_5 &= (153470676446712072388547733 7, 854295853460176942890210328627810727995 31), \\ P_6 &= (-273107948787567703334157506 3, 262521815484332191641284072623902143387531), \\ P_7 &= (277572626684457164970545853 7, 128457554740140602488694876990826403699 31), \\ P_8 &= (149438572932718895754183381 7, 884866055277334059861164945140492334114 51), \\ P_9 &= (186843822862088735850906525 7, 592374032144377087127251403930593585891 31), \\ P_{10} &= (200894510882574377486654253 7, 476906778801255528821517507815414247115 31), \end{aligned}$$

$P_{11} = (23483605409180251696516329 37, 17492930006200557857340332476448804363531)$,
$P_{12} = (-14720840070904811744700086 63, 24664345065350371419994744154975979846913 1)$,
$P_{13} = (29241286077080612133632889 37, 28350264431488878501488356474767375899531)$,
$P_{14} = (53749938910660618932939345 37, 28618890842726338645117503191647989373153 1)$,
$P_{15} = (17096907682333545233340085 57, 71898834974686089466159700529215980921631)$,
$P_{16} = (24509540113535931440725951 87, 44452281735326343570492625506107147365 31)$,
$P_{17} = (29692547092735591674646749 37, 32766893075366270801333682543160469687531)$,
$P_{18} = (27119149349416926013328829 37, 20684366127783816986504139815065906135 31)$,
$P_{19} = (20078586077996854528778328 937, 27796085411378066046560517256246240300915 31)$,
$P_{20} = (21580824502407347743178106 97, 34994373401964026809969662241800901254731)$,
$P_{21} = (20046454582470590224032249 37, 48049329780704645522439866999888475467531)$,
$P_{22} = (29757494509479962649470913 37, 33398989826075322320208934410104857869131)$,
$P_{23} = (-21024904676862851501473478 63, 25957639145987578957167739317168720322753 1)$,
$P_{24} = (31158317991506303490219453 7, 16810438522998060354010947291566015347393 1)$,
$P_{25} = (27739310083418652314437718 17, 12632162834649921002414116273769275813451)$,
$P_{26} = (21565811881437684093634613 87, 35125092964022908897004150516375178087331)$,
$P_{27} = (38663304998724125088156591 37, 12119775565594422629303692671502584732253 1)$,
$P_{28} = (22308682897735760237786787 37, 28558760030597485663387020600768640028531)$.

4 Uzupełnienia algebraiczne

4.1 Podstawowe definicje

Formy i odwzorowania kwadratowe

Definicja 4.1.1 ([Lan73, Def.str.385]). Niech R będzie pierścieniem przemiennym i takim, że element 2 jest w nim odwracalny, a E, F będą R-modułam. Mówimy, że $f : E \to F$ jest **odwzorowaniem kwadratowym** jeżeli istnieją odwzorowanie dwuliniowe symetryczne $g : E \times E \to F$ oraz odwzorowanie liniowe $h : E \to F$ takie, że dla każego $x \in E$ mamy

$$f(x) = g(x, x) + h(x).$$

Ponadto odwzorowanie $f : E \to R$ nazywamy **formą kwadratową** jeśli f jest odwzorowaniem kwadratowym, dla którego stowarzyszone odwzorowanie liniowe h spełnia $h(x) = 0$ dla każdego $x \in E$.

Lemat 4.1.2. *Niech E, F będą R-modułami (element 2 odwracalny w R), a odwzorowanie $f : E \to F$ spełnia prawo równoległoboku:*

$$h(x + y) + h(x - y) = 2h(x) + 2h(y)$$

dla dowolnych $x, y \in E$. Wówczas f jest formą kwadratową na E.

Dowód. Dla $x = y = 0$ dostajemy z prawa równoległoboku $h(0) = 0$. Następnie kładąc $p = 0$ dostajemy $h(-q) = q$. Stosując prawo równoległoboku dostajemy równości:

$$\begin{aligned}
A &= h(x + y + z) + h(x + z - y) - 2h(x + z) - 2h(y) = 0,\\
B &= h(x - z + y) + h(x + z - y) - 2h(x) - 2h(z - y) = 0,\\
C &= h(x - z + y) + h(x + z + y) - 2h(x + y) - 2h(z) = 0,\\
D &= 2h(z + y) + 2h(z - y) - 4h(z) - 4h(y) = 0.
\end{aligned}$$

Skoro $2 \in R^\times$, to możemy zdefiniować:

$$g(x, y) = \frac{h(x + y) - h(x) - h(y)}{2}$$

dla dowolnych x, y. Wówczas $g(x,y) = g(y,x)$ oraz:

$$g(x+z,y) - g(x,y) - g(z,y) = \frac{A - B + C - D}{4} = 0.$$

Korzystając z symetrii dostajemy, że g jest odwzorowaniem dwuliniowym, ponadto $g(x,x) = h(x)$. Z Definicji 4.1.1 wynika, że h jest formą kwadratową. □

Normy

Definicja 4.1.3. Niech K będzie ciałem. **Normą** określoną w ciele K nazywamy odwzorowanie

$$|\cdot| : K \to \mathbb{R}$$

spełniające następujące trzy warunki:

(1) $|x| \geq 0$ dla $x \in K$, $|x| = 0$ wtedy i tylko wtedy, gdy $x = 0$.

(2) $|xy| = |x| \cdot |y|$ dla $x, y \in K$.

(3) $|x + y| \leq |x| + |y|$ dla $x, y \in K$.

Ponadto normę nazywamy **niearchimedesowską** jeśli zachodzi silniejsza wersja warunku (3):

$$|x + y| \leq \max\{|x|, |y|\}.$$

Schematy i morfizmy

Definicja 4.1.4 (Przestrzeń ze snopem)**.** Parę $(X, \mathcal{O}_X)$, gdzie X jest przestrzenią topologiczną, a $\mathcal{O}_X$ jest snopem pierścieni nazywamy **przestrzenią ze snopem**.

Parę $(f, f^\#)$ nazywamy **morfizmem przestrzeni ze snopem** $(X, \mathcal{O}_X)$ do $(Y, \mathcal{O}_Y)$ jeśli $f : X \to Y$ jest ciągłym odwzorowaniem i $f^\# : \mathcal{O}_Y \to f_*\mathcal{O}_X$, gdzie $f_*\mathcal{O}_X(U) = \mathcal{O}_X(f^{-1}(U))$ dla dowolnego zbioru otwartego U.

Ponadto mówimy, że para $(X, \mathcal{O}_X)$ jest **lokalną przestrzenią ze snopem** o ile dla każdego punktu $P \in X$ kiełek $\mathcal{O}_{X,P} = \varinjlim_{P \in U} \mathcal{O}_X(U)$ jest pierścieniem lokalnym, tzn. ma jeden ideał maksymalny.

Para $(f, f^\#) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ jest **morfizmem lokalnych przestrzeni ze snopem** jeżeli jest morfizmem przestrzeni ze snopem i dla każdego $P \in X$ indukowany homomorfizm $f^\#_P : \mathcal{O}_{Y,f(P)} \to \mathcal{O}_{X,P}$ spełnia warunek

$$f^\#_P(\mathfrak{m}_{Y,f(P)}) = \mathfrak{m}_{X,P}$$

dla ideałów maksymalnych w $\mathcal{O}_{Y,f(P)}$ i $\mathcal{O}_{X,P}$.

