Uniwersytet im. Adama Mickiewicza w Poznaniu
Wydział Matematyki i Informatyki

Jędrzej Garnek
Nr albumu: 375564

O arytmetyce krzywych eliptycznych

On arithmetics of elliptic curves

Praca magisterska
na kierunku MATEMATYKA
specjalność: MATEMATYKA TEORETYCZNA

Praca wykonana pod kierunkiem
prof. dra hab. Wojciecha Gajdy

Czerwiec 2016

Tytuł

O arytmetyce krzywych eliptycznych

Streszczenie

W pracy przedstawiono zagadnienia związane z torsją krzywych eliptycznych nad ciałami lokalnymi. Definiujemy funkcję p-stopnia krzywej $E/\mathbb{Q}_p$ jako minimalny możliwy stopień rozszerzenia $\mathbb{Q}_p$ o niezerowy punkt p-torsyjny. Badamy własności tak określonej funkcji oraz obliczamy jej wartości dla pewnych krzywych. Użyte metody obejmują między innymi: teorię krzywych eliptycznych nad pierścieniami, teorię mnożenia zespolonego oraz uniformizację p-adyczną krzywych eliptycznych.

Słowa kluczowe

torsja krzywych eliptycznych, ciała lokalne, kanoniczne podniesienie, mnożenie zepolone, krzywa Tate'a

SPIS TREŚCI

WSTĘP

Krzywe eliptyczne stanowią jedną z najważniejszych klas krzywych algebraicznych. Mają związki z wieloma działami matematyki, między innymi z analizą zespoloną, topologią, geometrią algebraiczną i algebraiczną teorią liczb. Krzywe eliptyczne odegrały kluczową rolę w dowodzie Wielkiego Twierdzenia Fermata. Swoje zastosowanie znalazły także w życiu codziennym – algorytm wykorzystujący krzywe eliptyczne nad skończonymi ciałami jest dziś powszechnie stosowany w kryptografii.

Wyjątkowość krzywych eliptycznych wynika z tego, że stanowią one najprostszy przykład rzutowej grupy algebraicznej. Sposób na produkowanie punktów wymiernych na krzywej eliptycznej znaleźli już Bachet oraz Fermat w XVII wieku. Pierwszym matematykiem, który wykazał, że zbiór punktów na krzywej eliptycznej ma strukturę grupy, był jednak Poincaré. Struktura tej grupy była badana przez wielu kolejnych matematyków. Przełom nastąpił wraz z rozwojem nowoczesnej geometrii algebraicznej. Jak udowodnił Mordell w 1922 roku, grupa punktów wymiernych na krzywej eliptycznej $E/\mathbb{Q}$ jest skończenie generowana; jest więc postaci:

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{tors}$$

dla pewnej skończonej grupy $E(\mathbb{Q})_{tors}$. Ponadto, jak dowiódł Mazur w 1977 r. grupa $E(\mathbb{Q})_{tors}$ musi być jednej z niżej wymienionych postaci:

- $\mathbb{Z}/N$ dla $N = 1, \ldots, 10$ lub $N = 12$,
- $\mathbb{Z}/2 \oplus \mathbb{Z}/N$ dla $N = 2, 4, 6, 8$.

Elementy $E(\mathbb{Q})_{tors}$ można w efektywny sposób wyznaczyć, korzystając z twierdzenia Nagella-Lutza ([Sil09, Corollary VIII.7.2.]).

Okazuje się jednak, że część torsyjna grupy Mordella-Weila krzywych nad ciałami lokalnymi jest znacznie trudniejsza do zrozumienia i wiążą się z nią wciąż nieudowodnione hipotezy. Dla dowolnej krzywej eliptycznej $E/\mathbb{Q}_p$ określonej nad ciałem liczb p-adycznych zdefiniujmy jej **p-stopień** jako najmniejszy możliwy stopień rozszerzenia $\mathbb{Q}_p$ o punkt p torsyjny na E:

$$d_p(E) := \min\{[K : \mathbb{Q}_p] \quad | \quad E(K)[p] \neq 0\}$$

Rozważania związane z teorią deformacji reprezentacji Galois doprowadziły David oraz Westona do następującej hipotezy ([DW08]):

Hipoteza 1. *Jeżeli $E/\mathbb{Q}$ jest krzywą bez mnożenia zespolonego, to jej p-stopień dąży do nieskończoności przy p dążącym do nieskończoności.*

Autorzy pracy uzasadniają powyższe przypuszczenie obliczeniami numerycznymi oraz wynikiem analitycznym, pokazującym że krzywe posiadające p-torsję nad rozszerzeniem $K/\mathbb{Q}_p$ stopnia d powinny pojawiać się rzadko.
Pytań związanych z p-stopniem krzywej można postawić jednak znacznie więcej. Przykładowo, zastanowić się można, jakie wartości przyjmować może p-stopień na krzywych dobrej redukcji przy ustalonym p, tzn. jak wyglada zbiór:

$$D(p) := \{d_p(E) : E/\mathbb{Q}_p \text{ – krzywa eliptyczna dobrej redukcji w } p\}$$

Głównym celem tej pracy jest próba zbadania własności funkcji $d_p(E)$ oraz zbioru $D(p)$. Poniżej streszczamy wyniki przedstawione w dalszej części pracy.

Okazuje się, że umiemy wyznaczyć „małe liczby" w zbiorze $D(p)$. Krzywe dobrej redukcji o niskim p-stopniu ($d_p(E) < p-1$) można bowiem scharakteryzować na kilka równoważnych sposobów (patrz twierdzenie 3.1.5), w szczególności muszą one mieć p-torsję nad nierozgałęzionym rozszerzeniem $K/\mathbb{Q}_p$. Pozwoli nam to na udowodnienie następującego twierdzenia:

Twierdzenie A (wniosek 3.1.8)**.** *Jeżeli krzywa $E/\mathbb{Q}_p$ dobrej redukcji spełnia jeden z warunków:*

- $d_p(E) < p-1$,
- $E_{\mathbb{Z}/p^2}$ *(redukcja krzywej E do $\mathbb{Z}/p^2$) jest kanonicznym podniesieniem $E_{\mathbb{F}_p}$ (redukcji krzywej E do $\mathbb{F}_p$),*

to:

$$d_p(E) = \operatorname{ord}_p a_p(E)$$

gdzie $\operatorname{ord}_p(x)$ *jest rzędem x w grupie $\mathbb{F}_p^\times$, zaś $a_p(E)$ – śladem Frobeniusa krzywej E nad $\mathbb{F}_p$. W szczególności:*

$$D(p) \cap (0,p) = \{d \in \mathbb{N} : \exists_{|a|<2\sqrt{p}} \quad \operatorname{ord}_p a = d\}$$

Na podstawie Twierdzenia A udowodnimy również, że prawdopodobieństwo spełnienia przez losowo wybraną krzywą Hipotezy 1 jest równe 1:

Twierdzenie B (twierdzenie 3.1.10)**.**

$$\mathbb{P}\left(\lim_{p\to\infty} d_p(E_{A,B}) = \infty\right) = 1$$

Opisanie „dużych" liczb w zbiorze $D(p)$ nie wydaje się być tak proste. Obliczenia numeryczne doprowadziły autora niniejszej pracy do następującej hipotezy:

Hipoteza 2. *Dla $E : y^2 = x^3 + x$, $p \equiv 3 \pmod 4$ mamy: $d_p(E) = p^2 - 1$,*

którą uogólnimy i udowodnimy w podrozdziale 3.2. Okazuje się bowiem, że p-stopień krzywych eliptycznych z mnożeniem zespolonym można obliczyć dzięki opisowi działania grupy Galois na ich punktach poprzez Grossencharakter. Mamy przykładowo:

Twierdzenie C (twierdzenie 3.2.2)**.** *Niech $E : y^2 = x^3 - Dx$, gdzie $D \in \mathbb{Z}$, $D \neq 0$. Wtedy dla $p \nmid D$:*

$$d_p(E) = \begin{cases} \operatorname{ord}_p\left(D^{\frac{p-1}{4}} \cdot 2s\right), & \text{dla } p \equiv 1 \pmod 4, \\ p^2 - 1, & \text{dla } p \equiv 3 \pmod 4 \end{cases}$$

gdzie dla $p \equiv 1 \pmod 4$ liczba s zdefiniowana jest równością $p = s^2 + t^2$ oraz warunkami:

$$2 \nmid s, \quad s + t \equiv 1 \pmod 4.$$

W szczególności próba zweryfikowania Hipotezy 1 dla krzywych z mnożeniem przez $\mathbb{Z}[i]$ doprowadzi nas do poszukiwania liczb pierwszych w ciagu zadanym rekurencyjnie:

Twierdzenie D (wniosek 3.2.3(b)). *Niech $E : y^2 = x^3 - Dx$, gdzie $D \in \mathbb{Z}$, $D \neq 0$. Wówczas dla $p \nmid D$ mamy: $d_p(E) = 8$ wtedy i tylko wtedy, gdy p jest postaci $s_{k+1}^2 + s_k^2$, gdzie:*

$$s_0 = 0, \quad s_1 = 1, \quad s_{k+2} = 4s_{k+1} - s_k$$

Do innego pytania związanego z p-stopniem motywuje nas lemat Krasnera. Wynika z niego, że jeżeli p-adyczne wielomiany są „blisko", to ich ciała rozkładu są równe. Podobnie p-stopień krzywej eliptycznej powinien zależeć tylko od jej redukcji względem dostatecznie dużej potęgi p. Twierdzenie tego typu sprowadzałoby znalezienie zbioru $D(p)$ do obliczenia p-stopnia dla skończenie wielu krzywych, a także pozwalałoby np. na skonstruowanie krzywej eliptycznej o zadanych wartościach p-stopnia dla różnych p za pomocą Chińskiego Twierdzenia o Resztach. Wykażemy, że o p-stopniu krzywej decyduje jej redukcja do $\mathbb{Z}/p^{p^2+p+1}$:

Twierdzenie E (wniosek 3.1.4). *Jeżeli E_1, E_2 są krzywymi dobrej redukcji, których redukcje do $\mathbb{Z}/p^{p^2+p+1}$ są izomorficzne, to $d_p(E_1) = d_p(E_2)$.*

Dla krzywych niskiego stopnia wynik ten można znacznie poprawić, zastępując $p^2 + p + 1$ przez 2 (patrz wniosek 3.1.9).

Większość z uzyskanych przez nas wyników dotyczy krzywych dobrej redukcji. Krzywe redukcji multyplikatywnej są jednak o wiele prostsze do rozpatrzenia ze względu na istnienie tzw. krzywej Tate'a. Pozwala nam to na jawne obliczenie p-stopnia:

Twierdzenie F (twierdzenia 3.3.2 oraz 3.3.3). *Niech $E/\mathbb{Q}_p$ będzie krzywą o redukcji multyplikatywnej. Wtedy:*

$$d_p(E) = \begin{cases} p-1, & j(E) \notin \mathbb{Q}_p^p \\ 1, & j(E) \in \mathbb{Q}_p^p, \gamma(E/\mathbb{Q}_p) \in \mathbb{Q}_p^2 \\ 2, & j(E) \in \mathbb{Q}_p^p, \gamma(E/\mathbb{Q}_p) \notin \mathbb{Q}_p^2 \end{cases}$$

Twierdzenia A oraz B są luźno oparte na pracy [DW08], zaś D na pracy [CD14]. Dowód twierdzenia A różni się jednak od dowodu przedstawionego w pracy David oraz Westona. Rozważania związane z reprezentacją krzywej eliptycznej (patrz [DW08, Lemma 4.4.]) zastąpiłem obliczeniami dotyczącymi grupy formalnej (twierdzenie 3.1.1 oraz wniosek 3.1.6). Ponadto w celu obliczenia podniesień grupy p-podzielnej krzywej, klasyfikuję krzywe nad pierścieniami zupełnymi (twierdzenia 2.2.3 oraz 2.2.2). Twierdzenia C, E, F stanowią mój wkład własny. Wyniki związane z funkcją p-stopnia opisane są w Rozdziale 3, podczas gdy Rozdziały 1 oraz 2 stanowią przygotowanie. Opiszemy w nich między innymi teorię krzywych eliptycznych nad ciałami oraz pierścieniami, teorię mnożenia zespolonego, grup formalnych oraz uniformizację p-adyczną krzywych o multyplikatywnej redukcji. Praca zawiera również dodatek, podzielony na trzy części: pierwsza z nich opisuje wykorzystane twierdzenia z geometrii algebraicznej, druga część zajmuje się schematami grupowymi, zaś trzecia pokrótce opisuje najważniejsze twierdzenia teorii ciał klas. Na końcu pracy podany został spis używanych oznaczeń.

Pragnę serdecznie podziękować panu profesorowi doktorowi habilitowanemu Wojciechowi Gajdzie za cały trud włożony w opiekę nad moim rozwojem naukowym oraz za merytoryczną pomoc przy pisaniu pracy.

ROZDZIAŁ 1

PODSTAWY TEORII KRZYWYCH ELIPTYCZNYCH

W pierwszym rozdziale pracy omówimy standardową teorię krzywych eliptycznych, przedstawioną np. w [Sil09] oraz [Sil94]. Rozdział podzielony jest na trzy części. W pierwszej części zajmiemy się krzywymi eliptycznymi nad dowolnymi ciałami. Do sformułowanych w niej faktów wrócimy m.in. w rozdziale 2, zajmując się krzywymi eliptycznymi w ogólniejszym kontekście. W drugiej części zajmiemy się krzywymi eliptycznymi nad ciałami skończonej charakterystyki, zaś w trzeciej krzywymi z mnożeniem zespolonym.

1.1. Krzywe eliptyczne nad dowolnymi ciałami

Dla uproszczenia wzorów będziemy zakładali, że K jest doskonałym ciałem charakterystyki różnej od $2, 3$. Dowody przedstawionych stwierdzeń znaleźć można w [Sil09, rozdz. III] Zacznijmy od następujących definicji:

Definicja 1.1.1. Krzywą eliptyczną nad ciałem K nazywamy gładką krzywą rzutową genusu 1 wraz z wyróżnionym punktem K-wymiernym 0_E.

Definicja 1.1.2. Krzywą w postaci Weierstrassa o współczynnikach $A, B \in K$ nazywamy krzywą rzutową o części afinicznej zadanej wzorem:

$$E_{A,B}: \quad y^2 = x^3 + Ax + B. \tag{1.1}$$

Krzywa zadana równaniem (1.1) jest gładka wtedy i tylko wtedy, gdy wielomian $x^3 + Ax + B$ jest rozdzielczy, bądź też równoważnie, gdy wyróżnik krzywej zadany wzorem:

$$\Delta(E_{A,B}) = -16 \cdot (4A^3 + 27B^2) \tag{1.2}$$

jest niezerowy. Okazuje się, że każda gładka krzywa w postaci Weierstrassa wraz z wyróżnionym punktem $0_E := [0 : 1 : 0] \in \mathbb{P}^2(K)$ (tzw. punkt w nieskończoności) jest krzywą eliptyczną. Na odwrót, twierdzenie Riemanna–Rocha pozwala pokazać, że dowolna krzywa eliptyczna nad K jest izomorficzna z krzywą w postaci Weierstrassa wraz z wyróżnionym punktem $[0 : 1 : 0]$. Postać Weierstrassa krzywej eliptycznej jest wyznaczona jednoznacznie z dokładnością do podstawienia:

$$(x, y) \mapsto (u^4 \cdot x, u^6 \cdot y) \qquad \text{dla pewnego } u \in K^\times,$$

dającego równanie Weierstrassa $E_{A',B'}$, gdzie:

$$A' = u^4 \cdot A, \qquad B' = u^6 \cdot B.$$

W szczególności mamy:

$$\Delta(E_{A',B'}) = u^{12} \cdot \Delta(E_{A,B}),$$

więc wyróżnik krzywej staje się niezmiennikiem izomorfizmu dopiero, gdy traktujemy go jako element grupy $K^\times/(K^\times)^{12}$. Będziemy go oznaczali jako $\Delta(E/K)$.
Najważniejszym niezmiennikiem izomorfizmu jest jednak tzw. **j-niezmiennik** definiowany jako:

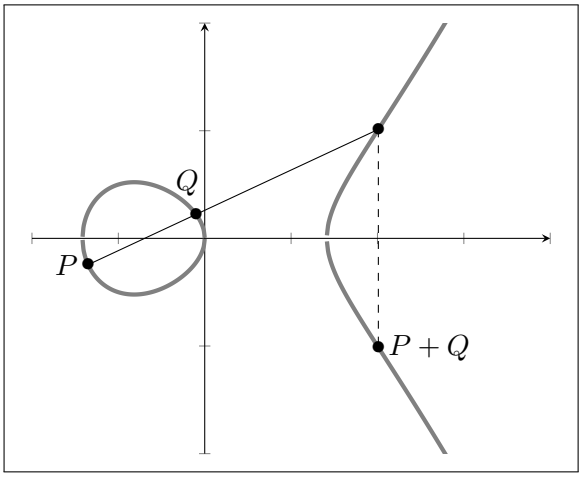
$$j(E_{A,B}) := -1728 \cdot \frac{(4A)^3}{\Delta(E_{A,B})}. \tag{1.3}$$

Z powyższych uwag widać, że j-niezmiennik krzywej nie zależy od klasy izomorfizmu oraz wyboru ciała bazowego K. Okazuje się, że jeżeli krzywe eliptyczne $E_1/K, E_2/K$ spełniają $j(E_1) = j(E_2) \neq 0, 1728$, to są izomorficzne nad ciałem $K\left(\sqrt{\frac{\gamma(E_1/K)}{\gamma(E_2/K)}}\right)$, gdzie:

$$\gamma(E_{A,B}/K) := -\frac{2A}{B} \in K^\times/(K^\times)^2 \tag{1.4}$$

(patrz [Sil94, Lemma V.5.2.]). W szczególności, krzywe eliptyczne o równym j-niezmienniku są $\overline{K}$-izomorficzne.

Własnością wyróżniającą krzywe eliptyczne spośród innych krzywych, jest możliwość dodawania ich punktów $\overline{K}$-wymiernych za pomocą funkcji K-wymiernych. Dodawanie to łatwo opisać geometrycznie:

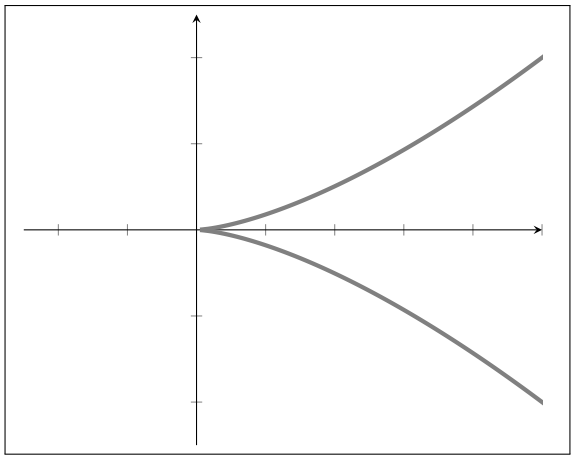


Rysunek 1.1: Prawo dodawania na krzywej eliptycznej nad $\mathbb{R}$

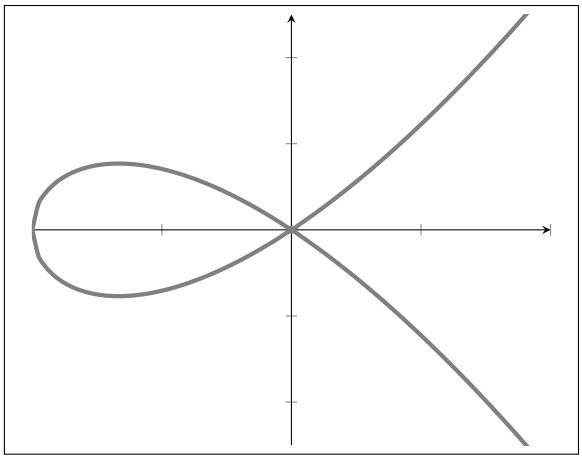
- elementem neutralnym jest punkt w nieskończoności 0_E,
- elementem przeciwnym do punktu $P = (x, y) \in E(\overline{K})$ jest punkt „symetryczny wg osi OX", tzn. $-P := (x, -y)$,
- punkty $P, Q, R \in E(\overline{K})$ sumują się do 0_E wtedy i tylko wtedy, gdy leżą na jednej prostej (jeżeli np. $P = Q$, to przyjmujemy, że prosta ta ma być styczna w punkcie P i podobnie dla $P = Q = R$).

Z powyższego opisu można w prosty sposób uzyskać konkretne wzory na sumę punktów, wyrażone przez funkcje wymierne ich współrzędnych. Okazuje się, że zdefiniowane w ten sposób działanie jest łączne, przemienne i niezmiennicze ze względu na działanie grupy Galois $\mathrm{Gal}(\overline{K}/K)$. W przypadku, gdy krzywa zadana równaniem Weierstrassa jest osobliwa, można w analogiczny zdefiniować strukturę grupy na zbiorze punktów nieosobliwych $E_{ns}(\overline{K})$. Wyróżniamy następujące dwa przypadki (patrz [Sil09, zad. 3.5.]):

- jeżeli $A = B = 0$, to krzywa ma w punkcie $(0, 0)$ osobliwość typu **ostrze**. Zachodzi wówczas: $E_{ns}(\overline{K}) \cong \overline{K}^+$ (jako $\mathrm{Gal}(\overline{K}/K)$-moduły).
- jeżeli $A, B \neq 0$, to krzywa ma osobliwość typu **węzeł**. Jeżeli ponadto proste styczne do E w punkcie osobliwym mają współczynniki w K, to $E_{ns}(\overline{K}) \cong \overline{K}^\times$.



(a) Krzywa Weierstrassa z ostrzem



(b) Krzywa Weierstrassa z węzłem

K**-izogenią** pomiędzy krzywymi eliptycznymi E_1/K oraz E_2/K nazywamy niestały morfizm $\phi : E_1 \to E_2$ zdefiniowany nad K oraz spełniający: $\phi(0_{E_1}) = 0_{E_2}$. Dowolna izogenia indukuje epimorfizm grup abelowych $E_1(\overline{K}) \to E_2(\overline{K})$. **Stopniem** (odpowiednio stopniem rozdzielczym/czysto nierozdzielczym) izogenii nazwiemy stopień rozszerzenia ciał funkcyjnych $K(E_2)/\phi^*(K(E_1))$ (odpowiednio stopień rozdzielczy/czysto nierozdzielczy); jest on oznaczany jako $\deg \phi$ (odpowiednio $\deg_s \phi$, $\deg_i \phi$). Stopień rozdzielczy jest istotny ze względu na następującą równość:

$$\#\ker\Big(\phi : E_1(\overline{K}) \to E_2(\overline{K})\Big) = \deg_s \phi,$$

która zachodzi dla dowolnej izogenii $\phi : E_1 \to E_2$. **Morfizmem mnożenia przez** n nazwie-

my izogenię $[n] : E \to E$ zadaną wzorem:

$$[n]P := \begin{cases} \underbrace{P + P + \ldots + P}_{n \text{ razy}}, & \text{dla } n \geqslant 0 \\ \underbrace{-P - P - \ldots - P}_{(-n) \text{ razy}}, & \text{dla } n < 0 \end{cases}.$$

Jej jądro oznaczamy przez $E[n]$. Okazuje się, że $\deg[n] = n^2$, zaś jeżeli $\operatorname{char} K = 0$ lub $\operatorname{char} K = p \nmid n$ to $\deg_s[n] = n^2$ oraz:

$$E[n](\overline{K}) \cong \mathbb{Z}/n \times \mathbb{Z}/n$$

jako grupy abelowe.
Z powyższych uwag widać w szczególności, że $\mathbb{Z}$ zanurza się w grupę $End(E)$ endomorfizmów krzywej eliptycznej jako grupy algebraicznej, określonych nad $\overline{K}$. Grupa $End(E)$ może być izomorficzna z $\mathbb{Z}$, z ordynkiem w algebrze kwaternionowej (jeżeli $\operatorname{char} K = p$, zaś krzywa jest supersingularna – patrz następny rozdział) lub z ordynkiem w urojonym ciele kwadratowym. Krzywe eliptyczne, dla których zachodzi ostatni przypadek nazywamy **krzywymi z mnożeniem zespolonym**. Stanowią one główny temat podrozdziału 1.3.

1.2. Krzywe eliptyczne nad ciałami charakterystyki p

W tym podrozdziale zajmiemy się krzywymi eliptycznymi nad doskonałym ciałem k charakterystyki p, gdzie p jest liczbą pierwszą. Nasze rozważania zaczniemy od zbadania struktury $E[p^i]$. Przypomnijmy, że $\deg[p^i] = p^{2i}$ – dlatego też $E[p^i]$ jest płaskim, skończonym schematem grupowym nad k rzędu p^{2i} (patrz Dodatek B). Okazuje się jednak, że $E[p^i](\overline{k}) \neq (\mathbb{Z}/p^i)^2$. Możliwe są dwa przypadki ([Sil09, III.6.4]):

- dla każdego i: $\deg_s[p^i] = p^i$ oraz $E[p^i](\overline{k}) \cong \mathbb{Z}/p^i$ (krzywa E jest **zwyczajna**),
- dla każdego i: $\deg_s[p^i] = 1$ oraz $E[p^i](\overline{k}) = 0$ (krzywa E jest **supersingularna**).

Opiszemy ciąg spójno-étalny schematu grupowego $E[p^i]$ (patrz twierdzenie B.9) w pierwszym przypadku:

Twierdzenie 1.2.1. *Niech k będzie doskonałym ciałem charakterystyki p, zaś E/k – zwyczajną krzywą eliptyczną. Wtedy:*

$$\begin{aligned} E[p^i] &\cong E[p^i]^o \times_k E[p^i]^{et} \\ &\cong \mu_p(\chi^{-1}) \times_k \mathbb{Z}/p(\chi) \end{aligned}$$

gdzie:

- $\chi : \operatorname{Gal}(\overline{k}/k) \to Aut(\mathbb{Z}/p^i) \cong (\mathbb{Z}/p^i)^\times$ *jest ciągłym homomorfizmem,*
- $\mathbb{Z}/p(\chi)$ *jest schematem étalnym (zdefiniowanym w przykładzie B.7),*
- $\mu_{p^i}(\chi^{-1}) := (\mathbb{Z}/p^i(\chi))^\vee$ *jest dualne w sensie Cartier do odpowiedniego schematu étalnego.*

Charakter χ jest trywialny wtedy i tylko wtedy, gdy E ma k-wymierny punkt rzędu p^i.

Dowód. Przypomnijmy, że nad ciałem doskonałym ciąg spójno-étalny z twierdzenia B.9 rozszczepia się. Ze zwyczajności krzywej E oraz stwierdzenia B.10 mamy:

$$\mathbb{Z}/p^i = E[p^i](\overline{k}) = E[p^i]^0(\overline{k}) \times E[p^i]^{et}(\overline{k}) = E[p^i]^{et}(\overline{k}).$$

Z lematu A.2 stwierdzamy więc, że $E[p^i]^{et} = \mathbb{Z}/p^i(\chi)$ dla pewnego charakteru

$$\chi : \mathrm{Gal}(\overline{k}/k) \to Aut(\mathbb{Z}/p^i).$$

Zauważmy jednak, że $E[p^i]$ jest samodualne w sensie Cartier (patrz twierdzenie 2.1.5). Korzystając z samodualności $E[p^i]$ stwierdzamy, że $\mu_{p^i}(\chi^{-1}) := (\mathbb{Z}/p^i(\chi))^\vee$ musi być również podgrupą $E[p^i]$. Zauważmy, że $\mu_{p^i}(\chi^{-1})$ jest spójne, jako że:

$$\mu_{p^i}(\chi^{-1})(\overline{k}) = \mu_{p^i}(\chi^{-1})_{\overline{k}}(\overline{k}) = \mu_{p^i}(\overline{k}) = \{1\}.$$

Stąd: $\mu_{p^i}(\chi^{-1}) \subset E[p^i]^0$, zaś porównując rangi dostajemy równość.

