Uniwersytet Śląski
Wydział Matematyki, Fizyki i Chemii
Instytut Matematyki

Paweł Gładki

Hipoteza Riemanna dla ciał funkcji algebraicznych

Praca magisterska
napisana pod kierunkiem
prof. dra hab. Kazimierza Szymiczka

Katowice 2002

Spis treści

Wstęp

> Teoria liczb (...) nie ma sobie równej, wśród nauk matematycznych, w odwoływaniu się do naturalnej ludzkiej ciekawości.
>
> G.H. Hardy

W roku 1859 B. Riemann opublikował obszerną pracę (por. [**11**]), w której zdefiniował między innymi **funkcję ζ Riemanna** jako szereg Dirichleta:

$$\sum_{n=1}^{\infty} n^{-t}, \text{ dla } \mathsf{Re}\,(t) > 1$$

i dostrzegł jej znaczenie dla teorii liczb, w szczególności dla problemu rozmieszczenia liczb pierwszych. Można pokazać (por. [**9**] str. 222), że funkcja ta daje się przedłużyć do funkcji meromorficznej na całej płaszczyźnie zespolonej ze zwykłym biegunem w punkcie $t = 1$. W swojej pracy niemiecki matematyk udowodnił też wiele innych własności, a ponadto wysunął szereg przypuszczeń i hipotez, których większość została następnie udowodniona. Nie znaleziono natomiast dotychczas dowodu dla następującego przypuszczenia, które obecnie nazywa się **hipotezą Riemanna**:

> *Wszystkie zera funkcji ζ Riemanna różne od $-2, -4, \ldots$ leżą na prostej $\mathsf{Re}\, t = \frac{1}{2}$*

Hipoteza ta zrobiła na przestrzeni ostatnich 150 lat zawrotną karierę. Znane jest powiedzenie Davida Hilberta, który stwierdził, że gdyby dano mu zmartwychwstać za dwieście lat, to nie spytałby o postępy ludzkie na polu społecznym ani o postępy techniczne, lecz przede wszystkim o to, co wiadomo o miejscach zerowych funkcji ζ, gdyż "jest to nie tylko najciekawsze zagadnienie matematyczne, ale najciekawsze zagadnienie w ogóle..." Pokazano, że zakładając prawdziwość hipotezy Riemanna można udowodnić deterministyczność niektórych testów pierwszości. Jej rozstrzygnięcie zostało zaliczone do siedmiu problemów milenijnych, rozwiązanie których premiowane jest nagrodą wysokości miliona dolarów.

Niezależnie od prób rozstrzygnięcia hipotezy riemannowskiej skonstruowano pewne jej uogólnienia. Jedną z podstawowych własności funkcji ζ jest następująca jej reprezentacja w postaci iloczynu bezwzględnie zbieżnego:

$$\zeta(s) = \prod_{p} \frac{1}{1 - p^{-s}}$$

gdzie produkt przebiega po wszystkich liczbach pierwszych. W dowodzie tego faktu wykorzystuje się jednoznaczność rozkładu liczb całkowitych na czynniki pierwsze. Dedekind zaproponował więc, aby rozważać ogólniejszą funkcję:

$$\zeta_K(s) = \sum_{\mathfrak{a}} \mathfrak{N}(\mathfrak{a})^{-s}$$

gdzie K jest ciałem liczbowym, suma przebiega po wszystkich ideałach właściwych pierścienia liczb całkowitych $\mathcal{O}_K$ ciała K, a symbol $\mathfrak{N}(\mathfrak{p})$ oznacza moc pierścienia

ilorazowego $\mathcal{O}_K/\mathfrak{p}$. Można udowodnić, że pierścień liczb całkowitych $\mathcal{O}_K$ takiego ciała jest pierścieniem Dedekinda (por. [**2**] str. 263), a więc pierścieniem z jednoznacznym rozkładem ideału na iloczyn ideałów pierwszych (por. [**2**] twierdzenie V.3.1.1). Korzystając z tego faktu da się pokazać, że:

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - \mathfrak{N}(\mathfrak{p})^{-1}}$$

gdzie produkt przebiega po wszystkich ideałach pierwszych pierścienia liczb całkowitych ciała K, widzimy więc, że jest to "porządne" uogólnienie funkcji ζ.