Definicja 4.1.5 (Schemat afiniczny)**.** Niech R będzie pierścieniem przemiennym z jedynką. Niech

$$\mathrm{Spec}(R) = \{\mathfrak{p} : \mathfrak{p} \text{ jest ideałem pierwszym w } R\}$$

będzie przestrzenią topologiczną z topologią Zariskiego, tj. bazę zbiorów otwartych tworzą $D(f) = \{\mathfrak{p} \in \mathrm{Spec}(R) : f \notin \mathfrak{p}\}$ dla dowolnego $f \in R$.

Przestrzeń $X = \mathrm{Spec}(R)$ wyposażamy w snop pierścieni $\mathcal{O}_X$ zadany na zbiorze otwartym $U \subset X$ następująco:

$$\mathcal{O}_X(U) = \{s : U \to \coprod_{\mathfrak{p} \in U} R_{\mathfrak{p}} \mid s(\mathfrak{p}) \in R_{\mathfrak{p}} \text{ dla dow.} \mathfrak{p} \in U \text{ i } s \text{ jest lok. stała}\}.$$

Pierścień $R_{\mathfrak{p}}$ oznacza lokalizację R na ideale $\mathfrak{p}$. Ponadto funkcja

$$s : U \to \coprod_{\mathfrak{p} \in U} R_{\mathfrak{p}}$$

jest lokalnie stała, gdy dla każdego ideału $\mathfrak{p} \in U$ istnieje otoczenie otwarte $V \subset U$ zawierające $\mathfrak{p}$ takie, że istnieją elementy $a, f \in R$ spełniające:

$$s(\mathfrak{q}) = \frac{a}{f} \in R_{\mathfrak{q}}$$

dla każdego ideału pierwszego $\mathfrak{q} \in V$ takiego, że $f \notin \mathfrak{q}$.

Definicja 4.1.6 (Schemat)**.** Schematem nazywamy parę $(X, \mathcal{O}_X)$, która jest lokalną przestrzenią ze snopem taką, że każdy punkt $P \in X$ posiada otoczenie otwarte $U \subset X$ takie, że para $(U, \mathcal{O}_X \mid_U)$ jest schematem afinicznym.

Morfizmem schematów nazywamy morfizm odpowiadających im lokalnych przestrzeni ze snopem.

Uwaga 4.1.7. Często dla uproszczenia notacji schemat $(X, \mathcal{O}_X)$ będziemy oznaczać przez X pomijając (o ile jest to jednoznaczne z kontekstu) oznaczenie snopa $\mathcal{O}_X$.

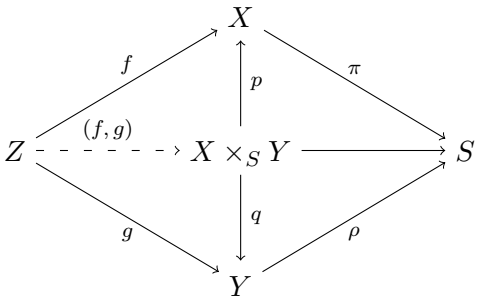
Definicja 4.1.8 (S-schemat)**.** Niech S będzie schematem. **S-schematem** lub **schematem nad S** będziemy nazywali schemat X wyposażony w morfizm schematów $\pi : X \to S$. Ponadto jeśli $S = \mathrm{Spec}(R)$ to będziemy pisali R-schemat zamiast $\mathrm{Spec}(R)$-schemat.

Jeśli $\pi : X \to S$ i $\rho : Y \to S$ są S-schematami, to morfizmem S-schematów będziemy nazywali morfizm schematów $f : X \to Y$, który spełnia równość $\rho \circ f = \pi$.

Definicja 4.1.9 (Produkt rozwłókniony)**.** Niech S będzie schematem oraz niech $\pi : X \to S$ oraz $\rho : Y \to S$ będą S-schematami. Wówczas **produktem rozwłóknionym** X i Y nad S nazywamy S-schemat $X \times_S Y$ wraz z dwoma S-morfizmami:

$$p : X \times_S Y \to X,$$
$$q : X \times_S Y \to Y$$

nazywanymi **projekcjami**. Schemat $X \times_S Y$ spełnia następujący warunek uniwersalności: dla dowolnych S-morfizmów $f : Z \to X$ i $g : Z \to Y$ istnieje jedyny S-morfizm $(f, g) : Z \to X \times_S Y$ taki, że następujący diagram jest przemienny.



Twierdzenie 4.1.10 ([Har06, Thm.3.3],Istnienie produktu rozwłóknionego)**.** *Niech X, Y będą S-schematami. Wówczas istnieje produkt rozwłókniony $(X \times_S Y, p, q)$ i jest jedyny z dokładnością do izomorfizmu S-schematów. Ponadto jeśli $S = \mathrm{Spec}(R)$, $X = \mathrm{Spec}(R_1)$ i $Y = \mathrm{Spec}(R_2)$, to $X \times_S Y = \mathrm{Spec}(R_1 \otimes_R R_2)$.*

Definicja 4.1.11 (Domknięta immersja)**. Domkniętą immersją** nazywamy morfizm schematów $(f, f^{\#}) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ taki, że $f : X \to Y$ jest homeomorfizmem X na obraz $f(Y)$ oraz odwzorowanie $f^{\#} : \mathcal{O}_Y \to f_*\mathcal{O}_X$ jest surjekcją , tj. dla każdego $P \in X$ homomorfizm pierścieni lokalnych $f_P^{\#} : \mathcal{O}_{Y,f(P)} \to f_*\mathcal{O}_{X,P}$ jest surjekcją.

Definicja 4.1.12 (Morfizm rozdzielony, schemat rozdzielony)**.** Niech $f : X \to Y$ będzie morfizmem schematów. Istnieje jedyny morfizm $\Delta_{X/Y} = (id_X, id_X) : X \to X \times_Y X$ (patrz Definicja 4.1.9 dla $f = g = id_X$ i $\pi = \rho = f$). Mówimy, że **morfizm f jest rozdzielony** jeśli morfizm $\Delta_{X/Y}$ jest domkniętą immersją. Ponadto mówimy wówczas, że **schemat X jest rozdzielony** nad Y. W szczególności jeśli $Y = \mathrm{Spec}(\mathbb{Z})$, to mówimy, że **schemat X jest rozdzielony**.

Definicja 4.1.13 (Schemat całkowity)**.** Schemat X nazywamy **całkowitym** jeśli dla każdego otwartego $U \subset X$, pierścień $\mathcal{O}_X(U)$ jest dziedziną całkowitości.