W celu wykazania drugiej części twierdzenia zauważmy, że:

$$E[p^i](k) = \mathbb{Z}/p^i(\chi)(k) = \{j \in \mathbb{Z}/p^i : \forall_{\sigma \in G_k} \quad \chi(\sigma) \cdot j = j\}$$

– widać więc, że $E[p^i](k)$ zawiera punkt rzędu p^i wtedy i tylko wtedy, gdy χ jest trywialny. □

Przejdziemy teraz do zliczania punktów wymiernych nad ciałem $k := \mathbb{F}_q$, gdzie $q = p^n$ jest potęgą liczby pierwszej. Głównym narzędziem będzie tzw. **q-ty morfizm Frobeniusa**, zdefiniowany jako:

$$F_q : E \to E, \qquad F_q(x, y) = (x^q, y^q).$$

Jest on czysto nierozdzielczą izogenią stopnia q. Jak łatwo zauważyć, punkt $P \in E(\overline{\mathbb{F}}_q)$ jest $\mathbb{F}_q$-wymierny wtedy i tylko wtedy, gdy $F_q(P) = P$. Izogenia $id - F_q$ okazuje się być rozdzielcza, mamy więc:

$$\#E(\mathbb{F}_q) = \deg(id - F_q).$$

Nierówność Cauchy'ego-Schwarza zastosowana do formy dwuliniowej:

$$\langle \phi_1, \phi_2 \rangle := \deg(\phi_1 + \phi_2) - \deg \phi_1 - \deg \phi_2$$

pozwala na udowodnienie tzw. nierówności Hassego, która jest odpowiednikiem hipotezy Riemanna dla E:

$$|q + 1 - \#E(\mathbb{F}_q)| \leqslant 2\sqrt{q}.$$

Rozważając działanie $End(E)$ na ℓ-adyczym module Tate'a $T_\ell(E) := \varprojlim E(\overline{k})[\ell^n] \cong (\mathbb{Z}_\ell)^2$ (gdzie $\ell \neq p$ jest liczbą pierwszą) możemy utożsamiać dowolny endomorfizm z macierzą o współczynnikach w $\mathbb{Z}_\ell$. Okazuje się, że wyznacznik takiej macierzy jest równy stopniowi odpowiadającego endomorfizmu. Ślad tej macierzy jest zaś liczbą całkowitą, niezależącą od wyboru ℓ. Ślad morfizmu Frobeniusa F_q będziemy oznaczali przez $a_q(E)$. Podstawiając $x = 1$ w wielomianie charakterystycznym morfizmu Frobeniusa dostajemy:

$$\begin{aligned} \#E(\mathbb{F}_q) &= \deg(I - F_q) = \det(I - F_q) = \\ &= 1^2 - a_q(E) \cdot 1 + q = \\ &= q + 1 - a_q(E). \end{aligned}$$

Ponadto, jeżeli $\alpha_1, \alpha_2 \in \mathbb{C}$ są pierwiastkami wielomianu charakterystycznego odwzorowania Frobeniusa, to:

$$a_{q^d}(E) = \alpha_1^d + \alpha_2^d$$

(wartości własne macierzy podniesionej do d-tej potęgi są d-tymi potęgami odpowiednich wartości własnych), więc:

$$\begin{aligned} \#E(\mathbb{F}_{q^d}) &= \det(I - F_{q^d}) = 1^2 - a_{q^d}(E) \cdot 1 + q^d \\ &= q^d + 1 - (\alpha_1^d + \alpha_2^d). \end{aligned}$$

To spostrzeżenie pozwala na udowodnienie następującego stwierdzenia dotyczącego p-torsji:

Stwierdzenie 1.2.2. *Jeżeli $E/\mathbb{F}_p$ jest krzywą eliptyczną, to:*

$$E(\mathbb{F}_{p^d})[p] \neq 0 \quad \textit{wtedy i tylko wtedy, gdy} \quad a_p(E)^d \equiv 1 \pmod{p}.$$

Dowód. Z powyższych uwag mamy:

$$\#E(\mathbb{F}_{p^d}) = p^d + 1 - (\alpha_1^d + \alpha_2^d)$$

gdzie $\alpha_1, \alpha_2 \in \mathbb{C}$ są pierwiastkami wielomianu charakterystycznego $x^2 - a_p(E)x + p$. Mnożąc równość $\alpha_i^2 = a_p(E) \cdot \alpha_i + p$ przez α_i^{d-2} dostajemy dla $d \geqslant 2$:

$$\begin{aligned} a_{p^d}(E) &= \alpha_1^d + \alpha_2^d = a_p(E) \cdot (\alpha_1^{d-1} + \alpha_2^{d-1}) + p \cdot (\alpha_1^{d-2} + \alpha_2^{d-2}) \\ &= a_p(E) \cdot a_{p^{d-1}}(E) + p \cdot a_{p^{d-2}}(E) \\ &\equiv a_p(E) \cdot a_{p^{d-1}}(E) \pmod{p}, \end{aligned}$$

więc iterując rozumowanie dostajemy: $a_{p^d}(E) \equiv a_p(E)^d \pmod{p}$. Stąd:

$$\begin{aligned} E(\mathbb{F}_{p^d})[p] \neq 0 \quad &\Leftrightarrow \quad p | \#E(\mathbb{F}_{p^d}) = p^d + 1 - a_{p^d}(E) \\ &\Leftrightarrow \quad p | a_p(E)^d - 1. \end{aligned}$$

□

Z powyższego twierdzenia wynika w szczególności, że krzywa $E/\mathbb{F}_p$ jest supersingularna wtedy i tylko wtedy, gdy $p | a_p(E)$. Z nierówności Hassego dla $p \geqslant 5$ jest to równoważne z warunkiem $a_p(E) = 0$. Innego kryterium na supersingularność dostarcza następujące twierdzenie sformułowane i udowodnione w pracy [Deu41]:

Twierdzenie 1.2.3 (kryterium Deuringa)**.** *Krzywa $E/\mathbb{F}_q$ jest supersingularna wtedy i tylko wtedy, gdy istnieje kwadratowy ordynek R, w którym p rozgałęzia się lub pozostaje pierwsza oraz który można zanurzyć w $End(E)$ tak, aby:*

$$R = End(E) \cap (R \otimes \mathbb{Q})$$

Na koniec tego podrozdziału zajmiemy się zliczaniem krzywych $E/\mathbb{F}_p$ o zadanym śladzie. Potrzebujemy w tym celu następującej definicji:

Definicja 1.2.4. Niech R będzie ordynkiem w urojonym ciele kwadratowym K.
Przez **grupę klas** ordynka będziemy rozumieli $I(R)/P(R)$, gdzie $I(R)$ jest grupą odwracalnych ideałów ułamkowych R, zaś $P(R)$ oznacza grupę głównych odwracalnych ideałów

ułamkowych. Rząd grupy klas nazywamy **liczbą klas** ordynka i oznaczamy przez $h(R)$. **Liczbą klas Hurwitza** ordynka R nazywamy:

$$H(R) = \sum_{R \subset R' \subset R_K} \frac{1}{|R'^{\times}|} h(R'),$$

gdzie R_K jest pierścieniem liczb całkowitych w ciele K. Jeżeli R jest ordynkiem o wyróżniku D w urojonym ciele kwadratowym, to jego liczbę klas Kroneckera oznaczamy zwyczajowo przez $H(D)$.

Stwierdzenie 1.2.5. *Dla* $|a| \leqslant 2\sqrt{p}$*:* $|H(a^2 - 4p)| \leqslant \sqrt{p}\log^2(p)$

Dowód. Oszacowanie to wynika z zastosowania analitycznej formuły Dirichleta ([Dav00, §6]) oraz trywialnego oszacowania $L(1, \chi_D) \ll \log D$, uzyskanego przez sumowanie częściowe. □

Twierdzenie 1.2.6 (wzór Deuringa, [Cox89, Theorem 14.18])**.** *Niech* $p > 3$ *będzie liczbą pierwszą, zaś* r *– liczbą naturalną spełniającą* $|r| \leqslant 2\sqrt{p}$*. Wtedy:*

$$\#\{(a, b) \in \mathbb{F}_p \times \mathbb{F}_p : \Delta(E_{a,b}) \neq 0, \quad a_p(E_{a,b}) = r\} = \frac{p-1}{2} H(r^2 - 4p)$$

1.3. Krzywe eliptyczne z mnożeniem zespolonym

Każda krzywa eliptyczna nad $\mathbb{C}$ jest powierzchnią Riemanna genusu 1, czyli zespolonym torusem. Jako zespolona rozmaitość Lie jest zatem izomorficzna z ilorazem płaszczyzny zespolonej przez odpowiednio dobraną kratę Λ. Wzory jawne na izomorfizm $f : \mathbb{C}/\Lambda \to E(\mathbb{C})$ zostały podane już przez Weierstassa i wyrażają się przez tzw. funkcje eliptyczne Weierstassa (patrz [Sil09, rozdz. VI]). Z punktu widzenia teorii liczb opis ten jest jednak zazwyczaj bezużyteczny, jako że nie uwzględnia własności arytmetycznych krzywej, czyli działania grupy Galois na punktach wymiernych krzywej.

W przypadku krzywej eliptycznej z mnożeniem zespolonym przez pierścień R okazuje się, że związana z nią krata Λ jest ideałem ułamkowym w ciele $K := R \otimes \mathbb{Q}$, wyznaczonym jednoznacznie z dokładnością do klasy w grupie klas. Działanie grupy Galois na punktach torusa $\mathbb{C}/\Lambda$ można wtedy opisać jawnie za pomocą Grossencharakteru stowarzyszonego z krzywą, symbolu Artina oraz grupy ideli (patrz Dodatek C). Aby uprościć sformułowanie głównego twierdzenia o mnożeniu zespolonym, będziemy rozpatrywali tylko krzywe z mnożeniem zespolonym przez maksymalny ordynek. Będziemy stosowali następujące oznaczenia:

- K będzie urojonym ciałem kwadratowym z pierścieniem liczb całkowitych R_K,
- E będzie krzywą eliptyczną nad ciałem $L := K(j(E))$ o pierścieniu endomorfizmów izomorficznym z R_K. Przez R_L oznaczymy pierścień liczb całkowitych w L,
- $[\cdot] : R_K \to End(E)$ będzie izomorfizmem spełniającym:

  $$[\alpha]^*\omega = \alpha\omega \text{ dla każdego } \alpha \in R_K$$

  dla niezmienniczej formy różniczkowej $\omega = dx/y$ na E. Istnienie i jedyność tego izomorfizmu wynika z [Sil94, Proposition II.1.1],
- dla ideału $\mathfrak{b} \trianglelefteq R_K$ oznaczamy:

  $$E[\mathfrak{b}] := \{P \in E(\overline{K}) : [b]P = 0 \text{ dla każdego } b \in \mathfrak{b}\}$$

Przypomnijmy pokrótce najważniejsze fakty dotyczące krzywych z mnożeniem zespolonym, do których nie będziemy się bezpośrednio odwoływać:

(1) $E[\mathfrak{b}]$ jest wolnym $R_K/\mathfrak{b}$-modułem rangi 1 ([Sil94, Proposition II.1.4. (b)]),

(2) wszystkie endomorfizmy krzywej E są określone nad ciałem L ([Sil94, Thm II.2.2 (b)]),

(3) $L(E(\overline{K})_{tors})/L$ jest rozszerzeniem abelowym ([Sil94, Thm II.2.3]),

(4) $K(j(E))$ jest ciałem Hilberta dla K (patrz [Sil94, Thm II.4.1.]), w szczególności $K(j(E)) = K$ wtedy i tylko wtedy, gdy R_K ma własność jednoznaczności rozkładu,

(5) istnieje 13 klas izomorfizmu krzywych z mnożeniem zespolonym o współczynnikach wymiernych (patrz [Sil94, A.§3]). Krzywe te odpowiadają pierścieniom postaci $\mathbb{Z}[f\omega_D]$, gdzie:

$$\omega_D = \begin{cases} \sqrt{-D}, & D \not\equiv 1 \pmod 4 \\ \frac{-1+\sqrt{D}}{2} & D \equiv 1 \pmod 4 \end{cases} \qquad \text{oraz}$$

$$(-D, f) = (3,1), (3,2), (3,3), (1,1), (1,2), (7,1), (7,2),$$
$$(2,1), (11,1), (19,1), (43,1), (67,1), (163,1).$$

Z poprzedniej uwagi wynika, że wszystkie podane pierścienie mają własność jednoznaczności rozkładu. (patrz [Sil94, Theorem II.4.1.]).

Aby sformułować główne twierdzenie o mnożeniu zespolonym, potrzebujemy zdefiniować mnożenie elementów ciała przez idele. Podstawowe definicje i oznaczenia związane z idelami znaleźć można w Dodatku C. Zauważmy najpierw, że dla dowolnego torsyjnego R_K-modułu M istnieje izomorfizm:

$$S : \bigoplus_{\mathfrak{p}} M[\mathfrak{p}^\infty] \to M, \qquad (x_\mathfrak{p})_\mathfrak{p} \mapsto \sum_{\mathfrak{p}} x_\mathfrak{p},$$

gdzie suma brana jest po wszystkich ideałach pierwszych $\mathfrak{p}$ pierścienia R_K, zaś

$$M[\mathfrak{p}^\infty] := \{m \in M : \mathfrak{p}^e m = 0 \text{ dla pewnego } e \geqslant 0\}.$$

Jest to tzw. twierdzenie o rozkładzie $\mathfrak{p}$-prymarnym – patrz np. [Sil94, Lemma II.8.1.(a)]. Rozważmy moduł $M := R_K/\mathfrak{a}$, gdzie $\mathfrak{a}$ jest ideałem ułamkowym ciała K. Jak łatwo zauważyć (patrz [Sil94, Lemma II.8.1.(b)]), naturalne zanurzenie $K \hookrightarrow K_\mathfrak{p}$ indukuje izomorfizm $K/\mathfrak{a}[\mathfrak{p}^\infty] \cong K_\mathfrak{p}/\mathfrak{a}_\mathfrak{p}$ – rozkład $\mathfrak{p}$-prymarny modułu $K/\mathfrak{a}$ przyjmuje więc postać:

$$K/\mathfrak{a} \cong \bigoplus_{\mathfrak{p}} K_\mathfrak{p}/\mathfrak{a}_\mathfrak{p}$$

Spostrzeżenie to pozwala nam na zdefiowanie **mnożenia przez idel** $x \in \mathbb{I}_K$ elementów kraty $K/\mathfrak{a}$, jako odwzorowania $K/\mathfrak{a} \to K/x\mathfrak{a}$ (przez $x\mathfrak{a}$ rozumiemy iloczyn ideałów $(x)\mathfrak{a}$), które po obcięciu do składowej $\mathfrak{p}$-prymarnej jest mnożeniem przez $x_\mathfrak{p}$. Innymi słowy, jest ono zdefiniowane przez następujący diagram:

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\cdot x} & K/x\mathfrak{a} \\ \wr\downarrow & & \wr\downarrow \\ \bigoplus_\mathfrak{p} K_\mathfrak{p}/\mathfrak{a}_\mathfrak{p} & \longrightarrow & \bigoplus_\mathfrak{p} K_\mathfrak{p}/x_\mathfrak{p}\mathfrak{a}_\mathfrak{p} \\ (t_\mathfrak{p})_\mathfrak{p} & \longmapsto & (x_\mathfrak{p} t_\mathfrak{p})_\mathfrak{p}. \end{array}$$

Twierdzenie 1.3.1 (główne twierdzenie o mnożeniu zespolonym, [Sil94, Theorem II.9.1])**.** *Niech E/L będzie krzywą eliptyczną z mnożeniem zespolonym przez R_K i załóżmy, że $K \subset L$. Niech $x \in \mathbb{I}_L$ będzie idelem, zaś $s = N_{L/K}x \in \mathbb{I}_K$ oznacza jego normę. Wtedy istnieje dokładnie jeden element $\alpha = \alpha_{E/L}(x) \in K^\times$ o następujących własnościach:*

- $\alpha R_K = (s)$,
- *dla dowolnego ideału ułamkowego $\mathfrak{a} \subset K$ oraz dowolnego analitycznego izomorfizmu $f : \mathbb{C}/\mathfrak{a} \to E(\mathbb{C})$ następujący diagram jest przemienny:*

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\cdot\alpha s^{-1}} & K/\mathfrak{a} \\ \downarrow f & & \downarrow f \\ E(L^{ab}) & \xrightarrow{[x,L]} & E(L^{ab}) \end{array}.$$

Funkcję $\Psi_{E/L} : \mathbb{I}_L \to \mathbb{C}^\times$ zdefiniowaną wzorem:

$$\Psi_{E/L}(x) := \alpha_{E/L}(x) \cdot N_{L/K}(x^{-1})_\infty$$

nazywamy **Grossencharakterem** związanym z krzywą E/K. Jest to ciągły homomorfizm spełniający warunek $\Psi(\iota(L^\times)) = 1$, gdzie $\iota : L^* \hookrightarrow \mathbb{I}_L$ jest naturalnym zanurzeniem. Pełni on ważną rolę między innymi przy przedłużaniu L-funkcji związanej z krzywą z mnożeniem zespolonym (patrz [Deu41]). Zauważmy najpierw, że jest on nierozgałęziony w miejscach dobrej redukcji krzywej:

Stwierdzenie 1.3.2 ([Sil94, Theorem II.9.2])**.** *Niech β będzie ideałem pierwszym w R_L takim, że E ma dobrą redukcję na β. Załóżmy, że $x \in \iota_\beta(R_\beta^\times)$ – wtedy:*

$$\Psi_{E/L}(x) = \alpha_{E/L}(x) = 1.$$

Dowód. Załóżmy, że β leży nad ideałem pierwszym $\mathfrak{p}$ ciała K. Zauważmy, że:

$$s = N_{L/K}(x) \in i_\mathfrak{p}((R_K)_\mathfrak{p}),$$

tak więc mnożenie elementu kraty przez idel s^{-1} zmienia tylko współrzędną $\mathfrak{p}$-prymarną; mamy więc:

$$f\left(\frac{1}{m}\right)^{[x,L]} = f\left(\alpha \cdot s^{-1} \cdot \frac{1}{m}\right) = f\left(\alpha \cdot \frac{1}{m}\right).$$

Z drugiej strony odwzorowanie Artina odwzorowuje $R_\beta^\times$ na grupę inercji I_β^{ab}, działającą trywialnie na $E[m]$ dla dowolnego $\beta \nmid m$ (kryterium Nérona-Ogga-Shafarevicha – patrz [Sil09, Theorem VII.7.1.]). Dostajemy zatem:

$$f\left(\frac{1}{m}\right)^{[x,L]} = f\left(\frac{1}{m}\right)$$

i porównując obie równości dostajemy $\alpha(x) = 1$. □

W szczególnych przypadkach można w prosty sposób wyznaczyć wartości $\alpha(x)$ na całej grupie $\iota_\beta(K_\beta^\times)$. Do sformułowania wzorów będziemy potrzebowali tak zwanego **symbolu reszt potęgowych**, zdefiniowanego np. w [IR90, Chapter 14 §2]. Niech $m \geqslant 2$ będzie liczbą naturalną, zaś $P \nmid m$ – ideałem pierwszym o normie NP w pierścieniu liczb cyklotomicznych $\mathbb{Z}[\zeta_m]$. Dla dowolnego $\alpha \in \mathbb{Z}[\zeta_m]$ definiujemy symbol $(\frac{\alpha}{P})_m$ jak następuje:

- dla $\alpha \in P$: $(\frac{\alpha}{P})_m = 0$,
- dla $\alpha \notin P$, $(\frac{\alpha}{P})_m$ określamy jako jedyny pierwiastek z jedności stopnia m spełniający kongruencję:
$$\alpha^{(NP-1)/m} \equiv \left(\frac{\alpha}{P}\right)_m \pmod{P}.$$

Dla uproszenia notacji będziemy oznaczali $(\frac{\alpha}{\pi})_m := (\frac{\alpha}{P})_m$ w przypadku, gdy $P = (\pi)$ jest ideałem głównym. Notacji tej będziemy stosowali w przypadkach m=4 oraz m=6. Wówczas $\mathbb{Z}[\zeta_m]$ jest odpowiednio pierścieniem Gaussa $\mathbb{Z}[i]$ lub pierścieniem liczb całkowitych Eisensteina $\mathbb{Z}[\omega]$ (gdzie $\omega = \frac{-1+\sqrt{-3}}{2}$). Będziemy nazywali element $\pi \in \mathbb{Z}[\zeta_m]$ **prymarnym**, jeżeli:

- dla $m = 4$: $\pi \equiv 1 \pmod{2+2i}$. Zapisując $\pi = s + ti$ łatwo stwierdzić, że jest to równoważne z warunkami:
$$\begin{cases} s & \equiv & 1 \pmod 4 \\ t & \equiv & 0 \pmod 4 \end{cases} \quad \text{lub} \quad \begin{cases} s & \equiv & 3 \pmod 4 \\ t & \equiv & 2 \pmod 4 \end{cases} \tag{1.5}$$
- dla $m = 6$: $\pi \equiv 2 \pmod 3$. Zapisując $\pi = s+t\omega$ łatwo stwierdzić, że jest to równoważne z warunkami:
$$\begin{cases} s & \equiv & 2 \pmod 3 \\ t & \equiv & 0 \pmod 3 \end{cases}. \tag{1.6}$$

Łatwo zauważyć, że dowolny ideał pierwszy $\mathfrak{p} \trianglelefteq \mathbb{Z}[\zeta_m]$ stopnia 1 można jednoznacznie zapisać w postaci $\mathfrak{p} = (\pi)$, gdzie π jest elementem prymarnym.

Stwierdzenie 1.3.3.

(a) Niech $E : y^2 = x^3 - Dx$ dla $D \in \mathbb{Z}$, $D \neq 0$. Wówczas dla dowolnego ideału pierwszego $\mathfrak{p} = (\pi)$ (gdzie π jest elementem prymarnym) w R_K, spełniającego $\mathfrak{p} \nmid 6D$ mamy:
$$\alpha(\iota_{\mathfrak{p}}(\pi)) = \overline{\left(\frac{D}{\pi}\right)_4}\pi.$$

(b) Niech $E : y^2 = x^3 + D$ dla $D \in \mathbb{Z}$, $D \neq 0$. Wówczas dla dowolnego ideału pierwszego $\mathfrak{p} = (\pi)$ (gdzie π jest elementem prymarnym) w R_K, spełniającego $\mathfrak{p} \nmid 2D$ mamy:
$$\alpha(\iota_{\mathfrak{p}}(\pi)) = -\overline{\left(\frac{4D}{\pi}\right)_6}\pi.$$

Dowód. Dowód można znaleźć w [Sil94, zadanie 2.34 oraz przykład II.10.6]. □

ROZDZIAŁ 2

KRZYWE ELIPTYCZNE NAD PIERŚCIENIAMI

W tej części pracy zajmiemy się ugólnianiem teorii krzywych eliptycznych, przedstawionej w pierwszym rozdziale. Skupimy się przede wszystkim na krzywych nad pierścieniami zupełnymi. W pierwszym podrozdziale pokrótce przedstawimy teorię krzywych eliptycznych nad dowolnym schematem bazowym na podstawie artykułu [KM85]. W dalszych podrozdziałach zajmiemy się klasyfikacją krzywych eliptycznych nad pierścieniami zupełnymi i badaniem odwzorowania redukcji. Przedstawione wyniki stanowią uogólnienie twierdzeń przedstawionych w [DW08] i zostaną wykorzystane w kolejnym rozdziale, na przykład w dowodzie twierdzenia 3.1.5.

2.1. Krzywe eliptyczne nad dowolnymi schematami

Celem tego podrozdziału jest uogólnienie definicji krzywej eliptycznej w taki sposób, aby rozważyć dowolny schemat bazowy S. Dla uproszczenia notacji będziemy zazwyczaj przyjmowali, że $6 \in \mathcal{O}_S(S)^\times$.

Definicja 2.1.1. S-schemat E o właściwym i gładkim morfiźmie strukturalnym $\pi : E \to S$ oraz cięciem $0_E \in E(S)$ nazywamy **krzywą eliptyczną nad** S, jeżeli dla dowolnego $y \in S$ włókno $E_y := \pi^{-1}(y)$ jest geometrycznie spójną krzywą genusu 1 nad ciałem residualnym $\kappa(y)$.

Zauważmy przy tym, że w przypadku, gdy $S = \mathrm{Spec}(K)$ pochodzi od ciała, otrzymujemy krzywą eliptyczną w sensie rozważanym w poprzednim rozdziale. Okazuje się, że w ogólniejszym przypadku krzywa zadana równaniem Weierstrassa jest również krzywą eliptyczną, o ile tylko jest nieosobliwa:

Przykład 2.1.2. *Niech R będzie dowolnym pierścieniem przemiennym, spełniającym warunek $6 \in R^\times$. **Krzywą w postaci Weierstrassa** $E_{A,B}$ nad* $\mathrm{Spec}(R)$ *nazywamy schemat postaci:*

$$\mathrm{Proj}(R[x,y,z]/(f(x,y,z))) \tag{2.1}$$

gdzie $f(x,y,z) = y^2z - x^3 - Axz^2 - Bz^3$ oraz $A, B \in R$.