Pierścienie Dedekinda mają naturalny związek z funkcjami, zwanymi waluacjami dyskretnymi (por. [**2**] str. 264 - 270), można więc pokusić się o przeniesienie uogólnienia w sensie Dedekinda na te ciała, w których waluacji jest "pod dostatkiem" i mają pewne naturalne i zarazem ważne interpretacje. Takimi ciałami są na przykład ciała funkcji algebraicznych, których teoria wyrosła na gruncie geometrii algebraicznej. Ciała funkcji algebraicznych można bowiem konstruować jako ciała szczególnego rodzaju funkcji wymiernych, związanych z krzywymi algebraicznymi. Pierścienie waluacyjne takich ciał odpowiadają nieosobliwym punktom na krzywych i pozwalają wykorzystać potężny aparat badawczy teorii ciał do ich studiowania. Możemy więc mówić o hipotezie Riemanna dla krzywych eliptycznych, krzywych hipereliptycznych itp.

Głównym celem tej pracy jest przestudiowanie twierdzenia Hasse'go - Weil'a i dyskusja wybranych jego interpretacji. W rozdziałach pierwszym i drugim podajemy podstawowe fakty z zakresu teorii ciał funkcji algebraicznych. Kolejność i układ wyłożonego materiału jest mniej więcej zgodny z wykładem monograficznym "Krzywe algebraiczne i ciała funkcji algebraicznych" prowadzonego przez prof. Kazimierza Szymiczka w roku akademickim 2000/2001 - w przypadku rozdziału 1 oraz z III rozdziałem książki [**14**] w przypadku rozdziału 2. Z uwagi tak na ograniczone ramy niniejszej pracy jak i na dosyć wysoki poziom trudności niektórych twierdzeń, znacznie odbiegających od głównego tematu, którym się zajmujemy, autor zdecydował się tutaj na bolesny, aczkolwiek konieczny zabieg pominięcia wszystkich dowodów. Zainteresowanego Czytelnika odsyłamy więc do literatury - dokładniej do książki Stichtenotha [**14**] - tymczasem potraktujmy te dwa rozdziały jako część informacyjną, w której cytujemy tylko twierdzenia i ustalamy notację.

Rozdział trzeci poświęcony jest w całości twierdzeniu Hasse'go - Weil'a. W pierwszym paragrafie wprowadzamy pojęcie funkcji dzeta ciała funkcji algebraicznych i studiujemy jej podstawowe własności. Pojawiają się tu też takie pojęcia jak grupa Piccarda oraz $L-$wielomian ciała funkcji algebraicznych. Paragraf drugi zawiera dowód twierdzenia Hasse'go - Weil'a wraz z wszystkimi potrzebnymi lematami. W ostatnim paragrafie podajemy definicję funkcji ζ ciała funkcji algebraicznych i pokazujemy, w jaki sposób udowodnione twierdzenie służy potwierdzeniu odpowiednio zmodyfikowanej hipotezy Riemanna.

W czwartym rozdziale zajmujemy się krzywymi algebraicznymi. W pierwszym paragrafie wprowadzamy pojęcie zbioru algebraicznego, rozmaitości, pierścienia współrzędnych, ciała funkcji wymiernych na rozmaitości, pierścienia lokalnego punktu i jego ideału maksymalnego, przy czym równolegle studiujemy teorię rozmaitości afinicznych i rzutowych. Podajemy tu szereg faktów z geometrii algebraicznej, część z nich udowadniając, a część tylko komentując i odsyłając do stosownej literatury. Osobny paragraf poświęcamy szczególnemu rodzajowi rozmaitości - mianowicie krzywym algebraicznym, dla których wyłożony materiał znacznie się upraszcza.

Przy tej okazji wyróżniamy też tak zwane punkty nieosobliwe i osobliwe na rozmaitościach i w tym kontekście rozpatrujemy krzywe nieosobliwe i osobliwe. Dokładniej zajmujemy się tak zwanymi punktami $F-$wymiernymi na rozmaitościach algebraicznych. Cały paragraf poświęcamy punktom F-wymiernym na krzywych algebraicznych - definiujemy tu ciało funkcji F-wymiernych na krzywych i za jego pomocą wprowadzamy strukturę ciała funkcji algebraicznych. Udowadniamy także, że pierścień współrzędnych krzywej nieosobliwej jest pierścieniem Dedekinda. Jako wnioski z przeprowadzonych w tym rozdziale rozważań podajemy przykład oszacowania liczby punktów F-wymiernych na krzywych eliptycznych nad ciałami skończonymi o charakterystyce różnej od dwóch i formułujemy oraz potwierdzamy hipotezę Riemanna dla krzywych algebraicznych. Rozdział ten kończymy dyskusją pewnych szczególnych przypadków twierdzenia Hasse'go - Weil'a oraz sygnalizujemy niektóre możliwości dalszego jego uogólniania, głównie w kontekście hipotezy Riemanna.