Twierdzenie 4.1.14 ([Har06, II,Prop.3.1])**.** *Schemat X jest całkowity wtedy i tylko wtedy, gdy X jest nierozkładalny jako przestrzeń topologiczna i dla każdego otwartego $U \subset X$ pierścień $\mathcal{O}_X(U)$ nie ma elementów nilpotentnych.*

Definicja 4.1.15 (Rozmaitość algebraiczna)**.** Niech k będzie ciałem i niech k-schemat X będzie rozdzielony oraz $X \times_{\mathrm{Spec}(k)} \mathrm{Spec}(\overline{k})$ jest całkowity.

Schemat X jest **rozmaitością afiniczną** nad k, gdy $X = \mathrm{Spec}(R)$, o ile R jest skończenie generowaną k-algebrą.

Schemat X jest **rozmaitością algebraiczną** nad k jeśli istnieje skończone otwarte pokrycie $X = \bigcup_i X_i$ takie, że $(X_i, \mathcal{O}_X \mid_{X_i})$ są rozmaitościami afinicznymi nad k.

Definicja 4.1.16 (Przestrzeń rzutowa, rozmaitość rzutowa)**.** Niech R będzie pierścieniem przemiennym z jedynką i $n \geq 0$ ustaloną liczbą całkowitą. Dla każdego $0 \leq i \leq n$ ustalamy zbiory:

$$X_i = \mathrm{Spec}(R[T_i^{-1}T_j]_{0 \leq j \leq n}),$$

$$X_{ij} = D(T_i^{-1}T_j) \subseteq X_i.$$

Ze względu na równości

$$\mathcal{O}_{X_i}(X_{ij}) = R[T_i^{-1}T_j, T_j^{-1}T_i, T_i^{-1}T_k]_{0\leq k\leq n} = \mathcal{O}_{X_j}(X_{ji}),$$

schematy afiniczne X_{ij} i X_{ji} są izomorficzne. Możemy skleić R-schemat wzdłuż X_{ij}. Otrzymany w rezultacie schemat nazywamy **przestrzenią rzutową nad R** wymiaru n i oznaczamy $\mathbb{P}^n_R$.

Rozmaitością rzutową nad ciałem k nazywamy domknięty podschemat schematu $\mathbb{P}^n_k$ dla pewnego $n \geq 0$.

Definicja 4.1.17. Schemat X jest **noetherowski** jeśli jest sumą skończenie wielu schematów afinicznych X_i takich, że pierścienie $\mathcal{O}_X(X_i)$ są noetherowskie.

Mówimy, że schemat X jest **lokalnie noetherowski**, gdy każdy punkt $x \in X$ posiada otoczenie U, które jest schematem noetherowskim.

Definicja 4.1.18 (Schemat regularny)**.** Niech X będzie schematem i $x \in X$. Przez $\mathfrak{m}_x$ oznaczmy jedyny ideał maksymalny w pierścieniu lokalnym $\mathcal{O}_{X,x}$. **Ciałem reszt** nazywamy ciało $k(x) = \mathcal{O}_{X,x}/\mathfrak{m}_x$. Określmy przestrzeń $k(x)$-liniową $m_x/m_x^2 = m_x \otimes_{\mathcal{O}_{X,x}} k(x)$. **Przestrzenią styczną w sensie Zariskiego** nazywamy przestrzeń $k(x)$-liniową:

$$T_{X,x} = Hom_{k(x)}(m_x/m_x^2, k(x)).$$

Mówimy, że schemat lokalnie noetherowski X jest **regularny w punkcie** $x \in X$ jeśli $\dim \mathcal{O}_{X,x} = \dim_{k(x)} T_{X,x}$. Jeżeli schemat X jest regularny w każdym punkcie, to mówimy, że jest on **regularny**.

Mówimy ponadto, że schemat X jest **gładki nad k** jeśli schemat $X \times_{\mathrm{Spec}(k)} \mathrm{Spec}(\overline{k})$ jest regularny.

W praktyce, lokalnie wokół każdego punktu x na rozmaitości X możemy znaleźć otwarte otoczenie afiniczne U takie, że $X \cap U$ jest domkniętą podrozmaitością $Z = V(I)$ w $\mathbb{A}^n_k$ i generujący ją ideał jest zadany przez wielomiany $F_1, \ldots, F_r$. Niech $x \in Z(k)$. Dana jest macierz:

$$J_x = \left(\frac{\partial F_i}{\partial T_j}(x)\right)_{1\leq i\leq r, 1\leq j\leq n}.$$

Wówczas X jest regularny w punkcie x wtedy i tylko wtedy, gdy:

$$\mathrm{rz} J_x = n - \dim \mathcal{O}_{X,x}.$$

Definicja 4.1.19 (Wymiar schematu, kowymiar schematu)**.** Niech $(X, \mathcal{O}_X)$ będzie schematem. **Wymiarem schematu** nazywamy liczbę $\dim X$ równą wymiarowi topologicznemu przestrzeni, tj. supremum po wszystkich liczbach naturalnych n takich, że istnieje łańcuch:

$$Z_0 \subset Z_1 \subset \ldots \subset Z_n$$

parami różnych nieredukowalnych (nierozkładalnych na sumę właściwych zbiorów domkniętych) zbiorów domkniętych w X.

Niech Z będzie nierozkładalnym domkniętym podzbiorem w X, wtedy **kowymiarem** Z w X, oznaczanym $\operatorname{codim}(Z, X)$ nazywamy supremum liczb naturalnych n takich, że istnieje ciąg:

$$Z = Z_0 \subset Z_1 \subset \ldots \subset Z_n$$

nierozkładalnych, parami różnych podzbiorów domkniętych w X.

Jeśli Y jest dowolnym zbiorem domkniętym w X, to definiujemy:

$$\operatorname{codim}(Y, X) = \inf_{Z \subset Y} \operatorname{codim}(Z, X),$$

gdzie inf bierzemy po zbiorach $Z \subset Y$ domkniętych i nierozkładalnych.

Definicja 4.1.20 (S-schemat grupowy)**.** Niech S będzie schematem. **Schematem grupowym** nad S nazywamy S-schemat G wyposażony w następujące S-morfizmy:

$$\begin{aligned} \text{mnożenie } & m : G \times_S G \to G, \\ \text{identyczność } & \varepsilon : S \to G, \\ \text{odwrotność } & \operatorname{inv} : G \to G \end{aligned}$$

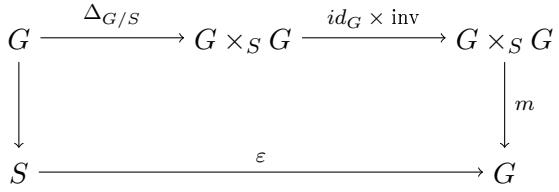
takie, że przemienne są następujące diagramy:

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

Rysunek 4.1: Łączność

$$\begin{array}{ccc} G \times_S S & \xrightarrow{id_G \times \varepsilon} & G \times_S G \\ & \searrow^{id_G} & \downarrow{\scriptstyle m} \\ & & G \end{array}$$

Rysunek 4.2: Prawa identyczność



Rysunek 4.3: Prawa odwrotność

W szczególności dla dowolnego S-schematu $\pi : T \to S$ zbiór $G(T) = \mathrm{Mor}_S(T, G)$ wszystkich S-morfizmów z T do G ma strukturę grupy z identycznością $(\varepsilon, \pi) : S \times_S T \to G \times_S T$ i indukowaną z m mapą $m(T) : G(T) \times G(T) \to G(T)$ oraz pochodzącym od inv odwzorowaniem $\mathrm{inv}(T) : G(T) \to G(T)$.