Okazuje się, że schemat $E_{A,B}$ jest gładki nad R wtedy i tylko wtedy, gdy wyróżnik $\Delta(E_{A,B})$ (zadany wzorem (1.2)) jest odwracalny w R, oraz że jest wówczas krzywą eliptyczną nad $\mathrm{Spec}(R)$. Przykład ten jest kluczowy ze względu na następujące twierdzenie:

Twierdzenie 2.1.3. *Załóżmy, że $6 \in \mathcal{O}_S(S)^\times$. Niech E będzie krzywą eliptyczną nad S. Wtedy istnieje otwarte pokrycie afiniczne schematu S takie, że E jest lokalnie izomorficzne z krzywymi w postaci Weierstrassa.*

Szkic dowodu na podstawie [Hid13, podrozdz. 6.2.1] oraz [KM85, rozdz. 2.2]:

Z obliczeń kohomologicznych wynika, że $\mathcal{L} := \pi_*(\Omega_{E/S})$ jest odwracalnym snopem (patrz [KM85, str. 67]). Zastępując S przez dostatecznie mały zbiór otwarty afiniczny $\mathrm{Spec}(R)$, możemy założyć, że $\mathcal{L}$ jest snopem wolnym. Wykażemy, że dla dowolnego wyboru bazy ω snopa $\mathcal{L}$ istnieje jedyne równanie Weierstrassa.
Wybieramy formalny lokalny parametr T w 0_E taki, że:

$$\omega = (1 + \ldots)\, dT.$$

Z [Hid13, Lemma 6.13] wynika, że $\operatorname{rank} \mathcal{L}(m[0_E]) = m$ dla $m > 0$. Korzystając z twierdzenia A.5, stwierdzamy więc, że istnieją morfizmy $x, y : E \to \mathbb{P}^1_S$ (jednoznacznie wyznaczone przez ω), takie że:

$$\mathcal{L}(2[0_E]) = R \oplus Rx, \qquad \mathcal{L}(3[0_E]) = R \oplus Rx \oplus Ry$$

oraz:

$$x = \frac{1}{T^2} + \ldots, \qquad y = \frac{1}{T^3} + \ldots .$$

Ponadto elementy:

$$1, x, y, x^2, xy, x^3, y^2 \in \mathcal{L}(6[0_E])$$

muszą być liniowo zależne, co pozwala na uzyskanie równania postaci:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Jednoznacznie określone podstawienia liniowe pozwalają na uzyskanie równania postaci:

$$y^2 = x^3 + Ax + B.$$

Dla krzywej określonej takim równaniem odzyskujemy formę różniczkową ω jako dx/y. □

Wniosek 2.1.4. *Niech R będzie pierścieniem lokalnym spełniającym $6 \in R^\times$. Każda krzywa eliptyczna nad R jest izomorficzna z pewną krzywą Weierstrassa. Dowolne dwa równania Weierstrassa odpowiadające jednej krzywej są powiązane zamianą zmiennych:*

$$x_1 = u^2 \cdot x_2, \quad y_1 = u^3 \cdot y_2, \quad \text{gdzie } u \in R^\times.$$

Dowód. Zauważmy, że $\mathrm{Spec}(R)$ zawiera dokładnie jeden punkt domknięty, więc dla dowolnego pokrycia otwartego

$$\mathrm{Spec}(R) = \bigcup_i U_i$$

musi istnieć indeks i taki, że $\mathrm{Spec}(R) = U_i$. Stąd oraz z powyższego twierdzenia, dowolna krzywa eliptyczna nad R jest zadana równaniem Weierstrassa.

W celu wykazania jednoznaczności zauważmy, że dowolne dwie niezerowe formy różniczkowe ω_1, ω_2 generujące snop $\pi_*(\Omega_{E/\mathrm{Spec}(R)})$ różnią się o stałą: $\omega_1 = u\omega_2$, gdzie $u \in R^\times$. Prześledzenie poprzedniego dowodu pokazuje, że morfizmy $(x_1, y_1), (x_2, y_2)$ wyznaczone przez ω_1, ω_2 muszą spełniać warunki tezy. □

Z wniosku 2.1.4 wynika w szczególności, że j-niezmiennik krzywej określonej nad pierścieniem lokalnym jest dobrze określonym niezmiennikiem izomorfizmu, nie zmieniającym się również przy zmianie bazy. Warto również zauważyć, że jeżeli E jest krzywą eliptyczną zadaną równaniem (2.1) nad pierścieniem lokalnym R, to zbiór punktów R-wymiernych na E można utożsamiać ze zbiorem:

$$\{[x : y : z] \in \mathbb{P}^3(R) : f(x, y, z) = 0\}. \tag{2.2}$$

Wynika to bezpośrednio z twierdzenia A.4.

Okazuje się, że krzywa eliptyczna nad dowolnym schematem S ma jednoznacznie wyznaczoną strukturę schematu grupowego. Dla dowolnego T-schematu X o morfizmie strukturalnym $f : X \to T$ wprowadzamy oznaczenie:

$$Pic^{(0)}(X/T) := \left\{ \mathcal{L} : \mathcal{L} \text{ jest snopem odwracalnym na } X \text{ oraz } \forall_{t \in T} \quad \deg \mathcal{L}_t = 0 \right\} \Big/ \sim$$

gdzie:

- $\mathcal{L}_t$ oznacza snop $\mathcal{L}$ obcięty do domkniętego podschematu X_t,
- $\deg \mathcal{L}_t$ oznacza stopień snopa odwracalnego $\mathcal{L}_t$, zdefiniowany jak w [Har77, Ex. II.6.12],
- $\mathcal{L}_1 \sim \mathcal{L}_2$ wtedy i tylko wtedy, gdy istnieje odwracalny snop $\mathcal{L}_0$ na T taki, że

$$\mathcal{L}_1 \cong \mathcal{L}_2 \otimes f^*(\mathcal{L}_0).$$

Zbiór $Pic^{(0)}(X/T)$ wraz z iloczynem tensorowym jest grupą abelową.
Niech $E_T := E \times_S T$. Okazuje się, że dla dowolnego S-schematu T odwzorowanie:

$$\begin{aligned} E(T) = E_T(T) &\longrightarrow Pic^{(0)}(E_T/T) \\ P &\longmapsto [I^{-1}(P) \otimes I(0_{E_T})] \end{aligned}$$

(gdzie $I(P)$ jest snopem $\mathcal{O}_{E_T}$-ideałów odpowiadającym punktowi P, traktowanemu jako efektywny dywizor Cartier stopnia 1) jest bijekcją. Szczegóły tego rozumowania przedstawione są w [KM85, Theorem 2.1.2]. Pozwala to na określenie w funktorialny sposób struktury grupy abelowej na $E(T)$, co zadaje strukturę schematu grupowego na E (patrz Dodatek B).

Zajmiemy się teraz n-torsją krzywej eliptycznej i spróbujemy uogólnić otrzymane wcześniej wyniki. W tym celu rozważmy najpierw tzw. **uniwersalną krzywą Weierstrassa** $\mathcal{C}$, czyli krzywą Weierstrassa $E_{A,B}$ nad pierścieniem $\mathcal{A} := \mathbb{Z}[A, B, \frac{1}{6}, \frac{1}{\Delta(A,B)}]$. Ma ona następującą własność uniwersalności: jeżeli E jest krzywą eliptyczną zadaną równaniem Weierstrassa nad dowolnym schematem afinicznym $S = \mathrm{Spec}(R)$ oraz $6 \in R^\times$, to istnieje dokładnie jedna para morfizmów $E \to \mathcal{C}$ oraz $S \to \mathrm{Spec}(\mathcal{A})$ (morfizmy te powstają przez zastąpienie zmiennych A, B odpowiednimi współczynnikami krzywej) taka, że diagram:

$$\begin{array}{ccccc} E & \longrightarrow & \mathbb{P}^2_S & \longrightarrow & S \\ \downarrow & & \downarrow & & \downarrow \\ \mathcal{C} & \longrightarrow & \mathbb{P}^2_{\mathcal{A}} & \longrightarrow & \mathrm{Spec}(\mathcal{A}) \end{array}$$

jest przemienny.

Twierdzenie 2.1.5. *Niech S będzie lokalnie noetherowskim schematem, spełniającym $6 \in \mathcal{O}_S(S)^\times$. Wtedy $E[n]$ jest skończonym i płaskim schematem grupowym rangi n^2, który jest samodualny w sensie Cartier.*

Szkic dowodu na podstawie [KM85, Theorem 2.3.1]. Wybierając pokrycie afiniczne, możemy bez straty ogólności zastąpić S przez schemat afiniczny. Z własności uniwersalności możemy założyć, że E jest uniwersalną krzywą eliptyczną. Wtedy $S = \operatorname{Spec} \mathbb{Z}[A, B, \frac{1}{6}, \frac{1}{\Delta}]$ jest regularnym schematem, więc E jest również regularny jako gładki schemat nad schematem regularnym. Zauważmy, że:

- $[n]$ jest płaski, bo każdy skończony morfizm między regularnymi schematami tego samego wymiaru jest płaski ([KM85, str. 507]),
- $[n]$ jest właściwy, bo morfizm $E \to S$ jest właściwy, więc każdy endomorfizm E musi być również właściwy ([Sta16, Tag 01W6]),
- $[n]$ ma skończone włókna. Wynika to z teorii krzywych eliptycznych nad ciałami, jako że włókno $E[n]$ nad punktem $s \in S$ jest n-torsją odpowiedniej krzywej eliptycznej nad ciałem $\kappa(s)$,
- $[n]$ jest skończony. Z Głównego Twierdzenia Zariskiego w wersji Grothendiecka ([Sta16, Tag 02LS]) wynika, że morfizm jest skończony wtw. gdy jest właściwy i ma skończone włókna.

Dla obliczenia rangi schematu grupowego $E[n]$ wystarczy zauważyć, że z teorii krzywych eliptycznych nad $\mathbb{C}$, włókna punktów $\mathbb{C}$-wymiernych mają n^2 elementów. Wykazanie samodualności grupy $E[n]$ sprowadza się do podania konstrukcji iloczynu Weila, którą można znaleźć w [KM85, rozdz. 2.8]. □

2.2. Niezmienniki krzywych nad pierścieniami zupełnymi

W tym podrozdziale oraz następnych przyjmiemy następujące oznaczenia:

- R – zupełny pierścień dyskretnej waluacji v o ideale maksymalnym $\mathfrak{m} = (\pi)$,
- K – ciało ułamków dla R,
- $k := R/\mathfrak{m}$ – ciało reszt. Zakładamy, że $\operatorname{char} k = p \neq 2, 3$ oraz że k jest doskonałe,
- $R_j := R/\mathfrak{m}^j$ oraz $\mathfrak{m}_j := \mathfrak{m}/\mathfrak{m}^j \trianglelefteq R_j$ dla $j = 1, 2, \ldots$. Przyjmujemy również: $\mathfrak{m}^\infty = (0)$,
- E/R_j – krzywa eliptyczna nad R_j.

Zauważmy, że jeżeli $i \leqslant j$, to możemy określić redukcję krzywej E/R_j do R_i jako $E \times_{R_j} R_i$. Będziemy ją zazwyczaj oznaczali przez E_{R_i}.

Okazuje się, że krzywe eliptyczne nad R_j są zasadniczo wyznaczone przez swój j-niezmiennik oraz klasę izomorfizmu redukcji do k. Problem stwarzają krzywe spełniające: $j(E_k) \in \{0, 1728\}$. Dla takich krzywych redukcja E_k przechowuje zbyt małą ilość informacji o wyjściowej krzywej. W tym celu potrzebujemy następującej niestandardowej definicji:

Definicja 2.2.1. Krzywa eliptyczna $E_{A,B}/R_j$ jest **typu** (m, n), jeżeli

$$A = \pi^m \cdot \alpha, \quad B = \pi^n \cdot \beta \quad \text{dla } \alpha, \beta \in R_j^\times$$

oraz jest **typu** $(\infty, 0)$ (odpowiednio $(0, \infty)$), jeżeli $A = 0$ (odpowiednio $B = 0$).

Z wniosku 2.1.4 wynika, że typ krzywej eliptycznej nie zależy od klasy izomorfizmu. Zauważmy przy tym, że:

- krzywa E/R_j jest typu $(m, 0)$ dla $1 \leqslant m \leqslant \infty$ wtedy i tylko wtedy, gdy $j(E_k) = 0$,
- krzywa E/R_j jest typu $(0, n)$ dla $1 \leqslant n \leqslant \infty$ wtedy i tylko wtedy, gdy $j(E_k) = 1728$,
- w pozostałych przypadkach krzywa E/R_j ma typ $(0, 0)$.

Zgodnie z tym, co zapowiadaliśmy, krzywe typu $(0, 0)$ są wyznaczone przez redukcję oraz j-niezmiennik:

Twierdzenie 2.2.2. *Klasa izomorfizmu krzywej eliptycznej E/R_j typu $(0, 0)$ jest wyznaczona jednoznacznie przez swoją redukcję E_k oraz j-niezmiennik $j(E) \in R_j$.*

Dowód. Załóżmy, że krzywe $E_{A,B}/R_j$ oraz $E_{a,b}/R_j$ spełniają:

$$E_{A,B} \times_{R_j} k \cong E_{a,b} \times_{R_j} k \tag{2.3}$$

$$j(E_{A,B}) = j(E_{a,b}) \tag{2.4}$$

oraz $A, B, a, b \in R_j^\times$. Wtedy z (2.3) istnieje $u \in k^\times$ takie, że

$$A \equiv u^4 \cdot a \pmod{\mathfrak{m}_j}, \qquad B \equiv u^6 \cdot b \pmod{\mathfrak{m}_j}.$$

Z (2.4) dostajemy zaś:

$$A^3 \cdot b^2 = a^3 \cdot B^2. \tag{2.5}$$

Zauważmy, że z lematu Hensela równania:

$$x^4 - A \cdot a^{-1} = 0$$
$$x^6 - B \cdot b^{-1} = 0$$

mają w R_j jedyne rozwiązania podnoszące u. Nazwijmy je odpowiednio u_1 oraz u_2. Z drugiej strony z równości (2.5) wynika, że zarówno u_1, jak i u_2 spełniają równanie:

$$0 = x^{12} - (A \cdot a^{-1})^3 = x^{12} - (B \cdot b^{-1})^2,$$

które z lematu Hensela ma jednoznaczne rozwiązanie podnoszące u. Stąd $u_1 = u_2$ oraz odwzorowanie $(x, y) \mapsto (u_1^2 \cdot x', u_1^3 \cdot y')$ jest izomorfizmem. □

Krzywe E/R_j pozostałych typów wymagają osobnego rozpatrzenia. Niech $E_{A,B}/R_j$ będzie krzywą typu $(m, 0)$ dla $1 \leqslant m < \infty$ oraz $A = \pi^m \cdot \alpha$. Zdefiniujmy:

$$j_1(E_{A,B}) = \frac{B^2}{\alpha^3} \pmod{\mathfrak{m}_j^{j-m}} \quad \in R_{j-m}.$$

Zauważmy, że α jest wyznaczone jednoznacznie modulo $\mathfrak{m}_j^{j-m}$. Podobnie jak poprzednio $j_1(E_{A,B})$ nie zależy od klasy izomorfizmu krzywej, a jedynie od wyboru uniformizatora π. Analogicznie dla krzywej typu $(0, n)$ dla $1 \leqslant n < \infty$ oraz $B = \pi^n \cdot \beta$ definiujemy:

$$j_1(E_{A,B}) = \frac{A^3}{\beta^2} \pmod{\mathfrak{m}_j^{j-n}} \quad \in R_{j-n}.$$

Twierdzenie 2.2.3.

(a) Klasa izomorfizmu krzywej E/R_j typu $(\infty, 0)$ lub $(0, \infty)$ jest wyznaczona jednoznacznie przez klasę izomorfizmu jej redukcji E_k.

(b) Załóżmy, że $3|(p-1)$. Wtedy klasa izomorfizmu krzywej typu $(m, 0)$ (gdzie $1 \leqslant m < \infty$) jest wyznaczona jednoznacznie przez klasę izomorfizmu E_k oraz przez $j_1(E) \in R_{j-m}$.

(c) Załóżmy, że $4|(p-1)$. Wtedy klasa izomorfizmu krzywej typu $(0, n)$ (gdzie $1 \leqslant n < \infty$) jest wyznaczona jednoznacznie przez klasę izomorfizmu E_k oraz przez $j_1(E) \in R_{j-n}$.

Dowód.

(a) Załóżmy, że:

$$E_{0,B} \times_{R_j} k \cong E_{0,b} \times_{R_j} k.$$

Wtedy istnieje $u \in k^\times$ takie, że $B \equiv b \cdot u^6 \pmod{\mathfrak{m}_j}$. Korzystając z lematu Hensela, możemy podnieść $u \in k^\times$ do $u_1 \in R_j^\times$ spełniającego równanie: $x^6 - B \cdot b^{-1} = 0$, otrzymując w ten sposób izomorfizm $E_{0,B} \cong E_{0,b}$. Dla krzywych typu $(0, \infty)$ przeprowadzamy analogiczne rozumowanie.

(b) Z założenia $3|(p-1)$ wynika, że $\mu_3 \subset k^\times$. Niech ζ będzie pierwiastkiem trzeciego stopnia z jedności podniesionym za pomocą lematu Hensela do $R_j^\times$. Załóżmy, że $A = \pi^m \cdot \alpha$, $a = \pi^m \cdot \gamma$ oraz:

$$E_{A,B} \times_{R_j} k \cong E_{a,b} \times_{R_j} k, \qquad j_1(E_{A,B}) = j_1(E_{a,b}).$$

Wtedy istnieje $u \in k^\times$ takie, że $B \equiv b \cdot u^6 \pmod{\mathfrak{m}_j}$; za pomocą lematu Hensela możemy podnieść u do $u_1 \in R_j^\times$ spełniającego: $B = b \cdot u_1^6$. Dostajemy wtedy:

$$\alpha^3 \cdot b^2 \equiv \gamma^3 \cdot B^2 \pmod{\mathfrak{m}_j^{j-m}},$$

co pociąga, że:

$$\alpha^3 \equiv \gamma^3 \cdot u_1^{12} \pmod{\mathfrak{m}_j^{j-m}}.$$

Korzystając z lematu Hensela dla równania $x^3 - \alpha^3$ stwierdzamy, że:

$$\alpha \equiv \zeta^t \cdot \gamma \cdot u_1^4 \pmod{\mathfrak{m}_j^{j-m}} \qquad \text{dla pewnego } t \in \{0, 1, 2\}.$$

Mnożąc powyższą kongruencję przez π^m oraz zastępując u_1 przez $\zeta^t \cdot u_1$ dostajemy równości:

$$A = a \cdot u_1^4, \qquad B = b \cdot u_1^6.$$

(c) Dowód jest analogiczny do dowodu (b).

□

Uwaga 2.2.4. *Zauważmy, że $\mathbb{Z}[\omega] \subset End(E_{0,b}/k)$, więc z twierdzenia 1.2.3 wynika, że krzywa $E_{0,b}/k$ jest zwyczajna wtedy i tylko wtedy, gdy p rozkłada się całkowicie w $\mathbb{Z}[\omega]$, czyli gdy $3|(p-1)$. Analogicznie krzywa $E_{a,0}/k$ jest zwyczajna wtedy i tylko wtedy, gdy $4|(p-1)$. Udowodnione przez nas twierdzenia 2.2.2 oraz 2.2.3 zostaną wykorzystane w dowodzie twierdzenia 2.2.7, które dotyczy wyłącznie podniesień krzywych zwyczajnych. Dlatego rezygnujemy z omówienia pozostałych przypadków.*

Z twierdzenia 2.1.5 wynika, że $E[p^\infty] := (E[p^n])_n$ jest grupą p-podzielną wysokości 2 (patrz Dodatek B). Przypomnijmy, że dla $j < \infty$ podniesienia krzywej eliptycznej nad $\mathrm{Spec}(k)$ do $\mathrm{Spec}(R_j)$ są wyznaczone jednoznacznie przez podniesienia jej grupy p-podzielnej.

Twierdzenie 2.2.5 (wniosek z twierdzenia Serre'a-Tate'a B.15)**.**
Niech $\mathcal{R}$ będzie lokalnym pierścieniem Artina o ideale maksymalnym $\mathfrak{m}$ oraz załóżmy, że $k := \mathcal{R}/\mathfrak{m}$ jest ciałem charakterystyki p. Rozważmy kategorię $\mathcal{D}$, której elementami są trójki (E, G, Φ), gdzie:

- *E jest krzywą eliptyczną nad k,*
- *G jest p-podzielną grupą nad $\mathcal{R}$,*
- *$\Phi : E[p^\infty] \to G_k$ jest izomorfizmem,*

z naturalnie zadanymi morfizmami. Wtedy funktor $\mathcal{E} \mapsto (\mathcal{E}_k, \mathcal{E}[p^\infty], \Phi)$ jest równoważnością kategorii krzywych eliptycznych nad $\mathcal{R}$ oraz kategorii $\mathcal{D}$.

Niech E/k będzie zwyczajną krzywą eliptyczną. Zauważmy, że z lematu A.3 wynika, że étalna grupa p-podzielna $E[p^\infty]^{et}$ ma jednoznaczne podniesienie étalne G^{et} do $\mathcal{R}$. Niech $G^0 := (G^{et})^\vee$ będzie grupą dualną w sensie Cartier. Wtedy z twierdzenia 2.2.5 wynika, że istnieje dokładnie jedno podniesienie $\mathbb{E}/\mathcal{R}$ krzywej E/k spełniające warunek:

$$\mathbb{E}[p^\infty] \cong G^{et} \times G^0.$$

Krzywą $\mathbb{E}/\mathcal{R}$ o tej własności nazywać będziemy **kanonicznym podniesieniem** krzywej E/k. Kanoniczne podniesienie zachowuje część własności wyjściowej krzywej. W szczególności jeżeli $\mathbb{E}_1/\mathcal{R}, \mathbb{E}_2/\mathcal{R}$ są kanonicznymi podniesieniami krzywych $E_1/k, E_2/k$, to odwzorowanie redukcji:

$$\mathrm{Hom}_{\mathcal{R}}(\mathbb{E}_1, \mathbb{E}_2) \xrightarrow{\sim} \mathrm{Hom}_k(E_1, E_2) \tag{2.6}$$

jest izomorfizmem. Istotnie, zauważmy, że z twierdzenia 2.2.5 wynika, że dowolny morfizm $f \in \mathrm{Hom}_k(E_1, E_2)$ jest wyznaczony jednoznacznie przez morfizmy

$$f^{et} : E_1[p^\infty]^{et} \to E_2[p^\infty]^{et}, \qquad f^0 : E_1[p^\infty]^0 \to E_2[p^\infty]^0.$$

Z lematu A.3 oraz z dualności Cartier wynika, że morfizmy te podnoszą się jednoznacznie do morfizmów $F^{et} : \mathbb{E}_1[p^\infty]^{et} \to \mathbb{E}_2[p^\infty]^{et}$, $F^0 : \mathbb{E}_1[p^\infty]^0 \to \mathbb{E}_2[p^\infty]^0$, zadając tym samym morfizm $F^{et} \times F^0 : \mathbb{E}_1[p^\infty] \to \mathbb{E}_2[p^\infty]$. To dowodzi izomorfizmu (2.6).

Opisaną wyżej teorię możemy zastosować do pierścienia $\mathcal{R} := R_j$, gdzie $j < \infty$. Okazuje się jednak, że kanoniczne podniesienie można zdefiniować również dla pierścienia R:

Uwaga 2.2.6. *Dowolna krzywa formalna jest algebraiczna. Dlatego też ciąg podniesień kanonicznych zwyczajnej krzywej $\widetilde{E}/k$ do pierścieni R_j dla $j = 2, 3, \ldots$ zadaje krzywą eliptyczną nad R. Tą krzywą eliptyczną nad R nazywamy **kanonicznym podniesieniem** $\widetilde{E}$ do R. Fakt ten znany jest jako **twierdzenie Deuringa o podniesieniu**. Relacja (2.6) pozostaje prawdziwa, tak więc włókno generyczne kanonicznego podniesienia jest krzywą eliptyczną nad K z mnożeniem zespolonym. Okazuje się, że jest to jedyna krzywa z mnożeniem zespolonym redukująca się do $\widetilde{E}$ (patrz [Lan87, Theorem 13.13]). Tak więc dowolna krzywa eliptyczna nad K dobrej redukcji z mnożeniem zespolonym jest kanonicznym podniesieniem swojej redukcji do k.*

Wykażemy teraz „efektywną wersję twierdzenia Serre'a-Tate'a" – okazuje się bowiem, że podniesienie już części grupy p-podzielnej do R_j wyznacza krzywą jednoznacznie.

Twierdzenie 2.2.7 (efektywna wersja twierdzenia Serre'a-Tate'a)**.**
Niech $\widetilde{E}/k$ będzie zwyczajną krzywą eliptyczną oraz $j \in \mathbb{N}$. Jeżeli E_1, E_2 są podniesieniami $\widetilde{E}$ do R_j oraz

$$E_1[p^{j-1}] \cong E_2[p^{j-1}],$$

to $E_1 \cong E_2$.

Przed dowodem ustalimy notację i udowodnimy prosty lemat. Dowód opiera się na obliczeniu odpowiedniej grupy rozszerzeń, powstałej z ciągu spójno-étalnego grupy p-podzielnej. Ciąg ten jest jednak „skręcony" przez pewien charakter χ (patrz twierdzenie 1.2.1), dlatego też musimy przejść do domknięcia algebraicznego $\overline{k}$.
Niech $\widehat{K^{un}}$ będzie uzupełnieniem maksymalnego nierozgałęzionego rozszerzenia K^{un} ciała K, zaś A – pierścieniem liczb całkowitych w $\widehat{K^{un}}$ o ideale maksymalnym $\mathfrak{M} = (\pi)$. Przyjmijmy standardowe oznaczenie $A_i := A/\mathfrak{M}^i$, $\mathfrak{M}_i = \mathfrak{M}/\mathfrak{M}^i$, wtedy $R_i \hookrightarrow A_i$. Zauważmy, że A spełnia założenia poprzednich twierdzeń. Ponadto $A/\mathfrak{M} = \overline{k}$ jest ciałem algebraicznie domkniętym, co pozwala na zastąpienie charakteru χ przez charakter trywialny. Powrót do pierścienia R_i umożliwią nam twierdzenia 2.2.2 oraz 2.2.3.