Autor pragnie tutaj złożyć najserdeczniejsze podziękowania swojemu Promotorowi, profesorowi Kazimierzowi Szymiczkowi, za nieustającą, życzliwą opiekę w ciągu całego czasu pisania pracy, za wiele cennych uwag i wytknięcie szeregu niedoskonałości. Jest to też dobre miejsce na wyrażenie wdzięczności pp. drowi hab. Andrzejowi Sładkowi i drowi Markowi Szyjewskiemu, za rozbudzenie u autora zainteresowania algebrą oraz pp. dr Krystynie Skórnik i mgr Elżbiecie Augustyniak za zachętę do podjęcia studiów matematycznych.

ROZDZIAŁ 1

Podstawowe definicje i twierdzenia

1. Punkty, waluacje i dywizory

DEFINICJA 1.1.1. **Ciałem funkcji algebraicznych** *jednej zmiennej nad ciałem K nazywamy rozszerzenie $F \supseteq K$ dla którego istnieje element $x \in F$ przestępny nad K i taki, że rozszerzenie $F \supseteq K(x)$ jest skończone. Ponadto domknięcie algebraiczne $\hat{K}$ ciała K w F nazywamy* **ciałem stałych** *ciała funkcji algebraicznych.*

Ponieważ w pracy tej zajmujemy się tylko ciałami funkcji algebraicznych jednej zmiennej, więc używać będziemy skróconej nazwy - ciało funkcji algebraicznych. Odnotujmy tu, że elementy ciała funkcji algebraicznych, które wprawdzie nazywamy funkcjami algebraicznymi, nie są funkcjami w klasycznym rozumieniu tego pojęcia - trudno mówić o ich dziedzinie, przeciwdziedzinie itp. Nazwa ta jest wszakże umotywowana historycznie, co bardziej zrozumiałe stanie się po jakimś czasie.

DEFINICJA 1.1.2. *Niech F/K będzie ciałem funkcji algebraicznych. Pierścień $\mathcal{O} \subseteq F$ nazywamy* **pierścieniem waluacyjnym**, *jeżeli ma następujące dwie własności:*

(1) $K \subsetneq \mathcal{O} \subsetneq F$
(2) $\bigwedge_{z \in F} \left(z \in \mathcal{O} \vee z^{-1} \in \mathcal{O}\right)$

Zwróćmy uwagę, że mówimy tu wyłącznie o pierścieniach waluacyjnych w rozszerzeniu ciał - nie jest to dokładnie to samo co "zwykły" pierścień waluacyjny znany z algebry przemiennej, w którego definicji nie uwzględniamy warunku (1). Najważniejsze z naszego punktu widzenia twierdzenie o pierścieniach waluacyjnych brzmi następująco:

TWIERDZENIE 1.1.1. *Niech F/K będzie ciałem funkcji algebraicznych, zaś $\mathcal{O} \subseteq F$ pierścieniem waluacyjnym. Pierścień ten jest lokalny, a jego jedynym ideałem maksymalnym jest $P = \mathcal{O} \setminus U(\mathcal{O})$.*

Twierdzenie to pozwala wprowadzić kolejną definicję:

DEFINICJA 1.1.3. *Niech F/K będzie ciałem funkcji algebraicznych, zaś $\mathcal{O} \subseteq F$ pierścieniem waluacyjnym. Jedyny ideał maksymalny P tego pierścienia nazywamy* **punktem** *ciała F. Pierścień waluacyjny związany w ten sposób z punktem P oznaczać będziemy przez $\mathcal{O}_P$, a zbiór wszystkich punktów ciała F przez $\mathbb{P}_F$.*

Punkty ciał funkcji algebraicznych mają szereg interesujących własności. Część z nich poznamy w dalszym toku pracy, a teraz podamy tylko dwie konieczne do sformułowania kolejnych pojęć.