Definicja 4.1.21 (Grupa algebraiczna)**.** Niech k będzie ciałem i niech dany będzie k-schemat X, który jest rozmaitością algebraiczną nad k. Rozmaitość X nazywamy **grupą algebraiczną** nad k jeśli jest k-schematem grupowym.

Wniosek 4.1.22. *Grupa algebraiczna G nad k jest gładka nad k.*

Dowód. Na mocy [Liu02, Lemm.4.2.21] G zawiera punkt regularny domknięty, czyli w kosekwencji schemat jest gładki nad k w tym punkcie. Używając morfizmu translacji o punkt domknięty otrzymujemy, że w każdym punkcie domkniętym schemat G jest gładki i skoro punkty $G(\overline{k})$ są gęste w schemacie G, to cały schemat jest gładki. □

Definicja 4.1.23 (Rozmaitość abelowa)**.** Grupę algebraiczną określoną nad ciałem k, która jest rozmaitością rzutową, nazywamy **rozmaitością abelową** zdefiniowaną nad k.

Twierdzenie 4.1.24 ([CS86, Milne,Sec.2,7])**.** *Rozmaitość abelowa X nad k jest przemienna, tzn. zbiór $X(L) = X(Spec(L))$ jest przemienną grupą dla każdego rozszerzenia ciał L/k, $L \subset \overline{k}$.*

Definicja 4.1.25 (Krzywa eliptyczna)**. Krzywą eliptyczną** nazywamy rozmaitość abelową E nad ciałem k wymiaru 1. W szczególności zbiór $E(k)$ zawiera identyczność $\varepsilon : \mathrm{Spec}(k) \to E$ oraz określone jest odwzorowanie $m(k) : E(k) \times E(k) \to E(k)$, które zadaje działanie w grupie abelowej $E(k)$. Ponadto schemat E jest gładki nad k.

4.2 Systemy liniowe i dywizory

Definicja 4.2.1 (Dywizor Weila)**.** Niech X będzie noetherowskim, rozdzielonym i całkowitym schematem, który jest regularny w kowymiarze 1 (tzn. dla każdego $x \in X$ takiego, że $\mathcal{O}_{X,x}$ jest wymiaru 1 zachodzi $\dim \mathcal{O}_{X,x} = \dim_{k(x)} T_{X,x}$).

Dywizorem pierwszym na X nazywamy domknięty nieredukowalny schemat $Y \subset X$ kowymiaru 1 w X.

Dywizorem Weila nazywamy element grupy abelowej wolnej $\mathrm{Div}(X)$ generowanej przez wszystkie dywizory pierwsze, tj. $D \in \mathrm{Div}(X)$ można zapisać

w postaci skończonej sumy $D = \sum_i n_i Y_i$, gdzie Y_i są dywizorami pierwszymi, a n_i są liczbami całkowitymi.

Niech Y będzie dywizorem pierwszym na X. Jeśli $\eta \in Y$ spełnia $\overline{\{\eta\}} = Y$ (jest punktem generycznym), to pierścień $\mathcal{O}_{\eta,X}$ jest pierścieniem z waluacją dyskretną v_Y i ciałem ułamków $K = K(X) = \mathrm{Frac}(\mathcal{O}_{X,\eta})$.

Lemat 4.2.2 ([Har06, II,Lemm.6.1]). *Niech X będzie noetherowskim, rozdzielonym i całkowitym schematem, regularnym w kowymiarze 1 i niech $f \in K^\times$. Wówczas $v_Y(f) = 0$ dla prawie wszystkich dywizorów pierwszych Y.*

Definicja 4.2.3 (Dywizor funkcji, liniowa równoważność dywizorów)**.** Niech X będzie noetherowskim, rozdzielonym i całkowitym schematem regularnym w kowymiarze 1 i niech $f \in K^\times$. **Dywizorem funkcji** f będziemy nazywać element $(f) \in \mathrm{Div}(X)$ postaci

$$(f) = \sum_Y v_Y(f) Y,$$

gdzie suma jest wzięta po wszystkich dywizorach pierwszych Y w X. Dywizory funkcji tworzą podgrupę w $\mathrm{Div}(X)$.

Dwa dywizory $D, D' \in \mathrm{Div}(X)$ nazywamy **liniowo równoważnymi** i piszemy $D \sim D'$ jeżeli ich różnica jest dywizorem pewnej funkcji. Grupę $\mathrm{Div}(X)/\{\text{grupa dywizorów funkcji}\}$ nazywamy **grupą klas dywizorów** i oznaczamy $\mathrm{Cl}(X)$.

Definicja 4.2.4 (Dywizor Cartier)**.** Niech X będzie rozmaitością algebraiczną nad ciałem k. Dywizorem Cartier będziemy nazywali klasę równoważności zbiorów par $\{(U_i, f_i)\}$ spełniających warunki:

(i) Zbiory otwarte U_i pokrywają X.

(ii) Elementy f_i należą do $K(X)^\times$.

(iii) Dla dowolnych i, j zachodzi $f_i f_j^{-1} \in \mathcal{O}_X(U_i \cap U_j)^\times$.

Dwie rodziny $\{(U_i, f_i)\}$ i $\{(V_j, f_j)\}$ uważamy za równoważne jeśli $f_i g_j^{-1} \in \mathcal{O}_X(U_i \cap V_j)^*$ dla wszystkich i, j.

Dywizory Cartier możemy dodawać w następujący sposób:

$$\{(U_i, f_i)\} + \{(V_j, f_j)\} := \{(U_i \cap V_j, f_i g_j)\}.$$

Z tą operacją dywizory Cartier tworzą grupę oznaczaną symbolem $\mathrm{CaDiv}(X)$.

Ponadto dywizor $\mathrm{div}(f) = \{(U, f)\}$ nazywać będziemy dywizorem funkcji $f \in K(X)^\times$.

Dywizory funkcji tworzą podgrupę w grupie dywizorów Cartier i grupę ilorazową $\mathrm{CaDiv}(X)/\{\text{dywizory funkcji}\}$ będziemy nazywać grupą klas $\mathrm{Pic}(X)$. Dywizory D, D' z tej samej klasy równoważności nazywamy liniowo równoważnymi, co oznaczamy symbolem $D \sim D'$.

Nośnikiem dywizora $D = \{(U_i, f_i)\}$ nazywamy zbiór:

$$\mathrm{Supp}(D) = \bigcup_i \{x \in U_i \mid f_i \notin \mathcal{O}_{X,x}^*\}.$$

Twierdzenie 4.2.5 ([Har06, II,Prop.6.11]). *Niech X będzie rozmaitością algebraiczną gładką nad k. Wówczas odwzorowanie:*

$$\mathrm{CaDiv}(X) \to \mathrm{Div}(X)$$

$$\{(U_i, f_i)\} \mapsto \sum_Y v_Y(f_i)Y,$$

gdzie suma jest wzięta po dywizorach pierwszych oraz $v_Y(f_i) = 0$ jeśli $Y \cap U_i = \emptyset$, jest izomorfizmem odwzorowującym grupę dywizorów funkcji w $\mathrm{CaDiv}(X)$ na grupę dywizorów funkcji w $\mathrm{Div}(X)$.