Lemat 2.2.8. *Zachowując powyższe oznaczenia mamy:*

$$(A_j^\times)^{p^m} = (A_j^\times)^{p^{m+1}} \qquad \textit{dla } m \geqslant j-1.$$

Dowód. Stosujemy indukcję ze względu na j. Dla $j = 1$ jest to oczywiste, jako że:

$$\overline{k} = \overline{k}^p = \dots.$$

Załóżmy, że teza zachodzi dla j. Niech $a = b^{p^m} \in (A_{j+1}^\times)^{p^m}$, $m \geqslant j$. Wtedy z założenia indukcyjnego:

$$(b^{p^{m-1}} \mod \mathfrak{M}_{j+1}^j) \in (A_j^\times)^{p^{m-1}} = (A_j^\times)^{p^m},$$

więc $b^{p^{m-1}} = c^{p^m} + m$, gdzie $m \in \mathfrak{M}_{j+1}^j$. Stąd:

$$\begin{aligned} a = (b^{p^{m-1}})^p &= (c^{p^m} + m)^p \\ &= c^{p^{m+1}} + \binom{p}{1} c^{p^m \cdot (p-1)} m + \dots \\ &= c^{p^{m+1}} \in (A_{j+1}^\times)^{p^{m+1}} \end{aligned}$$

jako że $\binom{p}{i} c^{p^m \cdot (p-i)} m^i = 0$ w A_{j+1} dla $i = 1, 2, \dots$. □

Dowód twierdzenia 2.2.7. Niech $\widetilde{E}/k$ będzie ustaloną krzywą zwyczajną, zaś E/A_j – jej dowolnym podniesieniem. Zauważmy najpierw, że ciąg spójno-étalny dla grupy p-podzielnej $G := E[p^\infty]$ jest postaci:

$$0 \to \mu_{p^\infty} \to G \to \underline{\mathbb{Q}_p/\mathbb{Z}_p} \to 0 \tag{2.7}$$

Istotnie, z twierdzenia 1.2.1 ciąg spójno-étalny dla $\widetilde{E}_{\overline{k}}$ jest postaci (2.7). Ponadto dowolny étalny skończony schemat grupowy nad $\overline{k}$ ma jednoznaczne podniesienie do A_j (lemat A.3), więc:

$$E[p^n]^{et} \cong \underline{\mathbb{Z}/p^n}.$$

Pozostaje zauważyć, że $E[p^n]$ jest samodualne w sensie Cartier, więc $\mu_{p^n} = (\underline{\mathbb{Z}/p^n})^\vee \hookrightarrow E[p^n]$. Porównując rangi dostajemy $\mu_{p^n} \cong E[p^n]^0$. To dowodzi, że ciąg spójno-étalny dla $E[p^\infty]$ ma postać (2.7). Na odwrót, jeżeli ciąg spójno-étalny grupy G jest postaci (2.7), to $G_{\overline{k}}$ również jest tej postaci, więc ponieważ ciąg spójno-étalny nad $\overline{k}$ rozszczepia się:

$$G_{\overline{k}} \cong \underline{\mathbb{Q}_p/\mathbb{Z}_p} \times_{\overline{k}} \mu_{p^\infty} \cong \widetilde{E}[p^\infty].$$

Z powyższych rozważań oraz z twierdzenia Serre'a-Tate'a wynika, że podniesienia krzywej $\widetilde{E}/k$ do A_j są w bijekcji z elementami grupy $\mathrm{Ext}^1_{p\text{-}\mathbf{div}/A_j}(\underline{\mathbb{Q}_p/\mathbb{Z}_p}, \mu_{p^\infty})$. Mamy:

$$\mathrm{Ext}^1_{p\text{-}\mathbf{div}/A_j}(\underline{\mathbb{Q}_p/\mathbb{Z}_p}, \mu_{p^\infty}) = \varprojlim \mathrm{Ext}^1_{\mathbf{GS}/A_j}(\underline{\mathbb{Z}/p^n}, \mu_{p^n})$$

oraz z twierdzenia B.12:

$$\mathrm{Ext}^1_{\mathbf{GS}/A_j}(\underline{\mathbb{Z}/p^n}, \mu_{p^n}) = A_j^\times/(A_j^\times)^{p^n}$$

Z lematu 2.2.8 stwierdzamy więc, że naturalne odwzorowanie:

$$\varprojlim \mathrm{Ext}^1_{\mathbf{GS}/A_j}(\underline{\mathbb{Z}/p^n}, \mu_{p^n}) \longrightarrow \mathrm{Ext}^1_{\mathbf{GS}/A_j}(\underline{\mathbb{Z}/p^{j-1}}, \mu_{p^{j-1}})$$

jest izomorfizmem oraz podniesienie $\widetilde{E}[p^{j-1}]$ do A_j wyznacza jednoznacznie podniesienie całej grupy p-podzielnej do A_j, a co za tym idzie podniesienie $\widetilde{E}$ do A_j.
Załóżmy, że krzywe $E_1, E_2/R_j$ spełniają założenia twierdzenia. Wtedy z powyższego rozumowania wynika, że są one izomorficzne nad A_j. W szczególności mają ten sam typ. Jeżeli są typu $(0,0)$ to z izomorfizmu $(E_1)_{A_j} \cong (E_2)_{A_j}$ stwierdzamy, że

$$j(E_1) = j((E_1)_{A_j}) = j((E_2)_{A_j}) = j(E_2),$$

co oznacza, że E_1 oraz E_2 są R-izomorficzne. Dla pozostałych typów przeprowadzamy podobne rozumowanie porównując niezmiennik j_1. □

W szczególności, z powyższego twierdzenia wynika, że podniesienie $\mathbb{E}/R_j$ zwyczajnej krzywej $\widetilde{E}/k$ jest kanoniczne wtedy i tylko wtedy, gdy:

$$E[p^{j-1}] \cong E[p^{j-1}]^0 \oplus E[p^{j-1}]^{et}.$$

Fakt ten wykorzystamy w twierdzeniu 3.1.5 dla $j = 2$.

2.3. Odwzorowanie redukcji

W tej części pracy zajmiemy się opisem odwzorowania redukcji $E \to E_{R_i}$ na punktach R_j-wymiernych. Przypomnijmy, że punkty te można utożsamiać z trójkami $[x : y : z] \in \mathbb{P}^2(R_j)$, spełniającymi równanie Weierstrassa (patrz równość (2.2)). Naturalne odwzorowanie redukcji $R_j \to R_i$ dla $i \leqslant j$ będziemy oznaczali przez $t \mapsto \widetilde{t}$. Pomijamy przy tym zazwyczaj zależność od i, j. Podobnie, jeżeli kontekst będzie jasny, będziemy oznaczali $\widetilde{E} := E_{R_i}$.

Wybierzmy punkt $P = [x_0 : y_0 : z_0] \in \mathbb{P}^2(R_j)$ – wtedy punkt $\widetilde{P} = [\widetilde{x_0} : \widetilde{y_0} : \widetilde{z_0}]$ jest dobrze zdefiniowanym elementem przestrzeni rzutowej $\mathbb{P}^2(R_i)$, a ponadto jeżeli $P \in E(R_j)$, to $\widetilde{P} \in \widetilde{E}(R_i)$. Postaramy się teraz opisać jądro oraz obraz tego przekształcenia. Wprowadźmy następujące oznaczenie:

$$E_i(R_j) := \{[x : y : z] \in E(R_j) : \quad x \in \mathfrak{m}_j^i, \quad y \in R_j^\times, \quad z \in \mathfrak{m}_j^{3i}\}, \text{ dla } i = 1, 2, \ldots \tag{2.8}$$

Okazuje się, że $E_i(R_j)$ jest podgrupą $E(R_j)$. Zachodzi ponadto następujące stwierdzenie:

Stwierdzenie 2.3.1. *Niech E/R_j będzie krzywą eliptyczną. Wówczas redukcja $E(R_j) \to \widetilde{E}(R_i)$ jest homomorfizmem grup abelowych. Ponadto ciąg:*

$$0 \to E_i(R_j) \to E(R_j) \to \widetilde{E}(R_i) \to 0$$

(gdzie pierwsze przekształcenie jest inkluzją, zaś drugie – redukcją) jest dokładny.

Dowód. Z teorii schematów grupowych wynika w prosty sposób, że redukcja jest homomorfizmem. Niech $P = [x_0 : y_0 : z_0]$. Z definicji wynika, że $\widetilde{P} = 0_{\widetilde{E}}$ wtedy i tylko wtedy, gdy istnieje $\lambda \in R_i^\times$ takie, że $(x_0, y_0, z_0) \equiv \lambda \cdot (0, 1, 0) \pmod{\mathfrak{m}_j^i}$, czyli gdy $x \in \mathfrak{m}_j^i, y \in R_j^\times, z \in \mathfrak{m}_j^i$. Z równania $y^2 \cdot z = x^3 + Axz^2 + z^3$ wynika jednak, że wówczas $z \in \mathfrak{m}_j^{3i}$. Stąd $E_i(R_j)$ jest jądrem redukcji.
Pozostaje zauważyć, że redukcja jest epimorfizmem. Wynika to jednak z lematu Hensela, jako że dowolny punkt na krzywej $\widetilde{E}/R_i$ jest gładki. □

Zajmiemy się teraz opisem grup $E_i(R_j)$. W tym celu będziemy potrzebowali pojecia grupy formalnej. Niech $\mathcal{R}$ będzie pierścieniem lokalnym o ideale maksymalnym $\mathfrak{m}$, który jest zupełny względem topologii $\mathfrak{m}$-adycznej. Zauważmy, że pierścienie R_j spełniają te założenia.

Definicja 2.3.2. Grupą formalną $\mathcal{F}$ nad $\mathcal{R}$ nazywamy szereg potęgowy $F \in \mathcal{R}[[X, Y]]$ o następujących własnościach:

- $F(X, Y) \equiv X + Y \pmod{(X, Y)^2}$,
- $F(X, F(Y, Z)) = F(F(X, Y), Z)$,
- $F(X, Y) = F(Y, X)$,
- istnieje dokładnie jeden szereg potęgowy $i(T) \in \mathcal{R}[[T]]$ spełniający: $F(T, i(T)) = 0$,
- $F(X, 0) = X$, $F(0, Y) = Y$.

Grupą związaną z $\mathcal{F}/\mathcal{R}$, oznaczaną przez $\mathcal{F}(\mathfrak{m})$, będziemy nazywali zbiór $\mathfrak{m}$ wraz z działaniem $x \oplus_{\mathcal{F}} y = F(x, y)$. Element odwrotny dany jest wzorem $\ominus_{\mathcal{F}} x = i(x)$. Podobnie, definiujemy grupy $\mathcal{F}(\mathfrak{m}^n)$ jako zbiór $\mathfrak{m}^n$ z działaniem $\oplus_{\mathcal{F}}$.

Zauważmy, że mając daną grupę formalną $\mathcal{F}/R$, możemy ją zredukować do grupy formalnej $\widetilde{\mathcal{F}}/R_j$ redukując jej współczynniki.

Twierdzenie 2.3.3. *Niech $\mathcal{F}/R$ będzie grupą formalną, zaś $\widetilde{\mathcal{F}}/R_j$ jej redukcją do R_j. Wtedy dla $r > v(p)/(p-1)$ mamy następujące izomorfizmy, które są przemienne z odwzorowaniem redukcji:*

- $\mathcal{F}(\mathfrak{m}^r) \cong \mathfrak{m}^r$,
- $\widetilde{\mathcal{F}}(\mathfrak{m}_j^r) = \mathfrak{m}_j^r$,

gdzie $\mathfrak{m}^r$, $\mathfrak{m}_j^r$ traktujemy jako grupy ze zwykłym dodawaniem.

Szkic dowodu na podstawie [Sil09, Thm IV.6.4]:
Niech grupa formalna $\mathcal{F}/R$ będzie zadana przez szereg potęgowy $F(X, Y)$. Rozważmy szeregi potęgowe:

$$F_X(0, T)^{-1} = 1 + c_1 T + c_2 T^2 + \ldots, \qquad \text{gdzie } c_i \in R$$

$$\log_{\mathcal{F}}(T) := \int F_X(0, T)^{-1} dT = T + \frac{c_1}{2} T^2 + \frac{c_2}{3} T^3 + \ldots$$

Zgodnie z algebraiczną wersją twierdzenia o funkcji uwikłanej ([Sil09, Thm IV.2.4]) istnieje dokładnie jeden szereg potęgowy $\exp_{\mathcal{F}} \in K[[T]]$ spełniający:

$$\log_{\mathcal{F}} \circ \exp_{\mathcal{F}}(T) = \exp_{\mathcal{F}} \circ \log_{\mathcal{F}}(T) = T$$

Dokładniejsza analiza współczynników ([Sil09, Lemma IV.5.4.]) pozwala na stwierdzenie, że $\exp_{\mathcal{F}}(T) = \sum_{n \geqslant 1} \frac{a_n}{n!} T^n$ dla pewnych $a_n \in R$. Zauważmy, że:

$$v(n!) = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right] v(p) \leqslant \sum_{i=1}^{[\log_p n]} \frac{n}{p^i} \cdot v(p) = \frac{n \cdot v(p)}{p-1} \cdot \left(1 - p^{-[\log_p n]}\right) \leqslant \frac{(n-1) \cdot v(p)}{p-1}$$

Stąd dla $x \in \mathfrak{m}^r$, $r > v(p)/(p-1)$ szeregi definiujące $\exp_{\mathcal{F}}, \log_{\mathcal{F}}$ są zbieżne oraz wyznaczają izomorfizmy:

$$\log_{\mathcal{F}} : \mathcal{F}(\mathfrak{m}) \to \mathfrak{m}$$
$$\exp_{\mathcal{F}} : \mathfrak{m} \to \mathcal{F}(\mathfrak{m})$$

Redukując wyrazy tych szeregów dostajemy szeregi $\exp_{\widetilde{\mathcal{F}}}, \log_{\widetilde{\mathcal{F}}}$, wyznaczające izomorfizmy $\widetilde{\mathcal{F}}(\mathfrak{m}_j^r) \cong \mathfrak{m}_j^r$. Z konstrukcji jasno wynika, że izomorfizmy te komutują z redukcją. □

Okazuje się, że z każdą krzywą eliptyczną związana jest grupa formalna. Opiszemy pokrótce jej konstrukcję; szczegóły można znaleźć w [Sil09, Proposition IV.1.1]. Podstawmy w równaniu Weierstrassa krzywej E:

$$z = -\frac{x}{y} \text{ oraz } w = -\frac{1}{y}, \qquad \text{tak aby } x = \frac{z}{w} \text{ oraz } y = -\frac{1}{w}.$$

Przenosimy w ten sposób punkt w nieskończoności na punkt $(0,0)$ oraz uzyskujemy równanie postaci:

$$w = z^3 + Azw^2 + Bw^3 = g(z,w).$$

Zdefiniujmy ciąg wielomianów $(g_m)_m$ za pomocą rekurencji:

$$g_1(z,w) = g(z,w), \qquad g_{m+1}(z,w) = g_m(z, g(z,w)).$$

Okazuje się, że ciąg $(g_m(z,0))_m$ jest zbieżny w pierścieniu szeregów formalnych $\mathbb{Z}[A,B][[z]]$. Oznaczmy jego granicę przez $w(z)$. Jest to jedyny szereg spełniający równość:

$$w(z) = g(z, w(z))$$

i jest on postaci:

$$w(z) = z^3 \cdot (1 + A_1 z + A_2 z^2 + \ldots),$$

gdzie $A_n \in \mathbb{Z}[A,B]$. Proste przeliczenia pozwalają na stwierdzenie, że trzeci punkt przecięcia prostej przechodzącej przez punkty $(z_1, w(z_1))$, $(z_2, w(z_2))$ z krzywą E ma współrzędną z zadaną wzorem:

$$z_3(z_1,z_2) = -z_1 - z_2 + \frac{-2A\lambda\nu - 3B\lambda^2\nu}{1 + A\lambda^2 + B\lambda^3}, \qquad \text{gdzie:}$$
$$\lambda(z_1,z_2) = \frac{w(z_2) - w(z_1)}{z_2 - z_1} \in \mathbb{Z}[A,B][[z_1,z_2]],$$
$$\nu(z_1,z_2) = w_1(z_1) - \lambda(z_1,z_2) \cdot z_1 \in \mathbb{Z}[A,B][[z_1,z_2]].$$

Wtedy szereg potęgowy $F(z_1,z_2) := -z_3(z_1,z_2)$ zadaje grupę formalną związaną z krzywą E. Jest ona zazwyczaj oznaczana jako $\widehat{E}$. Jej użyteczność przejawia się w następującym twierdzeniu:

Stwierdzenie 2.3.4. *Niech E/R_j będzie krzywą eliptyczną, zaś $\widehat{E}$ – związaną z nią grupą formalną. Wtedy dla $i \leqslant j$ odwzorowanie:*

$$\widehat{E}(\mathfrak{m}^i) \to E_i(R_j), \qquad z \mapsto [z : -1 : w(z)], \tag{2.9}$$

jest izomorfizmem grup.

Dowód. Zauważmy, że jeżeli $z \in \mathfrak{m}^i$, to $w(z) = z^3 \cdot (1 + \ldots) \in \mathfrak{m}^3$, więc $[z : -1 : w(z)] \in E_i(R_j)$. Odwzorowanie to jest homomorfizmem, co wynika z określenia szeregu $w(z)$, a ponadto jest iniektywne. Jeżeli zaś $[x : y : z] \in E_i(R_j)$, to $y \in R_j^\times$, możemy więc zdefiniować monomorfizm:

$$E_i(R_j) \hookrightarrow \widehat{E}(\mathfrak{m}_j^i), \qquad [x : y : z] \mapsto -x \cdot y^{-1}.$$

Łatwo zauważyć, że złożenie otrzymanych monomorfizmów:

$$\widehat{E}(\mathfrak{m}^i) \hookrightarrow E_i(R_j) \hookrightarrow \widehat{E}(\mathfrak{m}^i)$$

jest identycznością, co kończy dowód. □

Wniosek 2.3.5. *Jeżeli E/R jest krzywą eliptyczną oraz $\frac{v(p)}{p-1} < i$, to:*

$$E(R)_{tors} \hookrightarrow E_{R_i}(R_i)_{tors}.$$

Dowód. Wystarczy zauważyć, że dla $i > \frac{v(p)}{p-1}$ mamy izomorfizm: $E_i(R) \cong \mathfrak{m}^i$, więc jądro redukcji jest beztorsyjne. □

2.4. Krzywe eliptyczne nad ciałami zupełnymi

Skupimy się teraz na związku pomiędzy krzywymi eliptycznymi nad R oraz nad K. Zauważmy, że włókno generyczne dowolnej krzywej nad R jest krzywą eliptyczną nad K. Zastanowimy się, które krzywe eliptyczne nad K powstają w ten sposób. W tym celu wprowadźmy następującą definicję:

Definicja 2.4.1. Niech E/K będzie krzywą eliptyczną. Równanie Weierstrassa $E_{A,B}$ krzywej E nazwiemy **minimalnym**, jeżeli jego współczynniki należą do R, zaś waluacja wyróżnika $v(\Delta(E_{A,B}))$ jest minimalna ze wszystkich spełniających to założenie.

Proste przeliczenia pokazują, że równanie $E_{A,B}$ jest minimalne wtedy i tylko wtedy, gdy

$$\min\{v(\Delta(E_{A,B})), 3 \cdot v(A)\} < 12$$

(patrz [Sil09, Ex. VII.1(a)]). Zauważmy, że równanie minimalne zadaje pewną niekoniecznie gładką krzywą w postaci Weierstrassa nad R, której włóknem generycznym jest E/K. Pozwala to na przykład na redukowanie krzywej do pierścieni R_j. W dalszym ciągu będziemy zakładali, że wszystkie krzywe nad K dane są równaniem minimalnym, utożsamiając przy tym zazwyczaj krzywą nad K z odpowiednią krzywą nad R. Zauważmy, że E pochodzi od pewnej krzywej eliptycznej nad R wtedy i tylko wtedy, gdy wyróżnik jej równania minimalnego jest odwracalny, tzn. gdy $v(\Delta) = 0$. Mówimy wówczas, że E/K ma **dobrą redukcję**. Wtedy dowolna redukcja E_{R_j} krzywej E jest również krzywą eliptyczną. Sytuacja zmienia się, jeżeli $v(\Delta) > 0$. Krzywa zadana przez równanie minimalne nad R nie jest bowiem wówczas gładka. Mówimy wówczas o **złej redukcji**. Wyróżniamy następujące przypadki:

Definicja 2.4.2. Krzywa E/K o wyróżniku $\Delta \in \mathfrak{m}$ ma:

- **multyplikatywną redukcję**, jeżeli $\widetilde{E}/k$ jest krzywą osobliwą z tak zwanym węzłem, czyli gdy $\widetilde{A}, \widetilde{B} \neq 0$. Redukcja ta jest **rozłożona**, jeżeli proste styczne w węźle mają współczynniki w ciele k oraz **nierozłożona** w przeciwnym wypadku. Okazuje się, że redukcja multyplikatywna jest rozłożona wtedy i tylko wtedy, gdy $\gamma(E/K) \in (K^\times)^2$ (patrz [Sil94, Thm V.5.3 (b)]).
- **addytywną redukcję**, jeżeli $\widetilde{E}/k$ jest krzywą osobliwą z tak zwanym ostrzem, czyli gdy $\widetilde{\Delta} = 0$ oraz $\widetilde{A} = \widetilde{B} = 0$.

Nazwy poszczególnych typów redukcji pochodzą od struktury grupy punktów nieosobliwych $\overline{k}$-wymiernych krzywej – patrz podrozdział 1.1. Dobra oraz multyplikatywna redukcja bywają czasem nazywane **stabilną** oraz **semistabilną**. Jeżeli E/K jest krzywą jednego z wymienionych typów redukcji, to dla dowolnego skończonego rozszerzenia ciał L/K, E/L ma ten sam typ. Krzywa o redukcji multyplikatywnej nierozłożonej staje się jednak rozłożona po rozważeniu rozszerzenia kwadratowego. Redukcja addytywna jest **niestabilna**, jako że staje się stabilna lub semistabilna po zmianie bazy na skończone rozszerzenie ciała K. Fakty te można znaleźć w [Sil09, VII.5].

Podobnie jak w poprzednim rozdziale, wprowadzamy odwzorowanie redukcji $E(K) \to E(R_j)$. W tym celu wystarczy zauważyć, że $\mathbb{P}^2(K)$ oraz $\mathbb{P}^2(R)$ są w bijekcji – istotnie, dowolny punkt $P \in \mathbb{P}^2(K)$ można zapisać w postaci $[x : y : z]$ tak, by $v(x), v(y), v(z) \geqslant 0$ oraz $v(x) \cdot v(y) \cdot v(z) = 0$. Twierdzenia 2.3.1 oraz 2.3.4 można w oczywisty sposób uogólnić do tego przypadku, zastępując $\widetilde{E}(k)$ przez $\widetilde{E}_{ns}(k)$, patrz [Sil09, Proposition VII.2.1.] oraz [Sil09, Proposition VII.2.2.].

Zajmiemy się teraz krzywymi o redukcji multyplikatywnej. Przypomnijmy, że dla dowolnej krzywej eliptycznej $E/\mathbb{C}$ istnieje izomorfizm $\mathbb{C}/\Lambda \to E(\mathbb{C})$, gdzie $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$ jest kratą, zaś $Re\,\tau > 0$. Składając go z przekształceniem $z \mapsto \log(z/2\pi i)$ dostajemy izomorfizm $\mathbb{C}^\times/q^{\mathbb{Z}} \cong E(\mathbb{C})$ (gdzie $q = e^{2\pi i \tau}$). Okazuje się, że podobne twierdzenie zachodzi dla krzywych nad ciałami lokalnymi. Wprowadzamy następujące oznaczenia:

$$s_k(q) = \sum_{n \geqslant 1} \frac{n^k q^n}{1 - q^n}, \quad a_4(q) = -5s_3(q), \quad a_6(q) = -\frac{5s_3(q) + 7q_5(q)}{12}$$

Twierdzenie 2.4.3 (Tate, [Sil94, Theorem V.3.1., Remark 3.1.2.])**.**
Niech $q \in K^\times$ spełnia warunek: $v(q) > 0$. Wówczas szeregi $a_4(q), a_6(q)$ są zbieżne, a ponadto krzywa eliptyczna zdefiniowana wzorem:

$$E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q)$$

jest krzywą eliptyczną o wyróżniku $\Delta = q \cdot \prod_{n \geqslant 1}(1 - q^n)^{24}$ oraz j-niezmienniku

$$j(E_q) = \frac{1}{q} + 744 + 196884q + \ldots \in \frac{1}{q}\mathbb{Z}[[q]].$$

*Krzywą w takiej postaci nazywamy **krzywą Tate'a**. Grupa $E_q(\overline{K})$ punktów $\overline{K}$-wymiernych na krzywej Tate'a jest izomorficzna jako* $\mathrm{Gal}(\overline{K}/K)$*-moduł z grupą $\overline{K}^\times/q^{\mathbb{Z}}$, gdzie izomorfizm jest indukowany przez odwzorowanie:*

$$\begin{array}{rcl} \overline{K}^{\times} & \longrightarrow & E_q(\overline{K}) \\ u & \longmapsto & \begin{cases} (X(u,q), Y(u,q)), & dla\ u \notin q^{\mathbb{Z}} \\ 0_{E_q}, & dla\ u \in q^{\mathbb{Z}} \end{cases} \end{array}$$

a szeregi $X(u,q), Y(u,q)$ *zadane są wzorami:*

$$X(u,q) = \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} - 2s_1(q), \quad Y(u,q) = \sum_{n\in\mathbb{Z}} \frac{(q^n u)^2}{(1-q^n u)^3}.$$

Okazuje się, że nie każda krzywa eliptyczna E/K jest $\overline{K}$-izomorficzna z pewną krzywą postaci E_q. Istotnie mamy: $j(E_q) = \frac{1}{q} + \ldots$, zatem j-niezmiennik każdej takiej krzywej musi mieć ujemną waluację. Okazuje się, że twierdzenie odwrotne jest również prawdziwe:

Twierdzenie 2.4.4 (o p-adycznej uniformizacji, [Sil94, Lemma V.5.1.])**.** *Jeżeli* $\alpha \in K$ *spełnia warunek:* $v(\alpha) < 0$*, to istnieje dokładnie jedna liczba* $q \in K$*, taka że* $v(q) > 0$ *oraz* $j(E_q) = \alpha$*.*

Dowód. Niech:

$$f(q) = 1/j(E_q) = q - 744q^2 + 356652q^3 + \ldots \in \mathbb{Z}[[q]].$$

Wtedy, korzystając z algebraicznej wersji twierdzenia o funkcji uwikłanej ([Sil09, Thm IV.2.4]) stwierdzamy, że istnieje szereg potęgowy:

$$g(q) = q + 744q^2 + \ldots \in \mathbb{Z}[[q]] \tag{2.10}$$

spełniający $f(g(q)) = g(f(q)) = q$. Stąd $j(E_q) = \alpha$ wtedy i tylko wtedy, gdy $q = g(1/\alpha)$. Ostatni szereg ten jest zbieżny dla $v(q) < 0$. □

Ostatecznie okazuje się, że krzywe K-izomorficzne z pewną krzywą Tate'a to dokładnie krzywe o multyplikatywnej rozłożonej redukcji. Fakt ten wykorzystamy w dowodzie twierdzenia F.

Twierdzenie 2.4.5. *Niech* E/K *będzie krzywą eliptyczną o redukcji multyplikatywnej i niech* $q \in K^{\times}$ *spełnia:* $j(E_q) = \alpha$*. Wtedy krzywe* E *oraz* E_q *są* $K(\sqrt{\gamma(E/K)})$*-izomorficzne. W szczególności, jeżeli* E/K *ma rozłożoną redukcję multyplikatywną, to* $E \cong E_q$ *nad* K*.*

Dowód. Twierdzenie to wynika z [Sil94, Theorem V.5.3 (b)] oraz z uwagi po dowodzie. □

ROZDZIAŁ 3

WŁASNOŚCI FUNKCJI p - STOPNIA

Ten rozdział stanowi centralną część pracy. Zajmiemy się w nim **p-stopniem** krzywej eliptycznej $E/\mathbb{Q}_p$, zdefiniowanym jako:

$$d_p(E) := \min\{[K : \mathbb{Q}_p] \quad | \quad E(K)[p] \neq 0\}$$

oraz zbiorem jego wartości na krzywych dobrej redukcji:

$$D(p) := \{d_p(E) : E/\mathbb{Q}_p \text{ – krzywa eliptyczna dobrej redukcji w } p\}.$$

Rozdział podzielony jest na trzy części. Pierwsza z nich omawia podstawowe własności p-stopnia, skupiając się na krzywych o niskim stopniu. Druga dotyczy krzywych z mnożeniem zespolonym. W trzeciej części badamy krzywe z redukcją multyplikatywną.