TWIERDZENIE 1.1.2. *Niech F/K będzie ciałem funkcji algebraicznych, natomiast $\mathcal{O}_P \subseteq F$ pierścieniem waluacyjnym związanym z punktem $P \in \mathbb{P}_F$ tego ciała.*

(1) *P jest ideałem głównym pierścienia $\mathcal{O}_P$.*

(2) *Jeżeli* $P =< t >$, $t \in \mathcal{O}_P$, *to każdy element* $z \in F$ *można jednoznacznie przedstawić w postaci:*

$$z = t^k \cdot u$$

gdzie $u \in U(\mathcal{O}_P)$, *a* $k \in \mathbb{Z}$ *jest pewną liczbą całkowitą.*

DEFINICJA 1.1.4. *Niech* F/K *będzie ciałem funkcji algebraicznych, zaś* $\mathcal{O}_P \subseteq F$ *pierścieniem waluacyjnym związanym z punktem* $P \in \mathbb{P}_F$ *tego ciała. Element* $t \in \mathcal{O}_P$ *taki, że* $P =< t >$, *nazywamy* **elementem uniformizującym** *punktu* P.

Z pierścieniami waluacyjnymi i punktami zwiążemy teraz pewną klasę funkcji, zwanych waluacjami dyskretnymi. Tak jak przed chwilą odnotujmy tu, że chodzi nam o waluacje w rozszerzeniu ciała, będące szczególnego rodzaju waluacjami znanymi z ogólnej algebry.

DEFINICJA 1.1.5. *Niech* F/K *będzie ciałem funkcji algebraicznych. Funkcję* $v : F \to \mathbb{Z} \cup \{\infty\}$ *nazywamy* **waluacją dyskretną**, *jeżeli czyni zadość następującym pięciu warunkom:*

(1) $v(x) = \infty \iff x = 0$
(2) $\bigwedge_{x,y \in F} (v(x \cdot y) = v(x) + v(y))$
(3) $\bigwedge_{x,y \in F} (v(x + y) \geqslant \min\{v(x), v(y)\})$
(4) $\bigvee_{z \in F} (v(z) = 1)$
(5) $\bigwedge_{a \in K \setminus \{0\}} (v(a) = 0)$

Przydatne będzie nam następujące twierdzenie, zwane mocną nierównością trójkąta, które jest wzmocnieniem warunku (3) powyższej definicji:

TWIERDZENIE 1.1.3. *Niech* F/K *będzie ciałem funkcji algebraicznych i* $v : F \to \mathbb{Z} \cup \{\infty\}$ *waluacją dyskretną. Jeżeli dla elementów* $x, y \in F$ $v(x) \neq v(y)$ *to:*

$$v(x + y) = \min\{v(x), v(y)\}$$

TWIERDZENIE 1.1.4. *Niech* F/K *będzie ciałem funkcji algebraicznych.*

(1) *Jeżeli* $\mathcal{O}_P \subseteq F$ *jest pierścieniem waluacyjnym związanym z punktem* $P \in \mathbb{P}_F$ *i* $t \in \mathcal{O}_P$ *jest elementem uniformizującym dla* P, *to funkcja* $v_P : F \to \mathbb{Z} \cup \{\infty\}$ *zadana wzorem:*

$$v_P(z) = \begin{cases} k & \text{jeżeli } 0 \neq z = t^k u,\ u \in U(\mathcal{O}_P) \\ \infty & \text{jeżeli } 0 = z \end{cases}$$

jest waluacją dyskretną, o której będziemy mówić, że jest związana z punktem P. *Ponadto:*
- $\mathcal{O}_P = \{z \in F : v_P(z) \geqslant 0\}$
- $P = \{z \in F : v_P(z) > 0\}$
- $U(\mathcal{O}_P) = \{z \in F : v_P(z) = 0\}$

(2) *Jeżeli funkcja* $v : F \to \mathbb{Z} \cup \{\infty\}$ *jest waluacją dyskretną, to:*

$$\mathcal{O} = \{z \in F : v(z) \geqslant 0\}$$

jest pierścieniem waluacyjnym, o którym będziemy mówić, że jest związany z waluacją v.

Ponieważ dla ciała funkcji algebraicznych F/K punkt P jest ideałem maksymalnym pierścienia waluacyjnego $\mathcal{O}_P$ z nim związanego, więc pierścień ilorazowy $\mathcal{O}_P/P$ jest ciałem. Ponadto - zgodnie z definicją waluacji, pierścienia waluacyjnego i powyższym twierdzeniem - $K \subseteq \mathcal{O}_P$ oraz $K \cap P = \{0\}$, zatem ciało K można zanurzyć w ciało $\mathcal{O}_P/P$. Uprawomocnia to wprowadzenie kolejnej definicji:

DEFINICJA 1.1.6. *Niech F/K będzie ciałem funkcji algebraicznych, zaś $\mathcal{O}_P \subseteq F$ pierścieniem waluacyjnym związanym z punktem $P \in \mathbb{P}_F$ tego ciała.*