Ostatnie twierdzenie pozwala nam utożsamiać obie grupy dywizorów dla rozmaitości gładkich. Niektóre konstrukcje piszą się prościej w języku dywizorów Weila, a inne w języku dywizorów Cartier. Przykładem jest poniżej zdefiniowane cofnięcie dywizora.

Definicja 4.2.6 (Cofnięcie dywizora)**.** Niech $g : X \to Y$ będzie morfizmem k-rozmaitości i niech $D = \{(U_i, f_i)\} \in \mathrm{CaDiv}(Y)$. Przypuśćmy, że $g(X)$ nie jest zawarte w $\mathrm{Supp}(D)$. Wówczas istnieje dywizor $g^*(D) \in \mathrm{CaDiv}(X)$ zdefiniowany następująco:

$$g^*(D) = \{(g^{-1}(U_i), f_i \circ g\}.$$

Zachodzą własności $g^*(D + E) = g^*(D) + g^*(E)$ oraz $(f \circ g)^* = g^* \circ f^*$.

Lemat 4.2.7 ([HS00, Lemm.A.2.2.5,Prop.A.2.2.6])**.** *Niech $f : X \to Y$ będzie morfizmem rozmaitości. Jeśli $D, D' \in \mathrm{CaDiv}(Y)$ są liniowo równoważne i $f(X)$ nie jest zawarty w $\mathrm{Supp}(D) \cup \mathrm{Supp}(D')$, to $f^*(D) \sim f^*(D')$.*

Ponadto dla każdego dywizora $D \in \mathrm{CaDiv}(Y)$ istnieje pewien dywizor $D' \in \mathrm{CaDiv}(Y)$ spełniający:

$$D \sim D' \text{ oraz } f(X) \not\subset \mathrm{Supp}(D').$$

W szczególności odwzorowanie f indukuje $f^* : \mathrm{CaDiv}(Y) \to \mathrm{CaDiv}(X)$, które jest dobrze określone dla D takich, że $f(X) \not\subset \mathrm{Supp}(D)$, a to indukuje dobrze określony homomorfizm grup:

$$f^* : \mathrm{Pic}(Y) \to \mathrm{Pic}(X).$$

Twierdzenie Riemanna-Rocha

Definicja 4.2.8. Niech X będzie rozmaitością gładką nad k, a D dywizorem określonym nad k (tzn. niezmienniczym ze względu na działanie grupy $\mathrm{Gal}(\overline{k}/k)$ na punktach $X(\overline{k})$ rozmaitości X). Przez $L_K(D)$ będziemy oznaczali przestrzeń liniową:

$$L_K(D) = \{f \in K(X)^* \mid D + \mathrm{div}(f) \geq 0\} \cup \{0\}$$

dla $k \subseteq K \subseteq k^{\mathrm{sep}}$ oraz $K(X) = \mathrm{Frac}(\mathcal{O}_{X,\eta} \otimes_k K)$. Ponadto wymiar tej przestrzeni liniowej nad k oznaczamy przez $l_K(D)$.

Twierdzenie 4.2.9 ([HS00, Prop.A.2.2.10]). *Niech k będzie ciałem doskonałym. Wówczas zachodzi równość:*

$$L_k(D) \otimes_k \overline{k} = L_{\overline{k}}(D)$$

dla dowolnej rozmaitości X nad k i dywizora D zdefiniowanego nad k. W szczególności można wybrać bazę $L_{\overline{k}}(D)$ sposród elementów należących do $k(X)$.

Twierdzenie 4.2.10. *Niech X będzie rozmaitością nad $k = \overline{k}$ i oznaczmy $L(D) = L_{\overline{k}}$, a $D, D' \operatorname{Div}(X)$. Wówczas:*

(i) Zachodzi inkluzja $k \subset L(D)$ wtedy i tylko wtedy, gdy $D \geq 0$.

(ii) Jeśli $D \leq D'$, to $L(D) \subset L(D')$.

(iii) Jeśli $D' = D + div(g)$, to odwzorowanie $f \mapsto gf$ jest izomorfizmem przestrzeni liniowych $L(D')$ i $L(D)$.

Twierdzenie 4.2.11 ([HS00, Cor.A.3.2.7]). *Niech X będzie rozmaitością rzutową nad ciałem k. Jeśli D jest dywizorem na X, to wymiar $l_k(D) = \dim L_k(D)$ jest skończony.*

O przestrzeni $L(D)$ możemy powiedzieć więcej jeśli X jest krzywą.

Twierdzenie 4.2.12 ([HS00, Thm.A.4.2.1],Riemann-Roch). *Niech C będzie gładką krzywą rzutową nad ciałem $k = \overline{k}$. Wówczas istnieje liczba naturalna $g \geq 0$ taka, że dla dowolnego dywizora $D \in Div(C)$ określonego nad k zachodzi:*

$$l_k(D) - l_k(K_C - D) = \deg(D) - g + 1,$$

gdzie K_C jest dywizorem pochodzącym od niezerowej formy różniczkowej na C, natomiast $\deg(\sum n_i Y_i) = \sum n_i$.

Definicja 4.2.13 (Genus krzywej gładkiej). **Genusem** krzywej gładkiej C nazywamy liczbę g określoną w powyższym twierdzeniu.

Twierdzenie 4.2.14. *Niech C będzie krzywą gładką genusu g nad ciałem k, doskonałym i domkniętym algebraicznie. Wówczas zachodzą własności (niech $l(D) := l_k(D)$):*

(i) Wymiar $l(K_C) = g$ oraz $\deg K_C = 2g - 2$.

(ii) Jeśli $\deg(D) < 0$, to $l(D) = 0$.

(iii) Jeśli $\deg(D) \geq 2g - 1$, to $l(D) = \deg(D) - g + 1$.

(iv) Jeśli $l(D) \neq 0$ i $l(K_C - D) \neq 0$, to $l(D) \leq \frac{1}{2}\deg(D) + 1$.

Systemy liniowe

Definicja 4.2.15 (Zupełny system liniowy)**.** Niech X będzie rozmaitością. **Zupełnym systemem liniowym** $|D|$ stowarzyszonym z dywizorem $D \in \mathrm{Div}(X)$ nazywamy zbiór wszystkich dywizorów efektywnych D' (tzn. $D' = \sum_i n_i Y_i$ i $n_i \geq 0$) liniowo równoważnych z D.

Zbiorem **punktów bazowych** zupełnego systemu liniowego $|D|$ nazywamy przekrój wszystkich nośników dywizorów zawartych w $|D|$. System liniowy $|D|$ nazywamy **systemem bez punktów bazowych** jeśli przekrój ten jest pusty. Ponadto mówimy, że dywizor D **nie ma punktów bazowych** jeśli stowarzyszony z nim system liniowy $|D|$ nie ma punktów bazowych.