3.1. Podstawowe własności p-stopnia krzywej

W tym podrozdziale przedstawimy podstawowe własności p-stopnia krzywej. Zaczniemy od uogólnienia [DW08, Lemma 3.1]. Otrzymamy w ten sposób wygodne kryterium, pozwalające na stwierdzenie, czy krzywa posiada punkt p-torsyjny nad danym ciałem w zależności od jej redukcji. Dalsza część podrozdziału będzie oparta na tym właśnie twierdzeniu. Zaczniemy od wykazania twierdzenia E ze Wstępu pracy, a następnie podamy charakteryzację krzywych o punkcie p-torsyjnym $P \neq 0_E$ spełniającym: $e(\mathbb{Q}_p(P)/\mathbb{Q}_p) < p - 1$, gdzie przez $e(K/\mathbb{Q}_p)$ oznaczamy stopień rozgałęzienia rozszerzenia. To z kolei umożliwi nam dowód twierdzeń A oraz B ze Wstępu. Będziemy stosowali następujące oznaczenia:

- $K/\mathbb{Q}_p$ – skończone rozszerzenie ciał stopnia n o indeksie rozgałęzienia e,
- R – pierścień liczb całkowitych w K,
- $\mathfrak{m} = (\pi)$ – ideał maksymalny w R, v - waluacja na K,
- $R_i := R/\mathfrak{m}^i$, $\mathfrak{m}_i := \mathfrak{m}/\mathfrak{m}^i$,
- $k = R_1$ – ciało reszt dla R; $d = [k : \mathbb{F}_p]$.

Oprócz tego dla dowolnej grupy abelowej G oznaczymy przez $\operatorname{rank}_p G$ wymiar $G[p] := \{x \in G : p \cdot x = 0\}$ nad $\mathbb{F}_p$. Przez cały czas obowiązuje założenie $p \neq 2, 3$.

Twierdzenie 3.1.1. *Niech $E/\mathbb{Q}_p$ będzie krzywą dobrej redukcji, zaś i będzie najmniejszą liczbą całkowitą większą od $\frac{e}{p-1}$. Wtedy:*

(a) dla $i \leqslant j < i+e$ mamy:

$$\operatorname{rank}_p E_{R_j}(R_j) \geqslant d \cdot (j-i) + \operatorname{rank}_p E(K),$$

(b) dla $j \geqslant i+e$ zachodzi:

$$\operatorname{rank}_p E_{R_j}(R_j) = n + \operatorname{rank}_p E(K).$$

Przed dowodem przedstawimy kilka prostych obliczeń związanych z ideałami w pierścieniach ilorazowych R_j:

Lemat 3.1.2. *Załóżmy, że $i \leqslant j$ są liczbami naturalnymi. Wtedy:*

$$\mathfrak{m}_j^i[p] \cong \begin{cases} (\mathbb{Z}/p)^{d\cdot(j-i)} & dla\ j < i+e \\ (\mathbb{Z}/p)^n & dla\ j \geqslant i+e \end{cases}$$

Dowód. Zauważmy najpierw, że dowolny element $\mathfrak{m}_j^i$ jest postaci:

$$x + \mathfrak{m}^j = a_i\pi^i + a_{i+1}\pi^{i+1} + \ldots + a_{j-1}\pi^{j-1} + \mathfrak{m}^j$$

dla $a_i, a_{i+1}, \ldots \in R$ wyznaczonych jednoznacznie $\pmod{\mathfrak{m}}$.

- niech $j < i+e$. Wtedy dla dowolnego $x + \mathfrak{m}^j \in \mathfrak{m}_j^i[p]$ powyższej postaci mamy:

$$\begin{aligned} x + \mathfrak{m}^j \in \mathfrak{m}_j^i[p] &\Leftrightarrow p \cdot x \in \mathfrak{m}^j \\ &\Leftrightarrow p \cdot \left(a_i\pi^i + a_{i+1}\pi^{i+1} + \ldots + a_{j-1}\pi^{j-1}\right) \in \mathfrak{m}^j \\ &\Leftrightarrow \pi^e \cdot \left(a_i\pi^i + a_{i+1}\pi^{i+1} + \ldots + a_{j-1}\pi^{j-1}\right) \in \mathfrak{m}^j \end{aligned}$$

  zaś z założenia $j < i+e$ wynika, że ostatni warunek jest zawsze spełniony. Stąd $\mathfrak{m}_j^i[p] = \mathfrak{m}_j^i$. Zauważmy, że dowolny element $x + \mathfrak{m}^j \in \mathfrak{m}_j^i$ jest wyznaczony jednoznacznie przez klasy reszt $a_i, \ldots, a_{j-1} \pmod{\mathfrak{m}}$, więc

$$\#\mathfrak{m}_j^i = \#(R/\mathfrak{m})^{j-i} = p^{d\cdot(j-i)}$$

  oraz jako grupy abelowe, $\mathfrak{m}_j^i \cong (\mathbb{Z}/p)^{d\cdot(j-i)}$.

- załóżmy, że $j \geqslant i+e$. Wtedy analogicznie:

$$\begin{aligned} & x + \mathfrak{m}^j \in \mathfrak{m}_j^i[p] \\ \Leftrightarrow \quad & \pi^e \cdot \left(a_i\pi^i + a_{i+1}\pi^{i+1} + \ldots + a_{j-1}\pi^{j-1}\right) \in \mathfrak{m}^j \\ \Leftrightarrow \quad & a_i = a_{i+1} = \ldots = a_{j-e-1} = 0. \end{aligned}$$

  Stąd:

$$\mathfrak{m}_j^i[p] = \{a_{j-e}\pi^{j-e} + \ldots + a_{j-1}\pi^{j-1} + \mathfrak{m}^j : a_i, \ldots, \in R\}$$

  oraz $\#\mathfrak{m}_j^i[p] = \#(R/\mathfrak{m})^e = p^n$, $\mathfrak{m}_j^i[p] \cong (\mathbb{Z}/p)^n$.

□

Lemat 3.1.3. *Dla $j \geqslant i+e$ naturalne odwzorowanie:*

$$\mathfrak{m}^i/\mathfrak{m}^{i+e} \to \mathfrak{m}_j^i/\mathfrak{m}_j^{i+e}$$

jest izomorfizmem.

Dowód. Surjektywność jest natychmiastowa. Jeżeli zaś $x+\mathfrak{m}^j \in \mathfrak{m}_j^{i+e}$, to z warunku $j \geqslant i+e$ dostajemy $x \in \mathfrak{m}^{i+e}$, co dowodzi iniektywności. □

Dowód twierdzenia 3.1.1. Dla wygody będziemy oznaczali: $E'' := E_{R_j}$ oraz $E' := E_{R_i}$. Rozważmy następujący diagram grup, w którym pionowe strzałki oznaczają przekształcenia redukcji:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \widehat{E}(\mathfrak{m}^i) & \longrightarrow & E(K) & \longrightarrow & E'(R_i) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & \widehat{E}''(\mathfrak{m}_j^i) & \longrightarrow & E''(R_j) & \longrightarrow & E'(R_i) & \longrightarrow & 0 \end{array}$$

Wiersze w powyższym diagramie są dokładne na podstawie twierdzeń 2.3.1 oraz 2.3.4. Ponadto z teorii grup formalnych (twierdzenie 2.3.3) odwzorowanie $\widehat{E}(\mathfrak{m}^i) \to \widehat{E}''(\mathfrak{m}_j^i)$ można utożsamić z odwzorowaniem $\mathfrak{m}^i \to \mathfrak{m}_j^i$. Stosując diagram o wężu do poniższego diagramu:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \widehat{E}(\mathfrak{m}^i) & \longrightarrow & E(K) & \longrightarrow & E'(R_i) & \longrightarrow & 0 \\ & & {\scriptstyle [p]}\downarrow & & {\scriptstyle [p]}\downarrow & & {\scriptstyle [p]}\downarrow & & \\ 0 & \longrightarrow & \widehat{E}(\mathfrak{m}^i) & \longrightarrow & E(K) & \longrightarrow & E'(R_i) & \longrightarrow & 0 \end{array}$$

dostajemy ciąg dokładny:

$$0 \to \underbrace{\widehat{E}(\mathfrak{m}^i)[p]}_{=0} \to E(K)[p] \to E'(R_i)[p] \to \operatorname{coker}\left(\widehat{E}(\mathfrak{m}^i) \xrightarrow{[p]} \widehat{E}(\mathfrak{m}^i)\right) \cong \mathfrak{m}^i/p\mathfrak{m}^i \cong \mathfrak{m}^i/\mathfrak{m}^{i+e}.$$

Analogicznie dostajemy ciąg dokładny:

$$0 \to \widehat{E}''(\mathfrak{m}_j^i)[p] \to E''(R_j)[p] \to E'(R_i)[p] \to \operatorname{coker}\left(\widehat{E}''(\mathfrak{m}_j^i) \xrightarrow{[p]} \widehat{E}''(\mathfrak{m}_j^i)\right) \cong \mathfrak{m}_j^i/p\mathfrak{m}_j^i \cong \mathfrak{m}_j^i/\mathfrak{m}_j^{i+e}.$$

To pozwala na stwierdzenie, że w poniższym diagramie przemiennym wiersze są dokładne:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & 0 & \longrightarrow & E(K)[p] & \longrightarrow & E'(R_i)[p] & \longrightarrow & \mathfrak{m}^i/\mathfrak{m}^{i+e} \\ & & \downarrow & & \downarrow & & \| & & \downarrow \\ 0 & \longrightarrow & \mathfrak{m}_j^i[p] & \longrightarrow & E''(R_j)[p] & \longrightarrow & E'(R_i)[p] & \longrightarrow & \mathfrak{m}_j^i/\mathfrak{m}_j^{i+e} \end{array} \tag{3.1}$$

Dolny wiersz indukuje ciąg dokładny:

$$0 \to \mathfrak{m}_j^i[p] \to E''(R_j)[p] \to \ker(E'(R_i)[p] \to \mathfrak{m}_j^i/\mathfrak{m}_j^{i+e}) \to 0 \tag{3.2}$$

Rozważmy teraz dwa przypadki:

- załóżmy, że $i \leqslant j < i + e$ – wtedy z diagramu (3.1):

$$\begin{aligned}\ker(E'(R_i)[p] \to \mathfrak{m}_j^i/\mathfrak{m}_j^{i+e}) &\supset \ker(E'(R_i)[p] \to \mathfrak{m}^i/\mathfrak{m}^{i+e}) \\ &= \operatorname{im}(E(K)[p] \to E'(R_i)[p]) \cong E(K)[p]\end{aligned}$$

  więc z ciągu (3.2) oraz lematu 3.1.2 dostajemy:

$$\begin{aligned}\operatorname{rank}_p E''(R_j) &= \operatorname{rank}_p \mathfrak{m}_j^i[p] + \operatorname{rank}_p \ker(E'(R_i)[p] \to \mathfrak{m}_j^i/\mathfrak{m}_j^{i+e}) \\ &= d \cdot (j-i) + \operatorname{rank}_p \ker(E'(R_i)[p] \to \mathfrak{m}_j^i/\mathfrak{m}_j^{i+e}) \\ &\geqslant d \cdot (j-i) + \operatorname{rank}_p E(K)[p]\end{aligned}$$

  co dowodzi (a).

- niech $j \geqslant i+e$. Korzystając z lematu 3.1.3 oraz z dokładności i przemienności diagramu (3.1):

$$\begin{aligned}\ker(E'(R_i) \to \mathfrak{m}_j^i/\mathfrak{m}_j^{i+e}) &= \ker(E'(R_i) \to \mathfrak{m}^i/\mathfrak{m}^{i+e}) = \\ &= \operatorname{im}(E(K)[p] \to E'(R_i)[p]) \cong E(K)[p].\end{aligned}$$

  Z ciągu (3.2) dostajemy zatem:

$$0 \to \mathfrak{m}_j^i[p] \to E''(R_j)[p] \to E(K)[p] \to 0$$

  co na podstawie lematu 3.1.2 daje: $\operatorname{rank}_p E''(R_j) = n + \operatorname{rank}_p E(K)$.

□

Z twierdzenia 3.1.1 wynika twierdzenie E, zapowiadane we Wstępie do tej pracy:

Wniosek 3.1.4 (Twierdzenie E)**.** *Jeżeli E_1, E_2 są krzywymi dobrej redukcji, których redukcje do $\mathbb{Z}/p^{p^2+p+1}$ są izomorficzne, to $d_p(E_1) = d_p(E_2)$.*

Dowód. Oznaczmy redukcje krzywych E_1, E_2 do $\mathbb{Z}/p^{p^2+p+1}$ odpowiednio przez $\widetilde{E_1}, \widetilde{E_2}$. Niech $P \in E_1[p]$, $P \neq 0_{E_1}$ oraz $K := \mathbb{Q}_p(P)$. Zauważmy, że:

$$e \leqslant [K : \mathbb{Q}_p] \leqslant p^2 - 1.$$

Stąd w twierdzeniu 3.1.1 (b) możemy przyjąć $(i, j) = (p+2, p^2+p+1)$ uzyskując:

$$\begin{aligned}\operatorname{rank}_p E_2[p](K) &= \operatorname{rank}_p \widetilde{E_2}[p](R_{p^2+p+1}) - n = \\ &= \operatorname{rank}_p \widetilde{E_1}[p](R_{p^2+p+1}) - n = \\ &= \operatorname{rank}_p E_1[p](K) = 1,\end{aligned}$$

czyli $E_2[p](K) \cong \mathbb{Z}/p$. Stąd $d_p(E_2) \leqslant d_p(E_1)$; drugą nierówność uzyskujemy analogicznie. □

Przejdziemy teraz do twierdzenia, charakteryzującego krzywe z niezerowym punktem $P \in E(\overline{\mathbb{Q}}_p)[p]$, spełniającym:

$$e(\mathbb{Q}_p(P)/\mathbb{Q}_p) < p - 1.$$

Twierdzenie 3.1.5. *Przy oznaczeniach jak na początku podrozdziału, niech $e < p-1$ oraz niech $E/\mathbb{Q}_p$ będzie krzywą dobrej redukcji. Następujące warunki są równoważne:*

(1) $E(K)[p] \neq 0$,

(2) $\operatorname{rank}_p E_{R_2}(R_2)[p] = d+1$ *oraz* $E_k(k)[p] \neq 0$,

(3) $E_{\mathbb{Z}/p^2}$ *jest kanonicznym podniesieniem* $E_{\mathbb{F}_p}$ *oraz* $E_k(k)[p] \neq 0$,

(4) $E(K \cap \mathbb{Q}_p^{un})[p] \neq 0$.

Dowód.

(1) $\Rightarrow$ (2): załóżmy, że $E(K)[p] \neq 0$. Wtedy z twierdzenia 3.1.1 (a) dla $(i,j) = (1,2)$ mamy:

$$\operatorname{rank}_p E_{R_2}(R_2)[p] \geqslant d+1.$$

Ponadto z wniosku 2.3.5 $E(K)[p] \hookrightarrow E_k(k)[p]$, więc $E_k(k)[p] \neq 0$. Ze stwierdzenia 1.2.1, lematu A.3 oraz dualności Cartier ciąg spójno-étalny dla $E_{R_2}[p]$ musi być postaci:

$$0 \to \mu_p \xrightarrow{i} E_{R_2}[p] \xrightarrow{\pi} \underline{\mathbb{Z}/p} \to 0. \tag{3.3}$$

Przykładając lewodokładny funktor $\operatorname{Hom}_{R_2}(\operatorname{Spec}(R_2), -)$ dostajemy ciąg dokładny grup abelowych:

$$0 \to \mu_p(R_2) \to E_{R_2}[p](R_2) \to \underline{\mathbb{Z}/p}(R_2),$$

z którego wnioskujemy, że:

$$\operatorname{rank}_p E_{R_2}[p](R_2) \leqslant \operatorname{rank}_p \mu_p(R_2) + \operatorname{rank}_p \underline{\mathbb{Z}/p}(R_2).$$

Pozostaje zauważyć, że $\mu_p(R_2) = (\mathbb{Z}/p)^d$, jako że dla $x \in R$ mamy: $x^p \equiv 1 \pmod{\mathfrak{m}^2}$ wtedy i tylko wtedy, gdy $x = 1 + \pi \cdot y$ dla $y \in R$ wyznaczonego jednoznacznie modulo $\mathfrak{m}$. Dlatego też $\operatorname{rank}_p E_{R_2}[p](R_2) \leqslant d+1$, co dowodzi równości.

(2) $\Rightarrow$ (3): Załóżmy teraz, że $\operatorname{rank}_p E[p](R_2) = d+1$ oraz $E_k(k)[p] \neq 0$. Wtedy ciąg spójno-étalny dla $E_{R_2}[p]$ ma postać (3.3). Przykładając do niego lewodokładny funktor $\operatorname{Hom}_{R_2}(\operatorname{Spec}(R_2), -)$ dostajemy:

$$0 \to \mu_p(R_2) \xrightarrow{i} \widetilde{E}[p](R_2) \xrightarrow{\pi} \underline{\mathbb{Z}/p}(R_2).$$

i z porównania rang:

$$E[p](R_2)/i(\mu_p)(R_2) \cong \mathbb{Z}/p.$$

Wybierzmy $g \in E[p](R_2) \setminus i(\mu_p)(R_2)$; wtedy g odpowiada pewnemu morfizmowi $f : \underline{\mathbb{Z}/p} \to E[p]$ (patrz B.11) oraz:

$$\pi \circ f \in \operatorname{End}_{R_2}(\underline{\mathbb{Z}/p}) \cong \operatorname{End}(\mathbb{Z}/p) \cong \mathbb{Z}/p.$$

Ponadto $\pi \circ f \neq 0$ – istotnie, w przeciwnym wypadku:

$$g \in \ker(\widetilde{E}[p](R_2) \xrightarrow{\pi} \underline{\mathbb{Z}/p}(R_2)) = i(\mu_p)(R_2).$$

Stąd $\pi \circ f = [n]$ dla pewnego $n \in \mathbb{Z}/p$, $n \not\equiv 0 \pmod{p}$. Wtedy, jeżeli n^{-1} jest odwrotnością multyplikatywną $n \pmod{p}$, to $[n^{-1}] \circ f : \underline{\mathbb{Z}/p} \to E[p]$ jest cięciem morfizmu π. Istotnie:

$$\pi \circ [n^{-1}] \circ f = [n^{-1}] \circ [n] = id_{\underline{\mathbb{Z}/p}},$$

więc powyższy ciąg dokładny rozszczepia się. Stąd oraz z twierdzenia 2.2.7 stwierdzamy, że E_{R_2} jest kanonicznym podniesieniem E_k, więc $E_{\mathbb{Z}/p^2}$ musi być kanonicznym podniesieniem $E_{\mathbb{F}_p}$.

(3) $\Rightarrow$ (4): bez straty ogólności zastąpimy K przez $K \cap \mathbb{Q}_p^{un}$. Wtedy $e = 1$, a ponadto ciało reszt k pozostaje takie samo. Z (3) dostajemy: $E_{R_2}[p] \cong \mu_p \oplus \underline{\mathbb{Z}/p}$, więc:

$$E_{R_2}[p](R_2) \cong \mu_p(R_2) \oplus \underline{\mathbb{Z}/p}(R_2) \cong (\mathbb{Z}/p)^{d+1}$$

Z lematu 3.1.1 (b) oraz $(i, j) = (1, 2)$ dostajemy:

$$\operatorname{rank}_p E(K)[p] = \operatorname{rank}_p E_{R_2}(R_2)[p] - d \cdot (2 - 1) = 1$$

co kończy dowód.

(4) $\Rightarrow$ (1) : ta część jest oczywista.

□

Z twierdzenia 3.1.5 wyprowadzimy kilka ciekawych wniosków, w tym Twierdzenie A:

Wniosek 3.1.6. *Niech $E/\mathbb{Q}_p$ będzie krzywą dobrej redukcji. Zachodzą następujące implikacje:*

$$d_p(E) < p - 1 \quad \Rightarrow \quad E(\mathbb{Q}_p^{un})[p] \neq 0 \quad \Rightarrow \quad d_p(E) \leqslant p - 1$$

Dowód. Pierwsza implikacja wynika bezpośrednio z twierdzenia 3.1.5 zastosowanego dla $K := \mathbb{Q}_p(P)$, gdzie P spełnia warunek $[\mathbb{Q}_p(P) : \mathbb{Q}_p] < p - 1$. Drugą implikację otrzymujemy z tego samego twierdzenia zastosowanego dla $K := \mathbb{Q}_p(P)$, gdzie $e(\mathbb{Q}_p(P)/\mathbb{Q}_p) = 1$. Z implikacji (1) $\Rightarrow$ (3) twierdzenia 3.1.5 wynika wtedy, że $E_{\mathbb{Z}/p^2}$ jest kanonicznym podniesieniem $E_{\mathbb{F}_p}$. Ze stwierdzenia 1.2.2 wnioskujemy, że $E_{\mathbb{F}_p}$ ma punkt p-torsyjny nad $\mathbb{F}_{p^d}$, gdzie

$$d = \operatorname{ord}_p(a_p(E)) \leqslant p - 1.$$

Korzystając z implikacji (3) $\Rightarrow$ (1) twierdzenia 3.1.5 stwierdzamy, że E ma punkt p-torsyjny nad nierozgałęzionym rozszerzeniem $L/\mathbb{Q}_p$ stopnia $d \leqslant p - 1$. □

Uwaga 3.1.7. *Pierwsza implikacja we wniosku 3.1.6 została udowodniona w pracy [DW08] za pomocą analizy reprezentacji p-adycznej związanej z krzywą, zaś w pracy [Gam14] – za pomocą twierdzenia Raynaud, dotyczącego podnoszenia schematów grupowych nad ciałami do schematów nad pierścieniami. Zwróćmy uwagę, że w dowodzie [DW08, Lemma 4.4] twierdzenie to zostało sformułowane w następujący sposób:*

$$d_p(E) \leqslant p - 1 \quad \Rightarrow \quad E(\mathbb{Q}_p^{un})[p] \neq 0$$

*Implikacja ta **nie jest** prawdziwa. W przypadku, gdy $d_p(E) = p - 1$ może zdarzyć się, że $E(\mathbb{Q}_p^{un})[p] = 0$. Dla przykładu rozważmy krzywą $E := E_{3,3}$ nad $\mathbb{Q}_5$. Jej wielomian podziału Ψ_5 rozkłada się nad $\mathbb{Q}_5$ na czynniki stopni $2, 5, 5$, więc istnieje rozszerzenie $K/\mathbb{Q}_5$ stopnia 4, spełniające warunek: $E(K)[5] \neq 0$. Z drugiej strony czynnik stopnia 2 wielomianu Ψ_5 jest postaci:*

$$x^2 + \left(2 \cdot 5 + 4 \cdot 5^2 + \ldots\right) x + \left(5^{-1} + 2 + 5 + 3 \cdot 5^2 + \ldots\right).$$

Proste przeliczenie pokazuje, że jego pierwiastki są rozgałęzione. Podobne krzywe można znaleźć dla innych liczb pierwszych. Wniosek 3.1.6 jest więc optymalny.

Wniosek 3.1.8 (Twierdzenie A)**.** *Jeżeli krzywa $E/\mathbb{Q}_p$ dobrej redukcji spełnia co najmniej jeden z dwóch podanych niżej warunków:*

- $d_p(E) < p - 1$,

- *$E_{\mathbb{Z}/p^2}$ jest kanonicznym podniesieniem $E_{\mathbb{F}_p}$,*

to:

$$d_p(E) = \operatorname{ord}_p a_p(E).$$

W szczególności:

$$D(p) \cap (0, p) = \{d \in \mathbb{N} : \exists_{|a|<2\sqrt{p}} \quad \operatorname{ord}_p a = d\}.$$

Dowód. Z twierdzenia 3.1.5 wynika, że jeżeli $d_p(E) < p - 1$, to $E_{\mathbb{Z}/p^2}$ jest kanonicznym podniesieniem $E_{\mathbb{F}_p}$ oraz dla dowolnego skończonego rozszerzenia $K/\mathbb{Q}_p$ stopnia mniejszego od $(p-1)$ o ciele reszt k mamy wówczas:

$$E(K)[p] \neq 0 \quad \Leftrightarrow \quad E(k)[p] \neq 0.$$

Pozostaje skorzystać ze stwierdzenia 1.2.2.
Druga część wniosku wynika z twierdzenia 1.2.6. Istotnie, niech $\widetilde{E}/\mathbb{F}_p$ będzie krzywą spełniającą: $\operatorname{ord}_p a_p(E) = d$. Wtedy dowolna krzywa $E/\mathbb{Q}_p$ taka, że $E_{\mathbb{Z}/p^2}$ jest kanonicznym podniesieniem dla $\widetilde{E}$, spełnia $d_p(E) = d$. □

Z powyższego wniosku wynika natychmiastowo wynik, poprawiający w szczególnym przypadku wniosek 3.1.4:

Wniosek 3.1.9. *Niech E_1, E_2 będą krzywymi dobrej redukcji, izomorficznymi nad $\mathbb{Z}/p^2$. Załóżmy, że $d_p(E_1) < p - 1$. Wtedy:*

$$d_p(E_1) = d_p(E_2)$$

Zajmiemy się teraz dowodem twierdzenia B. W tym celu rozważmy zbiór:

$$S := \{(A, B) \in \mathbb{Z}^2 : \Delta(E_{A,B}) \neq 0\}$$

wraz z następującą miarą probabilistyczną:

$$\mu(X) = \lim_{N\to\infty} \frac{|X \cap S_N|}{|S_N|}.$$

gdzie $S_N := S \cap [-N, N]^2$. Łatwo zauważyć, że $|S_N| = 4N^2 \cdot (1 + o(1))$.

Twierdzenie 3.1.10.

$$\mathbb{P}\left(\lim_{p\to\infty} d_p(E_{A,B}) = \infty\right) = 1$$

Przed dowodem wykażemy następujący lemat:

Lemat 3.1.11. *Niech $E_{a,b}/\mathbb{F}_p$ będzie zwyczajną krzywą eliptyczną. Istnieje wtedy dokładnie p różnych par $(A, B) \in \mathbb{Z}/p^2 \times \mathbb{Z}/p^2$ takich, że $(A, B) \equiv (a, b) \pmod p$ oraz krzywa $E_{A,B}$ jest kanonicznym podniesieniem $E_{a,b}$ do $\mathbb{Z}/p^2$.*

Dowód. Załóżmy najpierw, że $j(E_{a,b}) \neq 0, 1728$ (wtedy $a, b \neq 0$) i niech $j_0 \in \mathbb{Z}/p^2$ będzie j-niezmiennikiem kanonicznego podniesienia $E_{a,b}$ do R_2. Niech $(A, B) \equiv (a, b) \pmod p$. Wtedy z twierdzenia 2.2.2 krzywa $E_{A,B}$ jest kanonicznym podniesieniem krzywej $E_{a,b}$ do R_2 wtedy i tylko wtedy, gdy $j(E_{A,B}) = j_0$. Rozważmy wielomian:

$$F(X, Y) = j_0 \cdot (4X^3 + 27Y^2) - 1728 \cdot 4X^3 \in \mathbb{Z}/p^2[X, Y]$$

Niech $A_0, B_0 \in \mathbb{Z}/p^2$ będą dowolnymi podniesieniami $a, b \in \mathbb{Z}/p$; wtedy z założenia $F(A_0, B_0) = p \cdot c$ dla pewnego $c \in \mathbb{Z}/p$. Zastanawiamy się, ile pierwiastków postaci $A = A_0 + p \cdot A'$, $B = B_0 + p \cdot B'$ ma wielomian $F(X, Y)$. Z rozwinięcia w szereg Taylora:

$$\begin{aligned} F(A, B) &= F(A_0, B_0) + \frac{\partial F}{\partial X}(A_0) \cdot (A - A_0) + \frac{\partial F}{\partial Y}(B_0) \cdot (B - B_0) \\ &= p \cdot \Big(c + 12 \cdot (j_0 - 1728) \cdot A_0^2 \cdot A' + 27 \cdot j_0 \cdot 2 \cdot B_0 \cdot B' \Big) \end{aligned}$$

więc $F(A, B) = 0$ wtedy i tylko wtedy, gdy:

$$12 \cdot (j_0 - 1728) \cdot A_0^2 \cdot A' + 27 \cdot j_0 \cdot 2 \cdot B_0 \cdot B' \equiv -c \pmod{p}.$$

Powyższe równanie jest równaniem liniowym o odwracalnym współczynniku przy zmiennej A' lub B', ma więc p rozwiązań (A', B'), co daje tezę.
Załóżmy teraz, że $a = 0$ oraz $3|(p-1)$. Kanoniczne podniesienie krzywej $E_{0,b}$ jest wówczas postaci $E_{0,B}$ (patrz uwaga 2.2.6), gdzie:

$$B \equiv b \pmod{p}$$

jest dowolne (twierdzenie 2.2.3). Analogiczne rozumowanie przeprowadzamy dla $b = 0$. □

Dowód Twierdzenia 3.1.10. Wystarczy udowodnić, że dla dowolnego $d \geqslant 1$ szereg:

$$\sum_p \mathbb{P}\left(d_p(E_{A,B}) = d\right)$$

jest zbieżny. Wtedy z lematu Borela-Cantelliego:

$$\mathbb{P}\Big(d_p(E_{A,B}) = d \text{ dla nieskończenie wielu } p \Big) = 0$$

co dowiedzie tezy. Ustalmy d i wybierzmy liczbę pierwszą $p > d$. Mamy:

$$\mathbb{P}\Big(d_p(E_{A,B}) = d \Big) = \mathbb{P}\Big(d_p(E_{A,B}) = d,\ p \nmid \Delta(E_{A,B}) \Big) + \mathbb{P}\Big(d_p(E_{A,B}) = d,\ p | \Delta(E_{A,B}) \Big)$$

Zajmiemy się najpierw krzywymi dobrej redukcji. Zauważmy, że z twierdzenia 1.2.6:

$$\begin{aligned} &\#\{(a, b) \in \mathbb{F}_p \times \mathbb{F}_p : \Delta(E_{a,b}) \neq 0 \text{ oraz } \operatorname{ord}_p(a_p(E_{a,b})) = d\} = \\ &= \sum_{\operatorname{ord}_p(a) = d} \frac{p-1}{2} H(a) \ll \varphi(d) \cdot \frac{p-1}{2} \sqrt{p} \log^2 p \\ &\ll \varphi(d) p^{3/2} \log^2 p \end{aligned}$$

jako że dla $d|(p-1)$ dokładnie $\varphi(d)$ elementów grupy $(\mathbb{Z}/p)^\times$ ma rząd d.

Stąd oraz z lematu 3.1.11 każda krzywa $E_{A,B}$ dobrej redukcji spełniająca $d_E(p) = d$ należy do jednej z co najwyżej $p \cdot \varphi(d) \cdot p^{3/2} \log^2 p$ klas przystawania modulo p^2. W każdej takiej klasie jest zaś $(\frac{2N}{p^2} + O(1))^2$ krzywych ze zbioru $\{E_{A,B} : (A, B) \in S_N\}$, więc:

$$\begin{aligned} &\mathbb{P}\Big(d_p(E_{A,B}) = d \text{ oraz } p \nmid \Delta(E_{A,B}) \Big) \ll \\ &\ll \lim_{N \to \infty} \frac{1}{\# S_N} \left(\frac{2N}{p^2} + O(1) \right)^2 \cdot \varphi(d) \cdot p^{5/2} \log^2 p = \\ &= \varphi(d) \cdot \frac{4 \log^2 p}{p^{3/2}}. \end{aligned}$$

Zauważmy, że prawdopodobieństwo tego, że wybrana krzywa ma redukcję addytywną w p wynosi $\frac{1}{p^2}$. Dla krzywych redukcji multyplikatywnej oraz $p > d$ możemy mieć $d_p(E_{A,B}) = d$ wtedy i tylko wtedy, gdy $d \in \{1, 2\}$ oraz $j(E_{A,B}) \in \mathbb{Q}_p^p$ (patrz twierdzenia 3.3.2 oraz 3.3.3, które wykażemy niebawem). Stąd:

$$\mathbb{P}\Big(d_p(E_{A,B}) = d,\, p|\Delta(E_{A,B}), p \nmid AB\Big) \leqslant \mathbb{P}\Big(p^p|\Delta(E_{A,B})\Big) \ll \frac{1}{p^2}$$

Pozostaje więc zauważyć, że szereg $\sum_p(\frac{\log^2 p}{p^{3/2}} + \frac{1}{p^2})$ jest zbieżny. □

3.2. Funkcja stopnia dla krzywych z mnożeniem zespolonym

Niech $E/\mathbb{Q}$ będzie krzywą z mnożeniem zespolonym przez $R_K = \mathbb{Z}[\omega_D]$, gdzie $K = \mathbb{Q}(\sqrt{D})$ jest urojonym ciałem kwadratowym. Przypomnijmy, że pierścień R_K musi mieć własność jednoznaczności rozkładu. Jeżeli M będzie ciałem liczbowym, to przez R_M oznaczymy jego pierścień liczb całkowitych. Zauważmy, że z twierdzenia 1.2.3, jeżeli p pozostaje pierwsza w R_K, to E jest supersingularna w p, więc (z twierdzenia 3.1.5) $d_p(E) \geqslant p - 1$. Okazuje się, że p-stopień jest wtedy największy możliwy:

Twierdzenie 3.2.1. *Załóżmy, że p jest liczbą pierwszą, która pozostaje pierwsza w R_K. Wtedy $d_p(E) = p^2 - 1$.*

Dowód. Niech $M = K(E[p])$ – wtedy M/K jest rozszerzeniem abelowym. Oznaczmy $\omega := \omega_D$. Przez $\mathfrak{p}$ będziemy oznaczali ideał pierwszy pierścienia R_K generowany przez p, zaś przez $\mathfrak{b}$ – ustalony ideał pierwszy w R_M nad ideałem $\mathfrak{p}$. Zauważmy, że wówczas: $K_\mathfrak{p} = \mathbb{Q}_p(\omega)$, $M_\mathfrak{b} = \mathbb{Q}_p(\omega, E[p])$.
Niech $f : \mathbb{C}/R_K \to E(\mathbb{C})$ będzie dowolnym analitycznym izomorfizmem – wtedy:

$$E(\overline{K})[p] = f\left(K/R_K[p]\right) = \left\{ f\left(\frac{a + b \cdot \omega_D}{p}\right) : a, b \in \mathbb{Z} \right\}.$$

Oznaczmy przez $P = f(\frac{c}{p}) \in E[p]$ (gdzie $c \in \mathbb{Z}$, $p \nmid c$) dowolny punkt rzędu p. Z elementarnej teorii ciał:

$$\begin{aligned}
[\mathbb{Q}_p(P) : \mathbb{Q}_p] &= \#\{\sigma(P) : \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)\} \\
&\geqslant \#\{\sigma(P) : \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p(\omega))\} \\
&= \#\{\sigma(P) : \sigma \in \mathrm{Gal}(\mathbb{Q}_p(\omega, E[p])/\mathbb{Q}_p(\omega))\}
\end{aligned}$$

Zauważmy, że rozważając zanurzenie $M \hookrightarrow M_\mathfrak{b}$ oraz korzystając z teorii ciał klas:

$$\mathrm{Gal}(M_\mathfrak{b}/K_\mathfrak{p}) = D(\mathfrak{b}/\mathfrak{p}) = \{[i_\mathfrak{p}(x), M/K] : x \in K_\mathfrak{p}^\times\},$$

gdzie $i_\mathfrak{p} : K_\mathfrak{p} \to \mathbb{I}_K$ oznacza kanoniczne zanurzenie (patrz Dodatek C). Jeżeli $a, b \in \mathbb{Z}$ spełniają $(a, b) \not\equiv (0, 0) \pmod p$ to $x := \frac{c}{a+b\omega} \in R_\mathfrak{p}^\times$, więc ze stwierdzenia 1.3.2:

$$P^{[i_\mathfrak{p}(x), M/K]} = f\left(\frac{c}{p}\right)^{[i_\mathfrak{p}(x), M/K]} = f\left(\alpha(x) \cdot i_\mathfrak{p}(x)^{-1} \cdot \frac{1}{p}\right) = f\left(\frac{a + b\omega}{p}\right)$$

co daje nam:

$$[\mathbb{Q}_p(P) : \mathbb{Q}_p] \geqslant \#\{\sigma(P) : \sigma \in \mathrm{Gal}(\mathbb{Q}_p(\omega, E[p])/\mathbb{Q}_p(\omega))\} \geqslant p^2 - 1$$

Z drugiej strony $[\mathbb{Q}_p(P) : \mathbb{Q}_p] \leqslant p^2 - 1$, co dowodzi tezy. □

W szczególności twierdzenie to podaje prosty warunek dostateczny na to, by $p^2-1 \in D(p)$. W tym celu wystarczy sprawdzić, czy:

$$\left(\frac{n}{p}\right) = -1$$

dla pewnego $n \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$. Obliczenia numeryczne pokazują, że warunek ten jest spełniony dla $5 \leqslant p \leqslant 15000$. Najmniejszą liczbą pierwszą, dla której nie jesteśmy w stanie rozstrzygnąć, czy $p^2 - 1 \in D(p)$, jest $p = 15073$.
Zajmiemy się teraz wyznaczeniem wartości $d_p(E)$ w przypadku, gdy $E/\mathbb{Q}$ ma mnożenie zespolone przez $\mathbb{Z}[i]$.

Twierdzenie 3.2.2 (twierdzenie C)**.** *Niech $E : y^2 = x^3 - Dx$, gdzie $D \in \mathbb{Z}$, $D \neq 0$. Wtedy dla $p \nmid D$:*

$$d_p(E) = \begin{cases} \operatorname{ord}_p\left(D^{\frac{p-1}{4}} \cdot 2s\right), & \text{dla } p \equiv 1 \pmod 4, \\ p^2 - 1, & \text{dla } p \equiv 3 \pmod 4 \end{cases}$$

gdzie dla $p \equiv 1 \pmod 4$ liczba s zdefiniowana jest równością $p = s^2 + t^2$ oraz warunkami:

$$2 \nmid s, \quad s + t \equiv 1 \pmod 4.$$

Dowód. Niech $K = \mathbb{Q}(i)$ oraz $M = K(E[p])$. Z założenia $p \nmid D$ wynika, że E ma dobrą redukcję w p. Jeżeli $p \equiv 3 \pmod 4$, to p pozostaje pierwsza w $R_K = \mathbb{Z}[i]$, więc z twierdzenia 3.2.1 mamy $d_p(E) = p^2 - 1$.
Załóżmy teraz, że $p \equiv 1 \pmod 4$; wtedy $p = s^2 + t^2 = \pi_1 \cdot \pi_2$, gdzie $\pi_1 = s + ti$, $\pi_2 = s - ti$ są prymarnymi elementami pierwszymi w pierścieniu R_K. Niech β będzie ustalonym ideałem pierwszym pierścienia R_M, leżącym nad $\mathfrak{p} := (\pi_1)$. Wtedy $K_\mathfrak{p} \cong \mathbb{Q}_p$ (stopień inercji i rozgałęzienia $\mathfrak{p}$ nad p wynosi 1), zaś grupa dekompozycji β nad $\mathfrak{p}$ to:

$$D(\beta/\mathfrak{p}) \cong \operatorname{Gal}(M_\beta/K_\mathfrak{p}) \cong \operatorname{Gal}(M_\beta/\mathbb{Q}_p).$$

Wybierzmy dowolny punkt P rzędu p; wtedy (podobnie jak w poprzednim dowodzie):

$$\begin{aligned} [\mathbb{Q}_p(P) : \mathbb{Q}_p] &= \#\{\sigma(P) : \sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)\} \\ &= \#\{\sigma(P) : \sigma \in \operatorname{Gal}(\mathbb{Q}_p(E[p])/\mathbb{Q}_p)\} \\ &= \#\{\sigma(P) : \sigma \in D(\beta/\mathfrak{p})\} \end{aligned}$$

Ustalmy dowolny analityczny izomorfizm $f : \mathbb{C}/\mathbb{Z}[i] \to E(\mathbb{C})$ i zauważmy, że $E[p] \cong E[\pi_1] \times E[\pi_2]$, więc $P = f(\frac{c}{\pi_1} + \frac{d}{\pi_2})$ dla pewnych $c, d \in \mathbb{Z}$, $(c, d) \not\equiv (0, 0) \pmod p$. Rozważmy następujące przypadki:

- **Przypadek I:** $c \not\equiv 0 \pmod p$

  Niech $x := \frac{c}{a}$, gdzie $p \nmid a$ jest dowolną liczbą całkowitą. Wtedy $x \in R_\mathfrak{p}^\times$, więc $[i_\mathfrak{p}(x), M/K] \in D(\beta/\mathfrak{p})$ oraz $\alpha(i_\mathfrak{p}(x)) = 1$, co daje nam:

  $$P^{[i_\mathfrak{p}(x), M/K]} = f\left(i_\mathfrak{p}(x)^{-1} \cdot \left(\frac{c}{\pi_1} + \frac{d}{\pi_2}\right)\right) = f\left(\frac{a}{\pi_1} + \frac{d}{\pi_2}\right)$$

  więc:

  $$[\mathbb{Q}_p(P) : \mathbb{Q}_p] = \#\{\sigma(P) : \sigma \in D(\beta/\mathfrak{p})\} \geqslant p - 1 \tag{3.4}$$

  Z drugiej strony, jeżeli $p|d$, to $P \in E[\mathfrak{p}]$, zatem $\{\sigma(P) : \sigma \in D(\beta/\mathfrak{p})\} \subset E[\mathfrak{p}] \setminus \{0_E\}$. Ale $\#(E[\mathfrak{p}] \setminus \{0_E\}) = p - 1$, więc w (3.4) mamy równość.

- **Przypadek II:** $c \equiv 0 \pmod{p}$

  W tym przypadku mamy: $P = f\left(\frac{d}{\pi_2}\right)$. Jak łatwo zauważyć, wykonując rachunki analogiczne do powyższych, grupa inercji $I(\beta/\mathfrak{p}) = \{[i_{\mathfrak{p}}(x), M/K] : x \in R_{\mathfrak{p}}^{\times}\}$ działa trywialnie na P. Stąd:

  $$\{\sigma(P) : \sigma \in D(\beta/\mathfrak{p})\} = \{P^{[i_{\mathfrak{p}}(\pi_1^n), M/K]} : n \in \mathbb{Z}\}$$

  Korzystając ze stwierdzenia 1.3.2 otrzymujemy, że $\alpha(i_{\mathfrak{p}}(\pi_1^n)) = \left(\frac{D}{\pi_1}\right)_4^{-n} \cdot \pi_1^n$. Ponadto mnożenie przez idel $i_{\mathfrak{p}}(\pi_1^n)^{-1}$ zmienia tylko składową odpowiadającą $\mathfrak{p}$, i działa trywialnie na $E[\pi_2]$, więc:

  $$P^{[i_{\mathfrak{p}}(\pi_1^n), M/K]} = f\left(\alpha(i_{\mathfrak{p}}(\pi_1^n)) \cdot i_{\mathfrak{p}}(\pi_1^n)^{-1} \cdot \frac{d}{\pi_2}\right) = f\left(\frac{\left(\frac{D}{\pi_2}\right)_4^n \cdot \pi_1^{-n}}{\pi_2}\right),$$

  co daje nam:

  $$\#\{P^{[i_{\mathfrak{p}}(\pi_1^n), M/K]} : n \in \mathbb{Z}\} = \operatorname{ord}_{\pi_2}\left(\left(\frac{D}{\pi_1}\right)_4 \cdot \pi_1^{-1}\right) = \operatorname{ord}_{\pi_2}\left(\left(\frac{D}{\pi_1}\right)_4^{-1} \cdot \pi_1\right),$$

  gdzie $\operatorname{ord}_{\pi_2}$ oznacza rząd w grupie $(R_K/\pi_2)^{\times}$. Pozostaje nam zauważyć, że:

  $$\left(\frac{D}{\pi_1}\right)_4^{-1} \equiv D^{\frac{p-1}{4}} \pmod{\pi_2} \qquad \text{oraz} \qquad \pi_1 \equiv \pi_1 + \pi_2 \equiv 2s \pmod{\pi_2}$$

  więc

  $$\begin{aligned}[\mathbb{Q}_p(P) : \mathbb{Q}_p] &= \operatorname{ord}_{\pi_2}\left(\left(\frac{D}{\pi_1}\right)_4^{-1} \cdot \pi_1\right) = \\ &= \operatorname{ord}_{\pi_2}\left(D^{\frac{p-1}{4}} \cdot 2s\right) = \\ &= \operatorname{ord}_p(D^{\frac{p-1}{4}} \cdot 2s)\end{aligned}$$

□

Zauważmy, że dla $p \equiv 1 \pmod{4}$ redukcja krzywej z twierdzenia 3.2.2 jest zwyczajna, więc korzystając z uwagi 2.2.6, moglibyśmy również użyć wniosku 3.1.8 oraz znanych wzorów na ślad Frobeniusa krzywej $E_{0,-D}$ (patrz np. [IR90, Theorem 18.5]). W podobny sposób można uzyskać wzór na p-stopień krzywych z mnożeniem przez $\mathbb{Z}[\omega]$. Zobaczmy, jak często funkcja p-stopnia krzywej $E_{-D,0}$ może przyjmować małe wartości:

Twierdzenie 3.2.3. *Niech $E/\mathbb{Q} : y^2 = x^3 - Dx$, gdzie $D \in \mathbb{Z}$, $D \neq 0$, zaś $p \equiv 1 \pmod{4}$ będzie liczbą pierwszą nie dzielącą D.*

(a) Jeżeli $d_p(E) \in \{1, 2, 4\}$, to $p = 5$.

(b) $d_p(E) = 8$ wtedy i tylko wtedy, gdy p jest postaci $s_{k+1}^2 + s_k^2$, gdzie:

$$s_0 = 0, \quad s_1 = 1, \quad s_{k+2} = 4s_{k+1} - s_k.$$

Dowód.

(a) załóżmy, że $d_p(E) \in \{1, 2, 4\}$ – wtedy zgodnie z twierdzeniem 3.2.2 również $\mathrm{ord}_p(2s) \in \{1, 2, 4\}$, jako że $(D^{\frac{p-1}{4}})^4 \equiv 1 \pmod p$. Rozważmy kolejno przypadki:

- $\mathrm{ord}_p(2s) = 1$ – oznacza to, że $2s \equiv 1 \pmod p$, więc $s = \frac{p+1}{2}$. To jednak nie jest możliwe, jako że $s^2 = (\frac{p+1}{2})^2 > p$.
- $\mathrm{ord}_p(2s) = 2$ – oznacza to, że $2s \equiv -1 \pmod p$, więc $s = \frac{p-1}{2}$. Nierówność $p > \left(\frac{p-1}{2}\right)^2$ zachodzi jednak tylko dla $p = 5$.
- $\mathrm{ord}_p(2s) = 4$ – oznacza to, że $(2s)^2 \equiv -1 \pmod p$, czyli:
$$(2t)^2 \equiv -4s^2 \equiv 1 \pmod p \quad \Rightarrow \quad 2t \equiv \pm 1 \pmod p$$
i podobnie jak w poprzednich podpunktach uzyskujemy sprzeczność dla $p > 5$.

(b) zgodnie z twierdzeniem 3.2.2 mamy: $d_p(E) = 8$ wtedy i tylko wtedy, gdy $(2s)^4 \equiv -1 \pmod p$. Wykażemy najpierw, że jest to możliwe wtedy i tylko wtedy, gdy $p = 4st + 1$. Istotnie, zauważmy, że:
$$(2s)^4 \equiv (2s)^2 \cdot 4s^2 \equiv (2s)^2 \cdot (-4t^2) \equiv -(4st)^2 \pmod p. \tag{3.5}$$
Stąd, jeżeli p jest tej postaci, to $(2s)^4 \equiv -1 \pmod p$.
Na odwrót, załóżmy, że $(2s)^4 \equiv -1 \pmod p$. Wtedy z (3.5) dostajemy:
$$4st \equiv \pm 1 \pmod p.$$
Z drugiej strony mamy:
$$0 < 4st \pm 1 < 4st + 2(s - t)^2 = 2p$$
więc $p = 4st \pm 1$. Z założenia mamy jednak $p \equiv 1 \pmod 4$, więc $p = 4st + 1$.
Rozważmy równanie $s^2 + t^2 = 4st + 1$. Podstawienie $x := s - 2t$, $y := t$ sprowadza je do równania w postaci Pella:
$$x^2 - 3y^2 = 1$$
Jego rozwiązanie fundamentalne to $(x_0, y_0) := (2, 1)$. Z teorii równań Pella wynika, że pozostałe rozwiązania dane są rekurencją:
$$x_{n+1} + \sqrt{3}y_{n+1} = (2 + \sqrt{3}) \cdot (x_n + \sqrt{3}y_n)$$
bądź też równoważnie:
$$\begin{cases} x_{n+1} &= 2x_n + 3y_n \\ y_{n+1} &= x_n + 2y_n \end{cases}.$$
Podstawiając w powyższej rekurencji $x_n = s_{n+1} - 2t_{n+1}$ oraz $y_n = t_{n+1}$ dostajemy równości $t_{n+1} = s_n$ oraz $s_{n+1} = 2s_n + 3s_{n-1}$. Stąd $p = 4st + 1$ wtedy i tylko wtedy, gdy $s = s_n$, $t = s_{n-1}$ dla pewnego n, co kończy dowód.

□

Obliczenia numeryczne pokazują, że elementy ciągu $(s_{k+1}^2 + s_k^2)_{k=1}^{\infty}$ przy $1 \leqslant k \leqslant 100000$ są pierwsze dla:

$$k \in \{1, 2, 3, 4, 5, 131, 200, 296, 350, 519, 704, 950, 5598, 6683, 7445, 8775, 8786, 11565, 12483\}.$$

Rozstrzygnięcie, czy ciąg liczb naturalnych zadany rekurencją zawiera nieskończenie wiele liczb pierwszych, jest w ogólności bardzo trudnym problemem. Wciąż nie jest to rozstrzygnięte na przykład dla ciągu Fibbonacciego. Okazuje się, że dla $p = s^2 + t^2$ resztę $2s \pmod p$ można podać jawnie jako $(\frac{p-1}{4})!$. Twierdzenie o tej treści pochodzi od Gaussa. Dowód tego faktu oraz dalsze rozważania dotyczące obliczania $\mathrm{ord}_p(2s)$ można znaleźć w pracy [CD14].

3.3. Funkcja stopnia dla krzywych z redukcją multyplikatywną

W tym podrozdziale zajmiemy się zbadaniem wartości $d_E(p)$ w przypadku, gdy $E/\mathbb{Q}_p$ ma redukcję multyplikatywną. Do wyznaczenia wartości funkcji stopnia w przypadku redukcji multyplikatywnej wykorzystamy krzywą Tate'a. Okaże się, że odpowiedź będzie zależała od tego, czy redukcja jest rozłożona oraz od tego, czy j-niezmiennik krzywej jest p-tą potęgą w ciele $\mathbb{Q}_p$. Poniższy lemat pozwala na sprawdzenie tego w praktyce, a a także znajduje zastosowanie w dowodzie twierdzenia 3.3.2.

Lemat 3.3.1. *Niech $p \neq 2$ będzie liczbą pierwszą. Liczba $a \in \mathbb{Q}_p$ jest p-tą potęgą innego elementu $\mathbb{Q}_p$ wtedy i tylko wtedy, gdy $a = p^{pb} \cdot c$, gdzie $b \in \mathbb{Z}$, $c \in \mathbb{Z}_p^\times$ oraz $c^{p-1} \equiv 1 \pmod{p^2}$.*

Dowód. ($\Rightarrow$) Jeżeli a jest p-tą potęgą pewnego elementu z $\mathbb{Q}_p$, to jego waluacja musi być podzielna przez p, więc $a = p^{pb} \cdot c$ dla pewnego $c \in \mathbb{Z}_p^\times$, które również jest p-tą potęgą: $c = C^p$ dla pewnego $C \in \mathbb{Z}_p^\times$. Zauważmy, że $C^p \equiv C \pmod{p}$, więc $C^p = C + p \cdot D$ dla pewnego $D \in \mathbb{Z}_p$. Stąd:

$$c^p = C^{p^2} = C^{\varphi(p^2)} \cdot C^p \equiv 1 \cdot C^p \equiv c \pmod{p^2}$$

($\Leftarrow$) Wykażemy najpierw, że jeżeli $\alpha \equiv 1 \pmod{p^2}$, to α jest p-tą potęgą. Niech $\alpha = 1 + p^2 \cdot \beta$, gdzie $\beta \in \mathbb{Z}_p$. Wtedy:

$$(1 + p \cdot \beta)^p = 1 + \binom{p}{1} p \cdot \beta + \binom{p}{2} (p \cdot \beta)^2 + \ldots \equiv 1 + p^2 \cdot \beta \equiv \alpha \pmod{p^3}$$

więc wielomian $f(x) = x^p - \alpha$ ma „przybliżony" pierwiastek $x_0 := 1 + p \cdot \beta$ spełniający $v(f(x_0)) = 3 > 2v(f'(x_0))$, a zatem z lematu Hensela ma również pierwiastek w $\mathbb{Z}/p$.

Załóżmy teraz, że a jest takiej postaci jak w tezie. Z założenia $c^{1-p} \equiv 1 \pmod{p^2}$, więc z powyższego spostrzeżenia c^{1-p} jest p-tą potęgą. Stąd również

$$a = p^{pb} \cdot c^p \cdot c^{1-p}$$

jest p-tą potęgą. □

Przejdziemy teraz do przypadku redukcji multyplikatywnej rozłożonej. W tym przypadku krzywa jest $\mathbb{Q}_p$-izomorficzna z pewną krzywą Tate'a, więc badanie jej punktów torsyjnych sprowadza się do badania torsji na torusie $\overline{\mathbb{Q}}_p^\times / q^{\mathbb{Z}}$.

Twierdzenie 3.3.2. *Jeżeli krzywa $E/\mathbb{Q}_p$ ma rozłożoną redukcję multyplikatywną, to:*

$$d_E(p) = \begin{cases} 1, & \text{jeżeli } j(E) \in \mathbb{Q}_p^p \\ p-1, & \text{w przeciwnym wypadku.} \end{cases}$$

Dowód. Oznaczmy: $x = 1/j(E) \in p\mathbb{Z}_p$. Zauważmy, że na podstawie twierdzeń 2.4.4 oraz 2.4.5 krzywa E jest $\mathbb{Q}_p$-izomorficzna z krzywą Tate'a E_q, gdzie $q = g(x)$, zaś g jest szeregiem potęgowym, danym wzorem (2.10). Mamy zatem następujący izomorfizm $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-modułów:

$$E[p] \cong \langle q^{1/p} \rangle \oplus \langle \zeta_p \rangle,$$

więc $E(\mathbb{Q}_p)[p] \neq 0$ wtedy i tylko wtedy, gdy $q \in \mathbb{Q}_p^p$.