Definicja 4.2.16 (Odwzorowanie stowarzyszone z dywizorem)**.** Niech X będzie rozmaitością rzutową i $D \in \mathrm{Div}(X)$. Wówczas istnieje skończona baza przestrzeni $L(D)$: $f_0, \ldots, f_n$. **Odwzorowaniem stowarzyszonym** z D nazywamy przekształcenie:

$$\phi_D : X \to \mathbb{P}^n$$

$$\phi_D : x \mapsto (f_0(x), \ldots, f_n(x)).$$

Dywizor D nazywamy **bardzo szerokim** jeśli ϕ_D jest injekcją, której obrazem jest zbiór domknięty w $\mathbb{P}^n$ oraz indukuje injekcję na poziomie przestrzeni stycznych $\phi_{D,x} : T_x X \to T_{\phi_D(x)}\mathbb{P}^n$, natomiast jeśli nD jest bardzo szeroki dla pewnego $n \geq 1$ to D nazywamy **dywizorem szerokim**.

Twierdzenie 4.2.17 ([BG06, A.6.10])**.** *Dowolny dywizor może być zapisany jako różnica dwóch dywizorów bardzo szerokich. Dokładniej jeśli D jest ustalonym dywizorem, a H dowolnym bardzo szerokim dywizorem to:*

(a) Istnieje stała $m \geq 0$ taka, że $D + mH$ jest dywizorem bez punktów bazowych.

(b) Jeśli D jest dywizorem bez punktów bazowych, to $D + H$ jest bardzo szeroki.

Stwierdzenie 4.2.18 (Hindry-Silverman A.3.2.4)**.** *Niech $f : X \to Y$ będzie morfizmem rozmaitości rzutowych. Jeśli D jest dywizorem bez punktów bazowych w Y, to f^*D jest dywizorem bez punktów bazowych w X.*

Dywizory na rozmaitościach abelowych

Definicja 4.2.19 (Izogenia)**.** Homomorfizm ϕ dwóch rozmaitości abelowych A, B nad ciałem k, tego samego wymiaru spełniający warunek surjektywności:

$$\phi(A(\overline{k})) = B(\overline{k})$$

nazywamy **izogenią**.

Twierdzenie 4.2.20 (Wzór Mumforda, [HS00, Cor.A.7.2.5])**.** *Niech D będzie dywizorem na rozmaitości abelowej A oraz niech $[n] : A \to A$ będzie morfizmem mnożenia przez n. Wówczas:*

$$[n]^*D \sim \left(\frac{n^2+n}{2}\right) D + \left(\frac{n^2-n}{2}\right) [-1]^*D.$$

Twierdzenie 4.2.21. *Niech A będzie rozmaitością abelową wymiaru g zdefiniowaną nad ciałem algebraicznie domkniętym K charakterystyki $p \geq 0$.*

(i) Morfizm mnożenia przez n $[n] : A \to A$ jest izogenią stopnia n^{2g}.

(ii) Jeśli $p = 0$ lub $p \nmid n$, to :

$$A[n] = ker[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}.$$

(iii) Jeśli $p > 0$, to istnieje liczba całkowita $0 \leq r \leq g$ taka, że dla dowolnego $t \geq 1$ $A[p^t] \cong (\mathbb{Z}/p^t\mathbb{Z})^r$.

Twierdzenie 4.2.22. *Niech A będzie rozmaitością abelową. Definiujemy morfizmy $\sigma, \delta, \pi_1, \pi_2 : A \times A \to A$ określone wzorami $\sigma(x, y) = x+y$, $\delta(x, y) = x-y$, $\pi_1(x, y) = x$ oraz $\pi_2(x, y) = y$. Wówczas dla dowolnej klasy $c \in Cl(A)$ następujące warunki są równoważne:*

(i) $[-1]^*c = c$

(ii) $\sigma^*c + \delta^*c = 2\pi_1^*c + \pi_2^*c$

Uwaga: w przypadku rozważania grupy dywizorów Div powyższe równości klas dywizorów przechodzą w relacje liniowej równoważności $\sim$ pomiędzy nimi.

Twierdzenie 4.2.23 ([BG06, Prop. 8.6.4])**.** *Niech A/K będzie rozmaitością abelową nad ciałem K. Wówczas istnieje dywizor $D \in Div(A)$, który jest bardzo szeroki. Równoważnie istnieje zanurzenie $A \hookrightarrow \mathbb{P}^n$.*

Ponadto dywizor $C = D + [-1]^*D$ jest bardzo szeroki oraz symetryczny, tj. $C \sim [-1]^*C$.

Rozmaitość abelowa dualna

Definicja 4.2.24 (Składowa spójna w Pic(A), grupa NS(A))**.** Niech A będzie rozmaitością abelową. Grupę dywizorów niezmienniczych na translacje o punkt domknięty z A będziemy oznaczali $\mathrm{Pic}^0(A)$:

$$\mathrm{Pic}^0(A) = \{c \in \mathrm{Pic}(A) \mid t_a^*c = c \text{ dla dowolnego punktu domkniętego } a \in A\},$$

gdzie $t_a : A \to A$ jest translacją o punkt domknięty $a \in A$. Grupą Nérona-Severiego rozmaitości A oznaczaną $\mathrm{NS}(A)$ nazywamy grupę ilorazową

$$\mathrm{Pic}(A)/\mathrm{Pic}^0(A).$$

Fakt 4.2.25. *Niech A, B będą rozmaitościami abelowymi nad ciałem k. Wówczas iloczyn rozwłókniony $A \to Spec(k)$ i $B \to Spec(k)$ postaci $A \times_{Spec(k)} B$ jest rozmaitością abelową*

Dowód. Wynika to z definiji rozmaitości abelowej jako schematu oraz zachowania własności całkowitości i zupełności schematu przy braniu produktów. □

Twierdzenie 4.2.26. *Niech A będzie rozmaitością abelową. Istnieje wówczas rozmaitość $\hat{A}$ oraz klasa dywizorów $\mathcal{P} \in Pic(A \times \hat{A})$ taka, że odwzorowania:*

$$\hat{A} \to Pic^0(A) : \hat{a} \mapsto i_{\hat{a}}^*(\mathcal{P}),$$

$$A \to Pic^0(\hat{A}) : a \mapsto i_a^*(\mathcal{P})$$

są bijekcjami. Odwzorowanie $i_{\hat{a}} : A \to A \times \hat{A}$ odwzorowuje $i_{\hat{a}}(a) = (a, \hat{a})$. Podobnie definiujemy odwzorowanie $i_a : \hat{A} \to A \times \hat{A}$, $i_a(\hat{a}) = (a, \hat{a})$.

Rozmaitość $\hat{A}$ spełniająca powyższe własności i klasa $\mathcal{P}$ (symetryczna) są jedyne z dokładnością do izomorfizmu rozmaitości abelowych.

Definicja 4.2.27 (Rozmaitość dualna)**.** Niech A będzie rozmaitością abelową i $\hat{A}$ będzie określona jak w twierdzeniu powyżej. Rozmaitość abelową $\hat{A}$ nazywamy **rozmaitością abelową dualną** do A, a każdy dywizor z klasy $\mathcal{P}$ nazywamy **dywizorem Poincarégo**.