Zauważmy, że $v(q) = v(x)$, więc jeżeli $p \nmid v(x)$, to $q \notin \mathbb{Q}_p^p$. Załóżmy, że $p | v(x)$. Mamy:

$$\frac{1}{x} g(x) = 1 + 744x + \ldots \equiv 1 \pmod{p^2}$$

więc na mocy stwierdzenia 3.3.1: $\frac{1}{x}g(x) \in \mathbb{Q}_p^p$. Stąd:

$$q \in \mathbb{Q}_p^p \quad \Leftrightarrow \quad x \in \mathbb{Q}_p^p \quad \Leftrightarrow \quad j(E) \in \mathbb{Q}_p^p.$$

Jeżeli $q \notin \mathbb{Q}_p^p$, to:

$$[\mathbb{Q}_p(\zeta_p^i \cdot q^{j/p}) : \mathbb{Q}_p] = \begin{cases} p, & p \nmid j \\ p-1, & p|j \text{ oraz } p \nmid i \end{cases},$$

więc $d_p(E) = p - 1$. □

Twierdzenie 3.3.3. *Jeżeli krzywa $E/\mathbb{Q}_p$ ma nierozłożoną redukcję multyplikatywną, to:*

$$d_E(p) = \begin{cases} 2, & \text{jeżeli } j(E) \in \mathbb{Q}_p^p \\ p-1, & \text{w przeciwnym wypadku.} \end{cases}$$

Dowód. Zgodnie z twierdzeniem 2.4.5 krzywa $E/\mathbb{Q}_p$ jest izomorficzna z krzywą Tate'a nad kwadratowym i nierozgałęzionym rozszerzeniem $\mathbb{Q}_p$:

$$L = \mathbb{Q}_p(\sqrt{\gamma}), \quad \text{gdzie } \gamma := \gamma(E/\mathbb{Q}_p).$$

Istnieje zatem izomorfizm $\mathrm{Gal}(\overline{\mathbb{Q}}_p/L)$-modułów $\Psi : \overline{\mathbb{Q}}_p^{\times}/q^{\mathbb{Z}} \to E(\overline{\mathbb{Q}}_p)$, spełniający:

$$\forall_{\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)} \qquad \sigma \circ \Psi = \chi(\sigma) \cdot \Psi \circ \sigma,$$

gdzie $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)/\mathrm{Gal}(\overline{\mathbb{Q}}_p/L) \cong \{-1, 1\}$ jest charakterem kwadratowym. Dowolny punkt p-torsyjny P jest wtedy postaci $\Psi(z)$ dla pewnego $z \in \overline{\mathbb{Q}}_p$ spełniającego:

$$z^p = q^j, \quad \text{gdzie} \quad j \in \{0, \ldots, p-1\}.$$

Oznaczmy $K := \mathbb{Q}_p(P)$ i zauważmy, że dla dowolnego $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ mamy:

$$\begin{aligned}
& \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/K) && \Leftrightarrow \\
\Leftrightarrow \quad & \sigma(\Psi(z)) = \Psi(z) && \Leftrightarrow \\
\Leftrightarrow \quad & \Psi(\sigma(z)) = \chi(\sigma) \cdot \Psi(z) && \Leftrightarrow \\
\Leftrightarrow \quad & \begin{cases} \sigma(z) \equiv z \pmod{q^{\mathbb{Z}}} \\ \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/L) \end{cases} && \text{lub} \quad \begin{cases} \sigma(z) \equiv z^{-1} \pmod{q^{\mathbb{Z}}}, \\ \sigma \notin \mathrm{Gal}(\overline{\mathbb{Q}}_p/L) \end{cases} \\
\Leftrightarrow \quad & \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/L) \cap \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p(z)) && \text{lub} \quad \begin{cases} \sigma(z) \equiv z^{-1} \pmod{q^{\mathbb{Z}}} \\ \sigma \notin \mathrm{Gal}(\overline{\mathbb{Q}}_p/L) \end{cases} \\
\Leftrightarrow \quad & \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/L(z)) && \text{lub} \quad \begin{cases} \sigma(z) \equiv z^{-1} \pmod{q^{\mathbb{Z}}} \\ \sigma \notin \mathrm{Gal}(\overline{\mathbb{Q}}_p/L) \end{cases}
\end{aligned} \tag{3.6}$$

Załóżmy najpierw, że $j \neq 0$, pokażemy, że nie może zajść drugi warunek z (3.6). Istotnie, jeżeli mielibyśmy $\sigma(z) = q^k \cdot z^{-1}$ dla pewnego k, to podnosząc równanie stronami do potęgi p uzyskalibyśmy $q^j = q^{kp-j}$, co dałoby $p|2j$, więc $p|j$ oraz $j = 0$, sprzeczność. Stąd dla $j \neq 0$ mamy:

$$\mathrm{Gal}(\overline{\mathbb{Q}}_p/K) = \mathrm{Gal}(\overline{\mathbb{Q}}_p/L(z)),$$

czyli $K = L(z)$. Pozostaje zauważyć, że $L \cap \mathbb{Q}_p(z) = \mathbb{Q}_p$, jako że $\mathbb{Q}_p(z)$ jest całkowicie rozgałęzione, zaś L jest nierozgałęzione. W tym przypadku dostajemy więc:

$$[\mathbb{Q}_p(P) : \mathbb{Q}_p] = 2 \cdot [\mathbb{Q}_p(z) : \mathbb{Q}_p] \in \{2, 2p\},$$

w zależności od tego, czy $z \in \mathbb{Q}_p$. Z twierdzenia 3.3.2 warunek $z \in \mathbb{Q}_p$ może zajść wtedy i tylko wtedy, gdy $j(E) \in \mathbb{Q}_p^p$.

Niech teraz $j = 0$; bez straty ogólności możemy założyć, że $z = \zeta_p$. Oznaczmy:

$$F := \mathbb{Q}_p(\zeta_p + \zeta_p^{-1}).$$

Wtedy $\mathbb{Q}_p(\zeta_p)$ jest kwadratowym rozszerzeniem F, zaś $L(\zeta_p)$ dwukwadratowym. Istotnie:

$$\begin{aligned}
\mathbb{Q}_p(\zeta_p) &= F\left(\zeta_p - \zeta_p^{-1}\right) = F\left(\sqrt{(\zeta_p - \zeta_p^{-1})^2}\right) = \\
&= F\left(\sqrt{(\zeta_p + \zeta_p^{-1})^2 - 4}\right) \\
L(\zeta_p) &= F\left(\sqrt{(\zeta_p + \zeta_p^{-1})^2 - 4}, \sqrt{\gamma}\right).
\end{aligned}$$

Z (3.6) stwierdzamy, że $\mathrm{Gal}(\overline{\mathbb{Q}}_p/L(\zeta_p)) \subset \mathrm{Gal}(\overline{\mathbb{Q}}_p/G_K) \subset \mathrm{Gal}(\overline{\mathbb{Q}}_p/F)$. Stąd $F \subset K \subset L(\zeta_p) = \mathbb{Q}_p(\sqrt{\gamma}, \zeta_p))$ oraz K odpowiada podgrupie

$$\{1, \sigma_0\} \subset \mathrm{Gal}(\mathbb{Q}_p(\sqrt{\gamma}, \zeta_p)/F) = \mathrm{Gal}(F(\zeta_p - \zeta_p^{-1}, \sqrt{\gamma})/F),$$

gdzie $\sigma_0(\zeta_p) = \zeta_p^{-1}$ oraz $\sigma_0(\sqrt{\gamma}) = -\sqrt{\gamma}$. Stąd $K = \mathbb{Q}_p(\sqrt{\gamma} \cdot (\zeta_p - \zeta_p^{-1}))$ oraz $[K : \mathbb{Q}_p] = \frac{1}{2}[L(\zeta_p) : \mathbb{Q}_p] = p - 1$. Stąd dostajemy tezę. □

DODATEK A

UZUPEŁNIENIA Z GEOMETRII ALGEBRAICZNEJ

W tym rozdziale podajemy twierdzenia z geometrii algebraicznej, używane w tej pracy. Zaczniemy od lematu pozwalającego na zdefiniowanie rangi skończonego i płaskiego schematu nad ustalonym schematem bazowym.

Lemat A.1. *Niech S będzie lokalnie noetherowskim schematem. S-schemat X jest skończony i płaski nad S wtedy i tylko wtedy, gdy $\mathcal{O}_X$ jest lokalnie wolny nad $\mathcal{O}_S$, czyli gdy istnieje takie pokrycie S zbiorami afinicznymi otwartymi U, że $X|_U \to U$ jest postaci* $\operatorname{Spec}(A) \to \operatorname{Spec}(R)$*, gdzie A jest wolnym R-modułem skończonej rangi. Ranga ta jest lokalnie stałą funkcją na X; oznaczamy ją przez $\#X$ oraz nazywamy* ***rangą*** *X* ***nad*** *S.*

Dowód. Patrz [Sta16, Tag 02K9]. □

Kolejne dwa lematy pozwalają na opis skończonych étalnych nakryć ustalonego schematu w szczególnych przypadkach. Są one wnioskiem z głębszego twierdzenia Grothendiecka, stwierdzającego równoważność skończonych nakryć étalnych schematu S z kategorią zbiorów z działaniem grupy podstawowej $\pi_1(S)$:

Lemat A.2 ([Mil80, Example I.5.2 (a)])**.** *Niech k będzie ciałem. Funktor:*

$$\{\textit{skończone étalne schematy nad } k\} \to \{\textit{skończone zbiory z ciągłym działaniem } \operatorname{Gal}(k^{sep}/k)\}$$

$$X \mapsto X(\overline{k})$$

jest równoważnością kategorii.

Lemat A.3 ([Mil80, Proposition I.4.4])**.** *Jeżeli R jest henselowskim pierścieniem o ciele reszt k, to funktor $G \mapsto G_k$ indukuje równoważność kategorii skończonych étalnych nakryć schematu* $\operatorname{Spec} R$ *oraz skończonych étalnych nakryć* $\operatorname{Spec} k$*. W szczególności kategoria skończonych étalnych schematów nad R jest równoważna z kategorią skończonych zbiorów z ciągłym działaniem grupy* $\operatorname{Gal}(k^{sep}/k)$*.*

Na koniec podamy interpretację punktów R-wymiernych schematów

$$\mathbb{A}^n_R := \operatorname{Spec}(R[x_1, \ldots, x_n]) \quad \text{oraz} \quad \mathbb{P}^n_R := \operatorname{Proj}(R[x_0, \ldots, x_n]).$$

Porównamy je ze zbiorami, znanymi z „klasycznej" geometrii algebraicznej. Niech:

$$\mathbb{A}^n(R) = R^n$$

$$\mathbb{P}^n(R) = \{(a_0, \ldots, a_n) \in R^{n+1} : (a_0, \ldots, a_n) = R\} \Big/ \sim$$

gdzie $(a_i)_i \sim (b_i)_i$ wtedy i tylko wtedy, gdy istnieje $u \in R^\times$ takie, że $ua_i = b_i$ dla każdego i. Klasę równoważności punktu $(a_0, \ldots, a_n)$ oznaczamy przez $[a_0 : \ldots : a_n]$.

Twierdzenie A.4.

(a) Istnieje bijekcja między zbiorem punktów R-wymiernych schematu $\mathbb{A}^n_R$ ze zbiorem $\mathbb{A}^n(R)$.

(b) Każdemu elementowi zbioru $\mathbb{P}^n(R)$ odpowiada pewien punkt R-wymierny na $\mathbb{P}^n_R$. Jeżeli pierścień R jest lokalny, to przyporządkowanie to jest bijekcją.

Aby udowodnić powyższe twierdzenie, będziemy potrzebowali następującego faktu:

Twierdzenie A.5 ([Har77, Theorem II.7.1, str. 150])**.**
Jeżeli $\varphi : X \to \mathbb{P}^n_R$ jest R-morfizmem, to snop $\varphi^*(\mathcal{O}_{\mathbb{P}^n_R}(1))$ jest odwracalny na X oraz generowany przez $n+1$ cięć globalnych: $s_i := \varphi^*(x_i)$. Na odwrót, dla dowolnego snopa odwracalnego $\mathcal{L}$ na X generowanego przez cięcia globalne $s_0, \ldots, s_n$ istnieje jednoznacznie określony R-morfizm $\varphi : X \to \mathbb{P}^n_R$ taki, że $\mathcal{L} = \varphi(\mathcal{O}_{\mathbb{P}^n_R}(1))$ oraz $\varphi^*(x_i) = s_i$.

Dowód twierdzenia A.4.

(a) Każdy element $(a_1, \ldots, a_n) \in \mathbb{A}^n(R)$ określa punkt wymierny

$$\varphi^* : \mathrm{Spec}(R) \to \mathrm{Spec}(R[x_1, \ldots, x_n]),$$

indukowany przez homomorfizm pierścieni $\varphi : R[x_1, \ldots, x_n] \to R$, $\varphi(x_i) = a_i$. Na odwrót, jeżeli $\varphi^* : \mathrm{Spec}(R) \to \mathrm{Spec}(R[x_1, \ldots, x_n])$ jest punktem R-wymiernym, to element $(a_0, \ldots, a_n) \in \mathbb{A}^n(R)$ możemy określić wzorami: $a_i := \varphi(x_i)$.

(b) Niech $P{=}[a_0 : \ldots : a_n] \in \mathbb{P}^n(R)$. Wtedy $a_0, \ldots, a_n \in R = \mathcal{O}_{\mathrm{Spec}(R)}(\mathrm{Spec}(R))$ są cięciami globalnym, generującymi snop odwracalny $\mathcal{O}_{\mathrm{Spec}\ R}$, więc z powyższego twierdzenia odpowiadają pewnemu R-wymiernemu punktowi $\varphi : \mathrm{Spec}(R) \to \mathbb{P}^n_R$. Załóżmy teraz, że R jest pierścieniem lokalnym, zaś $\varphi : \mathrm{Spec}(R) \to \mathbb{P}^n_R$ jest pewnym punktem R-wymiernym. Wtedy $\mathcal{L} := \varphi^*(\mathcal{O}_{\mathbb{P}^n_R}(1))$ jest odwracalnym snopem na $\mathrm{Spec}(R)$, generowanym przez cięcia $s_i := \varphi^*(x_i)$ $(i = 0, \ldots, n)$ – musi on być więc postaci $\widetilde{M}$ dla pewnego projektywnego R-modułu M rangi 1. Ale nad pierścieniami lokalnymi każdy moduł projektywny jest wolny – stąd $M \cong R$. W ten sposób stwierdzamy, że φ odpowiada pewnym cięciom globalnym: $a_0, \ldots, a_n$, generującym snop $\mathcal{O}_{\mathrm{Spec}(R)}$. Są one określone jednoznacznie z dokładnością do elementu $R^\times$. Stąd φ odpowiada jednoznacznie pewnemu punktowi $[a_0 : \ldots : a_n] \in \mathbb{P}^n(R)$. □

DODATEK B

SCHEMATY GRUPOWE

W tym Dodatku opiszemy w skrócie teorię schematów grupowych, skupiając się przy tym na płaskich skończonych schematach grupowych nad pierścieniami. Główne odniesienie stanowią teksty [Tat97] oraz [Sha86]. Niech $\mathcal{C}$ będzie kategorią mającą obiekt początkowy 1 oraz skończone iloczyny.

Definicja B.1. Mówimy, że obiekt $G \in Obj(\mathcal{C})$ wraz z morfizmami $\mu \in \mathrm{Hom}_{\mathcal{C}}(G \times G, G)$, $\varepsilon \in \mathrm{Hom}_{\mathcal{C}}(1, G)$, $\mathrm{inv} \in \mathrm{Hom}_{\mathcal{C}}(G, G)$ jest **obiektem grupowym** w kategorii $\mathcal{C}$, jeżeli dla każdego $T \in Obj(\mathcal{C})$ zbiór $G(T) := \mathrm{Hom}_{\mathcal{C}}(T, G)$ ma strukturę grupy zadaną przez $\mu, \varepsilon, \mathrm{inv}$.

Okazuje się, że aby nadać obiektowi $G \in Obj(\mathcal{C})$ strukturę obiektu grupowego, wystarczy dla każdego T zadać strukturę grupy na zbiorze $G(T)$ tak, aby działania te zachowywały się funktorialnie, to znaczy tak by dla $f \in \mathrm{Hom}_{\mathcal{C}}(T, T')$ indukowany morfizm $f^* : G(T) \to G(T')$ był homomorfizmem grup. Morfizmy $\mu, \varepsilon, \mathrm{inv}$ możemy odzyskać, rozpatrując działania grupowe na $G(G \times G)$ (patrz [Tat97, str. 124]). Stąd oraz z lematu Yonedy obiekty grupowe są w bijekcji z reprezentowalnymi funktorami działącymi z $\mathcal{C}$ do kategorii grup abelowych.

Definicja B.2. Niech S będzie ustalowym schematem. Przez **S-schemat grupowy** rozumieć będziemy obiekt grupowy w kategorii $\mathbf{Sch}/S$ schematów nad S. Kategorię S-schematów grupowych oznaczać będziemy przez $\mathbf{GS}/S$. Morfizmy w tej kategorii można utożsamiać z transformacjami naturalnymi między odpowiednimi funktorami, bądź też z morfizmami schematów komutującymi z działaniem μ.

Kategoria $\mathbf{GS}/S$ nie jest abelowa, istnieją w niej jednak jądra ([Sha86, str. 35]). Zauważmy też, że jeżeli G jest S-schematem grupowym, zaś T jest S-schematem, to $G_T := G \times_S T$ jest T-schematem grupowym. W dalszym ciągu będziemy zakładali, że $S = \mathrm{Spec}(R)$ jest schematem afinicznym, pochodzącym od pierścienia Noether, mówiąc dla uproszczenia o R-schematach grupowych. Kategorie schematów afinicznych oraz pierścieni przemiennych z jedynką są antyrównoważne. Dlatego każdy afiniczny R-schemat grupowy pochodzi od przemiennej R-algebry Hopfa, tzn. R-algebry wyposażonej w R-liniowe działania komnożenia $\mu : A \to A \otimes_R A$, kojedności $\varepsilon : A \to R$ oraz koodwrotności $\mathrm{inv} : A \to A$, które spełniają odpowiednie aksjomaty.

Przykład B.3. ***Grupą addytywną*** *nad R nazywamy schemat $\mathbb{G}_a = \mathrm{Spec}(R[x])$ wraz z naturalnym działaniem na grupie punktów X-wymiernych:*

$$\mathbb{G}_a(X) = \mathcal{O}_X(X).$$

Struktura algebry Hopfa na $R[x]$ dana jest przez: $\mu(x) = x \otimes 1 + 1 \otimes x$. $\varepsilon(x) = 0$, $\mathrm{inv}(x) = -x$.

Przykład B.4. ***Grupą multyplikatywną*** *nad R nazywamy schemat $\mathbb{G}_m = \mathrm{Spec}(R[x, x^{-1}])$ wraz z naturalnym działaniem na grupie punktów X-wymiernych:*

$$\mathbb{G}_m(X) = \mathcal{O}_X(X)^\times.$$

Struktura algebry Hopfa na $R[x, x^{-1}]$ dana jest przez: $\mu(x) = x \otimes x$. $\varepsilon(x) = 1$, $\mathrm{inv}(x) = x^{-1}$.

Przykład B.5. ***Grupą n-tych pierwiastków z jedności*** *nad R nazywamy schemat $\mu_n = \mathrm{Spec}(R[x]/(x^n - 1))$ wraz z naturalnym działaniem na grupie punktów X-wymiernych:*

$$\mu_n(X) = \{f \in \mathcal{O}_X(X)^\times : f^n = 1\}$$

Struktura algebry Hopfa na $R[x]/(x^n - 1)$ dana jest przez: $\mu(x) = x \otimes x$, $\varepsilon(x) = 1$, $\mathrm{inv}(x) = x^{-1}$.

Przykład B.6. ***Stałym schematem grupowym nad R o włóknie Γ*** *(gdzie Γ jest pewną grupą abelową) nazywamy schemat:*

$$\underline{\Gamma} := \coprod_{g \in \Gamma} A_g, \ \text{gdzie } A_g \cong \mathrm{Spec}(R)$$

wraz z morfizmem $\mu : \underline{\Gamma} \times_R \underline{\Gamma} \to \underline{\Gamma}$ zdefiniowanym tak, aby $\mu|_{A_g \times_R A_h}$ przenosiło identycznościowo $A_g \times_R A_h$ na A_{gh} – mamy bowiem:

$$A_g \times_R A_h = \mathrm{Spec}(R \otimes_R R) \cong \mathrm{Spec}(R) \cong A_{gh}$$

W szczególności dla spójnego R-schematu T mamy: $\underline{\Gamma}(T) = \Gamma$. Schemat grupowy $\underline{\Gamma}$ odpowiada R-algebrze Hopfa:

$$R^\Gamma := \{f : \Gamma \to R |\ f \text{ jest dowolną funkcją}\}$$

o bazie:

$$(e_g)_{g \in \Gamma}, \ \text{gdzie } e_g : \Gamma \to R, \quad e_g(h) = \delta_{gh}$$

(gdzie δ_{gh} jest deltą Kroneckera) wraz z mnożeniem $m : R^\Gamma \otimes_R R^\Gamma \to R^\Gamma$:

$$m(e_g \cdot e_h) = \delta_{gh} g$$

– jedynką mnożenia jest więc wówczas $\sum_{g \in \Gamma} e_g$. Struktura algebry Hopfa zadana jest przez odwzorowania:

$$\varepsilon(e_g) = \delta_{ge}, \qquad \mu(e_g) = \sum_{h_1 + h_2 = g} e_{h_1} \otimes e_{h_2}, \qquad \mathrm{inv}(e_g) = e_{-g}.$$

Przykład B.7. *Niech k będzie ciałem. Zgodnie z lematem A.2 dowolnej grupie skończonej Γ oraz ciągłemu homomorfizmowi grup $\chi : \mathrm{Gal}(k^{sep}/k) \to Aut(\Gamma)$ odpowiada pewien schemat grupowy $\Gamma(\chi)$ étalny nad $\mathrm{Spec}(k)$. W szczególności, dla trywialnego χ dostajemy stały schemat grupowy $\underline{\Gamma}$. Z lematu A.3 wynika, że schemat grupowy $\Gamma(\chi)$ można zdefiniować również nad $\mathrm{Spec}(R)$, w przypadku gdy R jest pierścieniem Hensela o ciele reszt k.*

Przykład B.8. *Podamy teraz przykład morfizmu schematów grupowych. Niech G będzie dowolnym przemiennym schematem grupowym. Niech $[n] : G \to G$ będzie morfizmem określonym na grupie punktów T-wymiernych jako mnożenie przez n (z uwag na początku rozdziału wynika, że jest to poprawne określenie morifzmu). Morfizm ten nazywamy* ***morfizmem mnożenia przez*** *n, zaś jego jądro $G[n]$ – schematem grupowym n-torsji na G.*

Ważną klasę schematów grupowych stanowią te, które są płaskie i skończone nad schematem bazowym. Dzielą one wiele wspólnych własności ze zwykłymi grupami. Wśród podanych przez nas przykładów μ_n, $\underline{\Gamma}$ oraz $\Gamma(\chi)$ są płaskie i skończone, o ile grupa Γ jest skończona.

W szczególności, gdy schemat bazowy jest noetherowski, dla dowolnego skończonego płaskiego schematu grupowego G można zdefiniować jego rząd $\#G$ (patrz A.1). Przykładowo $\#\mu_n = n$ oraz $\#\underline{\Gamma} = \#\Gamma(\chi) = \#\Gamma$. Dla tak zdefiniowanego rzędu zachodzi np. odpowiednik twierdzenia Lagrange'a – jeżeli N jest płaskim schematem podgrupowym G, to schemat ilorazowy G/N istnieje oraz jest płaski i skończony nad S. Ponadto mamy: $\#G = \#N \cdot \#(G/N)$ (patrz [Sha86, str. 38]).

Przypomnijmy, że jeżeli Γ jest grupą topologiczną, zaś składowa spójności elementu neutralnego Γ^0 jest otwarta to grupa składowych Γ/Γ^0 jest dyskretna. Odpowiednik tego faktu zachodzi również dla płaskich, skończonych schematów grupowych.

Twierdzenie B.9 (ciąg spójno-étalny, [Sha86, str. 43])**.** *Niech R będzie zupełnym pierścieniem lokalnym. Niech G będzie skończonym i płaskim R-schematem grupowym, zaś G^0 – składową spójności identyczności w G. Wtedy G^0 jest podgrupą normalną, zaś grupa ilorazowa $G^{et} := G/G^0$ jest étalna. Ciąg dokładny:*

$$0 \to G^0 \to G \to G^{et} \to 0$$

nazywamy ciągiem spójno-étalnym grupy G. Jeżeli ponadto $R = k$ jest ciałem doskonałym, zaś G – schematem przemiennym, to ciąg ten rozszczepia się.

Podamy jeszcze charakteryzację spójnych schematów grupowych w terminach ich punktów geometrycznych:

Stwierdzenie B.10. *Niech k będzie ciałem, zaś G – skończonym k-schematem grupowym. G jest spójne wtedy i tylko wtedy, gdy $G(\overline{k})$ jest grupą trywialną.*

Dowód. Zauważmy, że $G = \mathrm{Spec}(A)$, gdzie A jest skończoną k-algebrą Hopfa. W szczególności A jest pierścieniem Artina ([AM69, zad. 8.3]), można go więc zapisać jako iloczyn pierścieni lokalnych ([AM69, Tw. 8.7]). Schemat G jest spójny wtedy i tylko wtedy, gdy A nie można zapisać jako iloczyn pierścieni. Z powyższych uwag wynika zatem, że G jest spójny wtedy i tylko wtedy, gdy A jest pierścieniem lokalnym, czyli gdy $G(\overline{k})$ jest trywialne. □

W szczególności ze stwierdzenia B.10 widać od razu, że jeżeli $\mathrm{char}\, k = p$, to schemat μ_{p^n} jest spójny dla każdego n.

Ustalmy teraz S-schematy grupowe G, H oraz rozważmy następujący funktor $\underline{\mathrm{Hom}}(G, H)$ w kategorii $\mathbf{Sch}/S$:

$$T \mapsto \mathrm{Hom}_{\mathbf{GS}/T}(G \times_S T, H \times_S T).$$

Przykładowo, jeżeli G będzie dowolnym skończonym schematem grupowym nad $S = \mathrm{Spec}(R)$, zaś $H = \mathbb{G}_m$, to funktor $\underline{\mathrm{Hom}}(G, H)$ jest reprezentowalny przez tzw. **grupę dualną w sensie Cartier do** G, oznaczaną przez $G^\vee$. Pochodzi ona od dualnej algebry Hopfa $A^\vee := \mathrm{Hom}_{R-mod}(A, R)$. Łatwo zauważyć, że $\#(G^\vee) = \#G$ oraz $(G^\vee)^\vee \cong G$.
Przykładowo, grupę dualną do $\underline{\mathbb{Z}/n}$ stanowi μ_n – dowodzi tego następujący (ogólniejszy) fakt, który wykorzystamy również w dowodzie twierdzenia 3.1.5:

Twierdzenie B.11. *Niech G będzie skończonym, płaskim oraz przemiennym R-schematem grupowym. Wtedy $\underline{\mathrm{Hom}}(\underline{\mathbb{Z}/p}, G)$ jest reprezentowalny przez $G[p]$.*

Dowód. Zgodnie z lematem Yonedy wystarczy wykazać, że dla dowolnego $T \in Obj(\mathbf{Sch}/R)$:

$$\mathrm{Hom}_{\mathbf{GS}/T}(\underline{\mathbb{Z}/p} \times_S T, G \times_S T) \cong G[p](T)$$

Po zmianie bazy możemy przyjąć $T = S$. Niech $\underline{\mathbb{Z}/p} = \coprod_{i \in \mathbb{Z}/p} A_i$, gdzie $A_i \cong \mathrm{Spec}(R)$. Zauważmy, że obraz dowolnego morfizmu $\underline{\mathbb{Z}/p} \to G$ jest zawarty w $G[p]$, więc

$$\mathrm{Hom}_{\mathbf{GS}/R}(\underline{\mathbb{Z}/p}, G) = \mathrm{Hom}_{\mathbf{GS}/R}(\underline{\mathbb{Z}/p}, G[p])$$

Dowolnemu homomorfizmowi $f : \underline{\mathbb{Z}/p} \to G[p]$ odpowiada element

$$f|_{A_1} \in G[p](R) := \mathrm{Hom}_{\mathbf{GS}/R}(\mathrm{Spec}(R), G[p]).$$

Na odwrót, mając dane $g \in G[p](R)$ możemy zdefiniować $f : \underline{\mathbb{Z}/p} \to G[p]$ wzorem:

$$f|_{A_i} = [i]_G \circ g.$$

Wtedy f jest morfizmem schematów grupowych, tzn. $\mu_G \circ (f \times f) = f \circ \mu_{\mathbb{Z}/n}$ – istotnie:

$$\begin{aligned} \mu_G \circ (f \times f)|_{A_i \times_R A_j} &= \mu_G \circ ([i]_G \circ g \times [j]_G \circ g) = \\ &= [i+j]_G \circ g = f|_{A_{i+j}} = \\ &= (f \circ \mu_{\mathbb{Z}/p})|_{A_i \times_R A_j}. \end{aligned}$$

Pozostaje zauważyć, że skonstruowane przyporządkowania są wzajemnie odwrotne i funktorialne. □

Niech R będzie dowolnym pierścieniem lokalnym. Zajmiemy się teraz wyznaczeniem wszystkich płaskich, skończonych schematów grupowych, będących rozszerzeniem $\underline{\mathbb{Z}/n}$ o schemat grupowy μ_n, tzn. elementów grupy

$$\mathrm{Ext}^1_{\mathbf{GS}/R}(\underline{\mathbb{Z}/n}, \mu_n).$$

W tym celu będziemy potrzebowali płaskiej kohomologii. Przez płaską topologię rozumiemy topologię Grothendiecka wyznaczoną przez jedną z następujących rodzin odwzorowań:

- wiernie płaskie i quasi-zwarte (fpqc),
- wiernie płaskie i skończonej prezentacji (fppf).

Obie topologie są mocniejsze od topologii étalnej (dowolny morfizm étalny jest fpqc oraz fppf). Mając dany określony situs konstrukcja płaskiej kohomologii przebiega w sposób analogiczny do konstrukcji kohomologii étalnej (patrz np. [Mil80]).
Zauważmy, że dowolny płaski, przemienny R-schemat grupowy można traktować w naturalny sposób jako snop dla płaskiego situsa wraz z topologią fpqc lub fppf (patrz [Mil80, II Corollary 1.7]). Okazuje się, że kohomologia dla takiego snopa nie zależy od tego, czy wybierzemy mały, czy też duży situs, topologię fpqc, czy też fppf ([Mil80, III.3.4]). Wykażemy, że grupę $\mathrm{Ext}^1_{\mathbf{GS}/R}(\underline{\mathbb{Z}/n}, \mu_n)$ można utożsamić z grupą kohomologii $H^1_{fl}(R, \mu_n)$. Istotnie, jak wynika z twierdzenia B.11, δ-funktor $H^\bullet_{fl}(R, \cdot)$ w kategorii n-torsyjnych fppf snopów na $\mathrm{Spec}(R)$ jest funktorem pochodnym funktora

$$\Gamma(R, \cdot) = \mathrm{Hom}_{\mathbf{GS}/R}(\underline{\mathbb{Z}/n}, \cdot) = \mathrm{Hom}_{\mathcal{C}}(\underline{\mathbb{Z}/n}, \cdot)$$

gdzie $\mathcal{C}$ jest kategorią n-torsyjnych fppf snopów nad $\mathrm{Spec}(R)$. Stąd $H^1_{fl}(R,\mu_n) \cong \mathrm{Ext}^1_{\mathcal{C}}(\underline{\mathbb{Z}/n},\mu_n)$. Pozostaje zauważyć, że jeżeli snop $\mathcal{F}$ spełnia ciąg dokładny:

$$0 \to \mu_n \to \mathcal{F} \to \underline{\mathbb{Z}/n} \to 0,$$

to również pochodzi od pewnego skończonego i płaskiego R-schematu grupowego (wynika to z teorii spadku dla odwzorowań afinicznych), tak więc $\mathrm{Ext}^1_{\mathcal{C}}(\underline{\mathbb{Z}/n},\mu_n) = \mathrm{Ext}^1_{\mathbf{GS}/R}(\underline{\mathbb{Z}/n},\mu_n)$. Aby obliczyć $H^1_{fl}(R,\mu_n)$, wykorzystamy ciąg dokładny Kummera dla płaskiej topologii (patrz np. [Mil80, example II.2.18. (b), str. 66]):

$$0 \to \mu_n \to \mathbb{G}_m \xrightarrow{[n]} \mathbb{G}_m \to 0$$

który indukuje długi ciąg kohomologii:

$$0 \to \mu_n(R) \to \mathbb{G}_m(R) \xrightarrow{[n]} \mathbb{G}_m(R) \to H^1_{fl}(R,\mu_n) \to H^1_{fl}(R,\mathbb{G}_m) \to H^1_{fl}(R,\mathbb{G}_m)$$

Zauważając, że $H^1_{fl}(R,\mathbb{G}_m) = Pic(R) = 0$, dostajemy:

$$H^1_{fl}(R,\mu_n) \cong \mathrm{coker}(\mathbb{G}_m(R) \xrightarrow{[n]} \mathbb{G}_m(R)) = R^\times/(R^\times)^n$$

W ten sposób otrzymujemy następujące twierdzenie:

Twierdzenie B.12. *Jeżeli R jest pierścieniem lokalnym, to:*

$$\mathrm{Ext}^1_{\boldsymbol{GS}/R}(\underline{\mathbb{Z}/n},\mu_n) \cong R^\times/(R^\times)^n$$

Szkic tego dowodu można znaleźć również w [CGP15, str. 542].

Zdefiniujemy teraz grupy p-podzielne, zwane także grupami Barsotti'ego - Tate'a. Stanowią one ważny przykład tzw. formalnych schematów grupowych. Definicję można sformułować dla dowolnego pierścienia R, jednak najważniejszy dla nas przypadek stanowią pierścienie lokalne o charakterystyce ciała reszt $p > 0$.

Definicja B.13. **p-podzielną grupą** wysokości h nad R nazwiemy ciąg płaskich, skończonych i przemiennych R-schematów grupowych $(G_n)_n$ takich, że $\#G_n = p^{nh}$, $G_n \subset G_{n+1}$ oraz $G_n = \ker([p^n] : G_{n+1} \to G_{n+1})$. Kategorię grup p-podzielnych nad R oznaczymy przez p-$\mathbf{div}/R$.

Okazuje się, że podstawowe pojęcia oraz twierdzenia teorii płaskich, skończonych schematów grupowych przenoszą się na teorię grup p-podzielnych. Przykładowo grupę p-podzielną $G = (G_n)_n$ będziemy nazywali spójną (étalną), jeżeli dla każdego n schemat grupowy G_n jest spójny (odpowiednio: étalny). Analogicznie zdefiniować można m.in. dualność Cartier oraz ciąg spójno-étalny. W pracy główną rolę odegrają dwie grupy p-podzielne: stała grupa p-podzielna $\underline{\mathbb{Q}_p/\mathbb{Z}_p} := (\underline{\mathbb{Z}/p^n})_n$ oraz grupa pierwiastków z jedności $\mu_{p^\infty} := (\mu_{p^n})_n$.

Grupy p-podzielne pojawiają się w naturalny sposób w teorii schematów abelowych. Przypomnijmy definicję schematu abelowego nad schematem bazowym S:

Definicja B.14. S-schemat grupowy A o właściwym i gładkim morfiźmie strukturalnym $\pi : A \to S$ nazywamy **schematem abelowym nad S relatywnego wymiaru** d, jeżeli dla dowolnego $y \in S$ włókno $A_y := \pi^{-1}(y)$ jest geometrycznie spójne i ma wymiar d.

Zauważmy przy tym, że krzywa eliptyczna jest schematem abelowym relatywnego wymiaru 1. Z dowolnym schematem abelowym A nad $\mathrm{Spec}(R)$ można związać grupę p-podzielną zadaną wzorem: $A[p^\infty] := (A[p^n])_n$. Okazuje się, że w pewnych przypadkach podniesienia schematu abelowego z ciała reszt do pierścienia R są wyznaczone jednoznacznie przez podniesienia jego grupy p-podzielnej.

Twierdzenie B.15 (Serre'a-Tate'a, [Kat81, Theorem 1.2.1])**.**
Niech $\mathcal{R}$ będzie lokalnym pierścieniem Artina o ideale maksymalnym $\mathfrak{m}$ oraz załóżmy, że $k := \mathcal{R}/\mathfrak{m}$ jest ciałem charakterystyki p. Rozważmy kategorię $\mathcal{D}$, której elementami są trójki $(\mathcal{A}, G, \Phi)$, gdzie:

- *$\mathcal{A}$ jest schematem abelowym nad k,*
- *G jest p-podzielną grupą nad $\mathcal{R}$,*
- *$\Phi : \mathcal{A}[p^\infty] \to G_k$ jest izomorfizmem,*

z naturalnie zadanymi morfizmami. Wtedy funktor $A \mapsto (A_k, A[p^\infty], \Phi)$ jest równoważnością kategorii schematów abelowych nad $\mathcal{R}$ oraz kategorii $\mathcal{D}$.

DODATEK C

TEORIA CIAŁ KLAS

W tej części pracy przypomnimy najważniejsze definicje oraz twierdzenia teorii ciał klas. Zaczniemy od sformułowania twierdzenia o wzajemności Artina w przypadku lokalnym. Niech K będzie ciałem lokalnym o pierścieniu liczb całkowitych R_K, ideale maksymalnym $\mathfrak{m}$, waluacji $v_K : K^\times \to \mathbb{Z}$ oraz ciele reszt $\kappa(\mathfrak{m}) := R_K/\mathfrak{m} \cong \mathbb{F}_q$ (gdzie $q = p^n$).

Twierdzenie C.1 (lokalna wzajemność Artina)**.** *Istnieje homomorfizm $\rho_K : K^\times \to \mathrm{Gal}(K^{ab}/K)$ o następujących własnościach:*

(i) jeżeli rozszerzenie L/K jest abelowe i skończone, to

$$\rho_{L/K} := \rho_K|_L : K^\times \to \mathrm{Gal}(L/K)$$

jest surjekcją o jądrze $N_{L/K}L^\times$. W szczególności ρ_K jest ciągłą iniekcją o gęstym obrazie.

(ii) jeżeli rozszerzenie L/K jest abelowe, skończone oraz nierozgałęzione, a ponadto π jest uniformizatorem dla R_L, to $\rho_K(\pi)(x)$ jest automorfizmem Frobeniusa dla L/K.

(iii) $\rho_K|_{R_K^\times}$ indukuje izomorfizm $R_K^\times$ oraz grupy inercji $I_\mathfrak{m}^{ab}$.

Dowód. Konstrukcję odwzorowania Artina znaleźć można np. w [Ser79, XIII §4]. Własności (i), (ii), (iii) wynikają z [Ser79, XIII §4, Proposition 13, str. 197] oraz [Ser79, Corollary, str. 198] □

Przejdziemy teraz do przypadku globalnego. Niech K będzie ciałem liczbowym o pierścieniu liczb całkowitych R_K oraz zbiorze waluacji V. Przez V_0 będziemy oznaczali zbiór niearchimedesowych waluacji (które będziemy utożsamiali z ideałami pierwszymi w R_K), zaś przez V_∞ – zbiór archimedesowych waluacji. Jeżeli $v \in V$, to przez K_v będziemy oznaczali uzupełnienie K względem metryki indukowanej przez v, zaś $R_v := \{x \in K_v : v(x) \geqslant 0\}$. Ponadto dla ideału pierwszego $\mathfrak{p} \in Spec(R_K)$ będziemy oznaczali ciało reszt jako $\kappa(\mathfrak{p}) := R_K/\mathfrak{p}$. Niech L/K będzie abelowym rozszerzeniem o dyferencie $\mathcal{D}_{L/K}$, $\mathfrak{p} \in Spec(R_K)$ – dowolnym nierozgałęzionym ideałem pierwszym oraz $\mathfrak{b}|\mathfrak{p}$. Grupa dekompozycji:

$$D(\mathfrak{b}/\mathfrak{p}) := \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathfrak{b}) = \mathfrak{b}\}$$

nie zależy wówczas od wyboru $\mathfrak{b}$ oraz jest izomorficzna z grupą Galois $\mathrm{Gal}(L_{\mathfrak{b}}/K_{\mathfrak{p}})$.
Dla dowolnego ciała liczbowego K przez $\mathbb{I}_K$ będziemy oznaczali **grupę ideli** ciała K, tzn.

$$\mathbb{I}_K := \{(a_v)_v \in \prod_{v\in V} K_v^\times : \quad v(a_v) = 0 \text{ dla prawie wszystkich } v \in V\}$$

wraz z topologią tzw. produktu ograniczonego. Oznacza to, że bazę zbiorów otwartych tworzą zbiory postaci $\prod_{v\in V} U_v$, gdzie U_v są zbiorami otwartymi w K_v^* oraz $U_v = R_v^*$ dla prawie wszystkich v. Przypomnijmy pokrótce najważniejsze definicje związane z idelami:

- **ideał związany z idelem** $s = (s_v) \in \mathbb{I}_K$ definiujemy wzorem: $(s) := \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(s_{\mathfrak{p}})} \trianglelefteq R_K$,
- zanurzenie $\iota : K^\times \hookrightarrow \mathbb{I}_K$ (diagonalne) oraz $\iota_v : K_v^\times \hookrightarrow \mathbb{I}_K$ (na współrzędną odpowiadającą waluacji v),
- **norma dla ideli** – jeżeli L/K jest skończonym rozszerzeniem ciał, to możemy zdefiniować ciągły homomorfizm $N_{L/K} : \mathbb{I}_L \to \mathbb{I}_K$ wzorem:

$$N_{L/K}((s_w)_w) = (t_v)_v, \qquad t_v := \prod_{w|v} N_{L_w/K_v}(s_w)$$

Niech L/K będzie dowolnym skończonym rozszerzeniem abelowym L/K – definiujemy wtedy tzw. **homomorfizm Artina** wzorem:

$$[\cdot, L/K] : \mathbb{I}_K \to \mathrm{Gal}(L/K), \quad [(s_v)_v, L/K] := \prod_{v\in V} \rho_{L_w/K_v}(s_v)|_L$$

(gdzie w jest dowolną waluacją przedłużającą v). Zauważmy przy tym, że iloczyn ten jest dobrze określony – jeżeli waluacja v nie jest rozgałęziona w L/K oraz $v(s_v) = 0$, to z własności (iii) twierdzenia C.1 dostajemy $\rho_{L_w/K_v}(s_v) = 1$. Z funktorialności możemy stwierdzić, że zdefiniowane w ten sposób homomorfizmy są zgodne, co pozwala na określenie homomorfizmu $[\cdot, K] : \mathbb{I}_K \to \mathrm{Gal}(K^{ab}/K)$ wzorem $[(s_v)_v, K]|_L = [(s_v)_v, L/K]$. Poniższe twierdzenie podaje najważniejsze własności tego homomorfizmu:

Twierdzenie C.2 (globalna wzajemność Artina, [Sil94, Theorem II.3.5.])**.**

(a) ***(twierdzenie o iloczynie)*** $\iota(K^\times) \subset \ker[\cdot, K]$,

(b) $[\cdot, K] : \mathbb{I}_K \to \mathrm{Gal}(K^{ab}/K)$ *jest ciągłym epimorfizmem, zgodnym względem brania rozszerzeń:*

$$[x, L]|_{K^{ab}} = [N_{L/K}x, K]$$

(c) jeżeli L/K jest skończonym i abelowym rozszerzeniem, to

$$[\cdot, L/K] := [\cdot, K]|_L : \mathbb{I}_K \to \mathrm{Gal}(L/K)$$

jest epimorfizmem o jądrze $K^\times N_{L/K}\mathbb{I}_L$.

(d) niech $v \in V_0$. Wtedy:

- *jeżeli $\pi \in K_v^\times$ spełnia warunek $v(\pi) = 1$, to $[\iota_v(\pi), K]$ jest automorfizmem Frobeniusa odpowiadającym v,*
- *jeżeli $\alpha \in R_v^\times$, to element $[\iota_v(\alpha), K]$ należy do grupy inercji I_v^{ab}.*

OZNACZENIA

- schematy:
  - $\mathbf{Sch}/S$ – kategoria schematów nad ustalonym schematem S
  - $\mathcal{O}_X$ – snop strukturalny schematu X
  - $\kappa(y)$ – ciało rezydualne schematu X w punkcie y
  - $\Omega_{X/S}$ – snop form różniczkowych na S-schemacie X
  - $\Gamma(U, \mathcal{F})$ – zbiór cięć snopa $\mathcal{F}$ na zbiorze otwartym U
  - $X_T := X \times_S T$, $X_R := X_{\mathrm{Spec}(R)}$ – zmiana bazy S-schematu X
  - $\#X$ – rząd skończonego i płaskiego S-schematu ..... str. 49
  - $X(R)$ – punkty R-wymierne schematu X.
  - $H^1_{fl}(R, \mathcal{F})$ – płaska kohomologia snopa $\mathcal{F}$ nad $\mathrm{Spec}(R)$ ..... str. 54
  - $\mathbb{A}^n(R) = R^n$ ..... str. 50
  - $\mathbb{P}^n(R) = \{(a_0, \ldots, a_n) \in R^{n+1} : (a_0 \ldots a_n) = R\} \Big/ \sim$ ..... str. 50
- schematy grupowe:
  - $\varepsilon_G, \mu_G, inv_G$ – morfizmy zadające strukturę schematu grupowego ..... str. 51
    (indeks G pomijamy, gdy kontekst jest jasny)
  - $\mathbf{GS}/S$ – kategoria S-schematów grupowych ..... str. 51
  - μ_n – schemat grupowy n-tych pierwiastków z jedności ..... str. 52
  - $\underline{\Gamma}$ – stały schemat grupowy o włóknie Γ ..... str. 52
  - $\Gamma(\chi)$ – étalny schemat grupowy wyznaczony przez
    grupę Γ oraz charakter $\chi : G_k \to Aut(\Gamma)$ ..... str. 52
  - $G[n]$ – podgrupa n-torsji na G ..... str. 52
  - G^0 – składowa spójności elementu neutralnego w G ..... str. 53
  - G^{et} – maksymalny étalny iloraz grupy G ..... str. 53
  - $G^\vee$ – grupa dualna w sensie Cartier do G ..... str. 53
  - $\underline{Hom}(G, H)$ – funktor zadany jako: ..... str. 53

$$T \mapsto \mathrm{Hom}_{\mathbf{GS}/T}(G \times_S T, H \times_S T)$$

- p-**div**$/R$ – kategoria grup p-podzielnych nad R ..... str. 55
- $\underline{\mathbb{Q}_p/\mathbb{Z}_p}$ – grupa p-podzielna zadana jako: $\underline{\mathbb{Q}_p/\mathbb{Z}_p} = (\mathbb{Z}/p^n)_n$ ..... str. 55
- μ_{p^∞} – grupa p-podzielna zadana jako: $\mu_{p^\infty} = (\mu_{p^n})_n$ ..... str. 55

- pierścienie zupełne, ciała lokalne:
  - R – zazwyczaj: pierścień dyskretnej waluacji v o ideale maksymalnym $\mathfrak{m}$, uniformizatorze π, ciele ułamków K oraz ciele reszt $k := R/\mathfrak{m}$ ..... str. 22
  - $R_i := R/\mathfrak{m}^i$ – pierścień lokalny o ideale maksymalnym $\mathfrak{m}_i := \mathfrak{m}/\mathfrak{m}^i$ ..... str. 22
  - $e(L/K)$ – indeks rozgałęzienia rozszerzenia ciał lokalnych L/K
  - K^{un}/K – maksymalne nierozgałęzione rozszerzenie ciała K
  - K^{ab}/K – maksymalne abelowe rozszerzenie ciała K
  - $I^{ab}_{\mathfrak{m}}$ – abelowa grupa inercji, tzn.:

$$I^{ab}_{\mathfrak{m}} := \{\sigma \in \mathrm{Gal}(K^{ab}/K) : x \equiv \sigma(x) \pmod{\mathfrak{m}^{ab}} \quad \forall_{x \in R^{ab}}\}$$

    gdzie R^{ab} jest pierścieniem liczb całkowitych w K^{ab} zaś $\mathfrak{m}^{ab}$ – ideałem maksymalnym w R^{ab}.

- algebraiczna teoria liczb oraz teoria ciał klas:
  - R_K – pierścień liczb całkowitych w ciele K
  - $\left(\frac{\alpha}{P}\right)_m$, $\left(\frac{\alpha}{\pi}\right)_m$ – symbol reszt potęgowych ..... str. 18
  - $D(\beta/\mathfrak{p})$ – grupa dekompozycji ..... str. 57
  - K_v, $K_{\mathfrak{p}}$ – uzupełnienie ciała K wg waluacji v (odpowiednio: waluacji odpowiadającej ideałowi $\mathfrak{p}$)
  - ι – diagonalne zanurzenie $K \hookrightarrow \mathbb{I}_K$ ..... str. 58
  - ι_v, $\iota_{\mathfrak{p}}$ – kanoniczne zanurzenia $K_v, K_{\mathfrak{p}} \hookrightarrow \mathbb{I}_K$ ..... str. 58
  - $\mathbb{I}_K$ – grupa ideli ciała K ..... str. 58
  - ρ_K, $\rho_{L/K}$, $[\cdot K]$, $[\cdot L/K]$ – homomorfizmy Artina ..... str. 57, 58

- krzywe eliptyczne:
  - E_{AB} – krzywa zadana równaniem Weierstrassa: $y^2 = x^3 + Ax + B$ ..... str. 9
  - 0_E – punkt wyróżniony na krzywej eliptycznej ..... str. 9 (w przypadku krzywej Weierstrassa: $0_E = [0:1:0]$)
  - $\Delta(E_{AB}) = -16 \cdot (4A^3 + 27B^2)$ – wyróżnik krzywej Weierstrassa ..... str. 9
  - $j(E_{AB}) = -1728 \cdot \frac{(4A)^3}{\Delta(E_{AB})}$ – j-niezmiennik krzywej eliptycznej ..... str. 10
  - $\gamma(E_{AB}/K) = \sqrt{-2A/B}$ ..... str. 10
  - $E_{ns}(\overline{K})$ – grupa $\overline{K}$-wymiernych punktów nieosobliwych ..... str. 11
  - $End(E)$ – $\overline{K}$-izogenie $E \to E$
  - $a_q(E)$ – ślad morfizmu Frobeniusa F_q krzywej E ..... str. 13
  - $\widetilde{E}$ – redukcja krzywej E ..... str. 27
  - $E_i(R_j)$ – jądro redukcji $\pmod{\pi^j}$ ..... str. 27

- $\widehat{E}$ – grupa formalna związana z krzywą eliptyczną ..... str. 29
- $E[p^\infty]$ – grupa p-podzielna związana z krzywą eliptyczną ..... str. 25, 56

- inne:
  - $d_p(E)$ – p-stopień krzywej eliptycznej $E/\mathbb{Q}_p$ ..... str. 5
  - $D(p) := \{d_p(E) : E/\mathbb{Q}_p$ – krzywa eliptyczna dobrej redukcji w $p\}$. ..... str. 6
  - $\operatorname{ord}_p x$, $\operatorname{ord}_\pi x$ – rząd x w grupie odp. $(\mathbb{Z}/p)^\times$ lub $(R_K/\pi)^\times$ ..... str. 8, 43
  - $G[n] = \ker(G \xrightarrow{\cdot n} G)$ – n-torsja w grupie abelowej G
  - $G_{tors} = \bigcup_n G[n]$ – podgrupa torsyjna G
  - $\operatorname{rank}_p G := \dim_{\mathbb{F}_p} G[p]$ ..... str. 33
  - $\mathbb{Q}_p^k = \{a^k : a \in \mathbb{Q}_p\}$

BIBLIOGRAFIA

[AM69] Michael F. Atiyah and Ian G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[CD14] John B. Cosgrave and Karl Dilcher. The Gauss-Wilson theorem for quarter-intervals. *Acta Math. Hungar.*, 142(1):199–230, 2014.

[CGP15] Brian Conrad, Ofer Gabber, and Gopal Prasad. *Pseudo-reductive groups*, volume 26 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, second edition, 2015.

[Cox89] David A. Cox. *Primes of the form $x^2 + ny^2$*. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1989. Fermat, class field theory and complex multiplication.

[Dav00] Harold Davenport. *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2000. Revised and with a preface by Hugh L. Montgomery.

[Deu41] Max Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–272, 1941.

[DW08] Chantal David and Tom Weston. Local torsion on elliptic curves and the deformation theory of Galois representations. *Math. Res. Lett.*, 15(3):599–611, 2008.

[Gam14] Adam Gamzon. Local torsion on abelian surfaces with real multiplication by $\mathbf{Q}(\sqrt{5})$. *Int. J. Number Theory*, 10(7):1807–1827, 2014.

[Har77] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[Hid13] Haruzo Hida. *Elliptic curves and arithmetic invariants*. Springer Monographs in Mathematics. Springer, New York, 2013.

[IR90] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[Kat81] Nicholas M. Katz. Serre-Tate local moduli. In *Algebraic surfaces (Orsay, 1976–78)*, volume 868 of *Lecture Notes in Math.*, pages 138–202. Springer, Berlin-New York, 1981.

[KM85] Nicholas M. Katz and Barry Mazur. *Arithmetic moduli of elliptic curves*, volume 108 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1985.

[Lan87] Serge Lang. *Elliptic functions*. Graduate texts in mathematics. Springer, New York, Berlin, 1987. Index, bibliogr.

[Mil80] James S. Milne. *Étale cohomology*, volume 33 of *Princeton Mathematical Series*. Princeton University Press, Princeton, N.J., 1980.

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

[Sha86] Stephen S. Shatz. Group schemes, formal groups, and p-divisible groups. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 29–78. Springer, New York, 1986.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[Sta16] The Stacks Project Authors. *Stacks Project*. `http://stacks.math.columbia.edu`, 2016.

[Tat97] John Tate. *Modular Forms and Fermat's Last Theorem*, chapter Finite Flat Group Schemes, pages 121–154. Springer New York, New York, NY, 1997.