Dalsze własności krzywych eliptycznych

W poniższym paragrafie omówimy pokrótce konstrukcję modelu Weierstrassa krzywej eliptycznej i pokażemy jak w naturalny sposób skonstruować działanie grupowe i podamy jego interpretację geometryczną, która umożliwi nam późniejsze praktyczne obliczenia na punktach krzywej.

Twierdzenie 4.2.14 pociąga, że dywizor kanoniczny K_E dla rozmaitości abelowej E wymiaru 1 jest równy 0. Stosując Twierdzenie 4.2.12 dla dowolnego efektywnego dywizora $D \geq 0$ otrzymamy, że $l_k(D) = deg(D)$. W szczególności z definicji krzywej eliptycznej wynika, że istnieje punkt $P_0 \in E(k)$ i dla $n \geq 1$ zachodzi:

$$\dim L_k(nP_0) = n.$$

Poniżej skonstruujemy z pewnych wybranych elementów z $L_n = L_k(nP_0)$ funkcje, które na punktach domkniętych schematu będą przyjmować wartości w rozszerzeniach ciała k. Dokładniej, dla każdego punktu domkniętego $x \in E$ element $f \in \mathcal{O}_X(U)$ dla $x \in U$ przyjmuje wartość:

$$f(x) = \bar{f} \in \mathcal{O}_{X,x}/\mathfrak{M}_x,$$

który jest obrazem f przy odwzorowaniu kanonicznym:

$$\mathcal{O}_X(U) \to \mathcal{O}_{X,x}/\mathfrak{M}_x = k(x).$$

Ponadto w przypadku rozmaitości algebraicznych ciało $k(x)$ jest skończonym rozszerzeniem k, czyli funkcje $f \in \mathcal{O}_X(U)$ na punktach domkniętych przyjmują zawsze wartości w ustalonym domknięciu $\overline{k}$.

Zerem funkcji $f \in \mathcal{O}_X(U)$ nazywamy punkt domknięty $x \in U$ dla którego wartość $f(x) = 0$. Podobnie jeśli $y \in X$, punkt domknięty i $y \notin U$, to funkcja $f \in \mathcal{O}_X(U)$ ma **biegun** w y jeśli f nie przedłuża się do funkcji $g \in \mathcal{O}_X(V)$ określonej w punkcie $x \in V$ i takiej, że $g \mid_{U \cap V} = f \mid_{U \cap V}$.

Można pokazać, że zachodzą następujące równości:

$$L_1 = k$$
$$L_2 = k \oplus kx$$
$$L_3 = k \oplus kx \oplus ky$$
$$L_4 = k \oplus kx \oplus ky \oplus kx^2$$
$$L_5 = k \oplus kx \oplus ky \oplus kx^2 \oplus kxy$$

Elementy $x, y \in k(E)$. Ponadto przestrzeń L_6 ma wymiar 6 i zawiera 7 funkcji:

$$1, x, x^2, x^3, y, xy, y^2 \in L_6.$$

Istnieje nietrywialna liniowa relacja między elementami. Analizując zera i bieguny poszczególnych z nich oraz wykorzystując bardzo szeroki system liniowy $|3P_0|$ dostajemy izomorfizm na obraz:

$$\phi : E \to \mathbb{P}^2_k$$

na punktach domkniętych $p \in E(\overline{k})$ postaci $\phi(p) = (1, x(p), y(p))$. Nietrywialna relacja zadaje rozmaitość algebraiczną w $\mathbb{P}^2_k$.

Ogólne równanie krzywej eliptycznej E w $\mathbb{P}^2_k$ przymuje postać:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{4.1}$$

gdzie $a_1, a_2, a_3, a_4, a_6 \in k$. Punkt $P_0 \in E(k)$ odwzorowuje się na $\phi(P_0) = (0, 1, 0)$ zwany **punktem w nieskończoności** (jest to jedyny punkt na krzywej (4.1) spełniający warunek $Z = 0$).

Przy założeniu, że $chark \neq 2, 3$ można sprowadzić równanie krzywej eliptycznej E w $\mathbb{P}^2_k$ do postaci:

$$Y^2Z = X^3 + AXZ + BZ^3.$$

Definicja 4.2.28 (Postać Weierstrassa)**.** Niech E będzie krzywą eliptyczną nad ciałem k. **Postacią Weierstrassa** krzywej nazywamy równanie w $\mathbb{P}^2_k$ postaci:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

definiujące krzywą gładką.

Skróconą postacią Weierstrassa krzywej E nad ciałem k charakterystyki różnej od 2 i 3 nazywamy równanie:

$$Y^2Z = X^3 + AXZ + BZ^3.$$

W szczególności na części afinicznej $\mathbb{P}^2_k$ zadanej przez $Z = 1$ dostaniemy odpowiednie równania afiniczne krzywej eliptycznej.

Definiujemy stowarzyszone z równaniem

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

pomocnicze funkcje:

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ c_4 &= b_2^2 - 24b_4, \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \\ j &= \frac{c_4^3}{\Delta}. \end{aligned}$$

Definicja 4.2.29 (Wyróżnik krzywej i j-niezmiennik krzywej eliptycznej)**.** **Wyróżnikiem krzywej eliptycznej** w postaci Weierstrassa nazywamy zdefiniowaną powyżej liczbę Δ.

Liczbę j określoną powyżej nazywamy **j-niezmiennikiem** krzywej eliptycznej w postaci Weierstrassa.

Twierdzenie 4.2.30 ([Sil86, III,Prop.1.4])**.** *Niech E będzie krzywą eliptyczną nad ciałem k. Wówczas krzywa E jest gładka wtedy i tylko wtedy, gdy $\Delta \neq 0$.*

Niech E i E' będą krzywymi nad ciałem k o j-niezmiennikach j i j' odpowiednio. Wówczas $E_{\overline{k}}$ i $E'_{\overline{k}}$ są izomorficzne wtedy i tylko wtedy, gdy $j = j'$.

Metodą siecznych można zdefiniować geometryczne dodawanie w zbiorze punktów $E(K)$ dla dowolnego rozszerzenia $k \subset K \subset \overline{k}$ (patrz [Sil86, III]).

Przykład 4.2.31 (Prawo dodawania na krzywej eliptycznej)**.** Niech E będzie krzywą eliptyczną nad ciałem k o afinicznej cześci w postaci Weierstrassa:

$$E_{aff} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Krzywą eliptyczną E będziemy utożsamiali z jej modelem rzutowym. Punkt $\mathcal{O} = (0, 1, 0)$ jest punktem w nieskończoności.

Wszystkie morfizmy rozmaitości algebraicznych będziemy poniżej definiować wyłącznie na punktach domkniętych.
(Element przeciwny)

$$\mathrm{inv} : E \to E$$

Niech $P_0 = (x_0, y_0) \in E(\overline{k})$. Definiujemy:

$$\mathrm{inv}(P_0) = \begin{cases} \mathcal{O} & P_0 = \mathcal{O} \\ (x_0, -y_0 - a_1x_0 - a_3) & P_0 \neq \mathcal{O} \end{cases}$$

(Dodawanie punktów)

$$m : E \times E \to E$$

Niech $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(\overline{k})$. Wówczas zachodzą 3 przypadki.
Jeśli $x_1 = x_2$ oraz $y_1 + y_2 + a_1x_2 + a_3 = 0$, to

$$m(P_1, P_2) = \mathcal{O}.$$

W przeciwnym przypadku, gdy $x_1 \neq x_2$, to mamy:

$$\begin{aligned} P_3 &= (x_3, y_3), \\ \lambda &= \frac{y_2 - y_1}{x_2 - x_1}, \\ \nu &= \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}, \\ x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \\ y_3 &= -(\lambda + a_1)x_3 - \nu - a_3 \end{aligned}$$

i $m(P_1, P_2) = P_3$.

Jeżeli $x_1 = x_2$, to definiujemy:

$$\begin{aligned} \lambda &= \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} \\ \nu &= \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} \end{aligned}$$

i formuły na x_3, y_3 identyczne jak w przypadku $x_1 \neq x_2$ oraz

$$m(P_1, P_2) = P_3.$$

Tak określone odwzorowania przedłużają się do morfizmów schematu grupowego E nad k. W szczególności dla każdego ciała $k \subset K \subset \overline{k}$ zbiór $E(K)$ jest grupą przemienną z identycznością $\mathcal{O}_K$ i dodawaniem oraz elementem przeciwnym określonymi powyższymi formułami.

Spis oznaczeń

$k(x)$ ciało reszt 84

$Div(X)$ dywizor Weila 86
$\{(U_i, f_i)\}$ dywizor Cartier 87
$div(f)$ dywizor funkcji 87

$CaDiv(X)$ grupa dywizorów Cartier 87
Pic(A) grupa Picarda rozmaitości abelowej A 91
Pic$^0(A)$ grupa Picarda dywizorów stopnia zero rozmaitości abelowej A 91

$H^1_S(G_{\overline{K}/K}, M)$ grupa klas nierozgałęzionych 52

j j-niezmiennik krzywej eliptycznej 93

$\mathcal{O}_{X,P}$ kiełek snopa w punkcie P 81

$D \sim D'$ liniowa równoważność dywizorów 87

$|\cdot|$ norma 81

ϕ_D odwzorowanie stowarzyszone z dywizorem D 89

$\mathcal{O}_{K,S}$ pierścień liczb S-całkowitych nad K 11
$X \times_S Y$ produkt rozwłókniony 82
$\mathbb{P}^n_R$ przestrzeń rzutowa 83
$L_K(D)$ przestrzeń lin. dywizorów dod. okr. liniowo równoważnych z D 88
$K(S, 2)$ grupa elementów parzystej waluacji poza S 62
f^* cofnięcie dywizora 88

$Sel^{(\alpha)}$ grupa Selmera 51
Ш grupa Szafarewicza-Tate'a 51
$\mathcal{O}_X$ snop strukturalny schematu 82
$Spec(R)$ spektrum pierścienia R 81

$Supp(D)$ nośnik dywizora D 87

$t(\cdot,\cdot)$ odwzorowanie Kummera 36
$\mu(\cdot,\cdot)$ główna przestrzeń jednorodna 52

K_v uzupełnienie ciała liczbowego względem normy v 10

ord_p waluacja p-adyczna 9
$\dim X$ wymiar schematu 84
Δ wyróżnik krzywej eliptycznej 93
H wysokość absolutna 13
$\hat{h}_{V,\phi,D}$ wysokość kanoniczna na V stow. z dywizorem D i morfizmem ϕ 26
H_K wysokość stowarzyszona z ciałem liczbowym 11

Indeks

Bibliografia

[BG71] P. Berthelot and A. Grothendieck. *Séminaire de Géométrie Algébrique du Bois Marie - 1966-67 - Théorie des intersections et théoreme de Riemann-Roch - (SGA 6)*. Springer-Verlag, 1971.

[BG02] G. Banaszak and W. Gajda. *Elementy algebry liniowej. Cz. 1.* Wydawnictwa Naukowo-Techniczne, 2002.

[BG06] E. Bombieri and W. Gubler. *Heights in Diophantine Geometry.* Cambridge University Press, 2006.

[BLR90] S. Bosch, W. Lütkebohmert, and M. Raynaud. *Néron Models.* Springer-Verlag, 1990.

[BM02] E. Brown and B. T. Myers. Elliptic curves from Mordell to Diophantus and back. *Am. Math. Mon.*, 109(7):639 – 649, 2002.

[BSD65] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. ii. *J. Reine Angew. Math.*, 218:79–108, 1965.

[Con06] B. Conrad. Chow's K/k-image and K/k-trace, and the Lang-Néron theorem. *Enseign. Math. (2)*, 52(1-2):37–108, 2006.

[Cre97] J. Cremona. *Algorithms for Modular Elliptic Curves.* Cambridge University Press, 1997.

[CS86] G. Cornell and J. H. Silverman. *Arithmetic Geometry.* Springer, 1986.

[Fal83] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Inventiones Mathematicae*, 73(3):349–366, 1983.

[Har06] Robin Hartshorne. *Algebraic Geometry.* Springer, 2006.

[HS00] M. Hindry and J. H. Silverman. *Diophantine Geometry: An Introduction.* Springer, 2000.

[Kah09] B. Kahn. Démonstration géometrique du théoréme de Lang-Néron et formules de Shioda-Tate. *Fields Inst. Commun.*, 56:149–155, 2009.

[KM05] K.Wentang and M. R. Murty. On a Conjecture of Birch and Swinnerton-Dyer. *Canad. J. Math.*, 57(2):328–337, 2005.

[Lan70] S. Lang. *Algebraic number theory.* Springer, 1970.

[Lan73] S. Lang. *Algebra.* Państwowe Wydawnictwo Naukowe, 1973.

[Liu02] Q. Liu. *Algebraic Geometry and Arithmetic Curves.* Oxford University Press, 2002.

[LN59] Serge Lang and André Néron. Rational points of abelian varieties over function fields. *Amer. J. Math.*, 81:95–118, 1959.

[Mes91] J.-F. Mestre. Courbes elliptiques de rang ≥ 11 sur $Q(t)$. *C. R. Acad. Sci. Paris Sér. I Math.*, 313(3):139–142, 1991.

[Nas10] B. Naskręcki. Infinite family of elliptic curves of rank at least 4. *Involve*, 3(3):297–316, 2010.

[Sil86] J. H. Silverman. *The Arithmetic of Elliptic Curves.* Springer, 1986.

[SS09] M. Schütt and T. Shioda. Elliptic surfaces. pages 1–93, 2009. arXiv:0907.0298v2.

[Ulm10] D. Ulmer. Explicit points on the Legendre curve. pages 1–8, 2010. arXiv:1002.3313v1.

[vH95] M. van Hoeij. An algorithm for computing the Weierstrass normal form. *ISSAC '95 Proceedings*, pages 90–95, 1995.

[Wei94] Charles Weibel. *Homological algebra.* Cambridge Univ. Press, 1994.