(1) *Ciało $\mathcal{O}_P/P$ nazywamy* **ciałem reszt** *punktu P i oznaczamy F_P.*
(2) *Stopień rozszerzenia $F_P \supseteq K$ oznaczamy $\deg P$ i nazywamy* **stopniem punktu** *P.*
(3) *Odwzorowanie $\pi_P : F \to F_P \cup \{\infty\}$ określone wzorem:*

$$\pi_P(x) = \begin{cases} x + P & \text{jeżeli } x \in \mathcal{O}_P \\ \infty & \text{jeżeli } x \notin \mathcal{O}_P \end{cases}$$

nazywamy **odwzorowaniem** *F* **w ciało reszt**. *Dla oznaczenia warstwy $x+P$ (lub symbolu ∞, gdy $x \notin \mathcal{O}_P$) stosujemy też zapis $x(P)$ i w tym sensie mówimy o* **wartości** *funkcji algebraicznej w punkcie.*

Bezpośrednio z powyższych definicji widzimy, że dla ciała funkcji algebraicznych F/K, elementu $x \in F$, punktu $P \in \mathbb{P}_F$ i związanych z nim pierścienia waluacyjnego $\mathcal{O}_P$ oraz waluacji dyskretnej v_P prawdziwe są następujące ciągi równoważności:

$$(x(P) = 0) \iff (x \in P) \iff (v_P(x) > 0)$$

$$(x(P) = \infty) \iff (x \notin \mathcal{O}_P) \iff (v_P(x) < 0)$$

Wiąże się z nimi następna definicja:

DEFINICJA 1.1.7. *Niech F/K będzie ciałem funkcji algebraicznych, natomiast v_P waluacją dyskretną związaną z punktem $P \in \mathbb{P}_F$ tego ciała.*

(1) *P nazwiemy* **zerem** *elementu $x \in F$, jeżeli $x(P) = 0$, a liczbę $v_P(x)$ nazwiemy* **krotnością zera**.
(2) *P nazwiemy* **biegunem** *elementu $x \in F$, jeżeli $x(P) = \infty$, a liczbę $-v_P(x)$ nazwiemy* **krotnością bieguna**.

Zastępując w powyższej definicji słowo "element" zwrotem "funkcja algebraiczna" możemy w pewnym stopniu usprawiedliwić nazwę "ciało funkcji algebraicznych" - pojęcia tu definiowane wydają się bowiem bliskie teorii funkcji analitycznych. Dalsze analogie odkryjemy w kolejnych rozdziałach i w podobny sposób zinterpretujemy otrzymane wyniki jako potwierdzenie hipotezy Riemanna. Odnotujmy tymczasem jeszcze jedno twierdzenie, które okaże się nam nader pomocne:

TWIERDZENIE 1.1.5. *Niech F/K będzie ciałem funkcji algebraicznych.*

(1) *Każdy element (funkcja algebraiczna) ciała F ma co najmniej jedno, lecz zarazem skończenie wiele zer.*
(2) *Każdy element (funkcja algebraiczna) ciała F ma co najmniej jeden, lecz zarazem skończenie wiele biegunów.*

Zajmijmy się obecnie dywizorami. Wyjaśnienie tego, jak również innych związanych z teorią dywizorów pojęć ujmuje:

DEFINICJA 1.1.8. *Niech F/K będzie ciałem funkcji algebraicznych.*

(1) *Wolną grupę abelową z bazą $\mathbb{P}_F$ oznaczamy $\mathcal{D}_F$ i nazywamy* **grupą dywizorów**, *a jej elementy* **dywizorami**. *Dla ustalonego dywizora $A = \sum_{P \in \mathbb{P}_F} n_P \cdot P$ często zamiast n_P pisać będziemy $v_P(A)$.*
(2) *Dla ustalonego elementu $x \in F$ dywizory:*
    - $(x) := \sum_{P \in \mathbb{P}_F} v_P(x) \cdot P$
    - $(x)_0 := \sum_{P \in \mathbb{P}_F, v_P(x) > 0} v_P(x) \cdot P$

♦ $(x)_\infty := \sum_{P\in\mathbb{P}_F, v_P(x)<0} v_P(x)\cdot P$

nazywamy, odpowiednio, **dywizorem głównym**, **dywizorem zer** *i* **dywizorem biegunów** *funkcji algebraicznej x. Przy tym zbiór dywizorów głównych oznaczamy $\mathcal{P}_F$.*

(3) **Dywizorami pierwszymi** *nazywamy punkty ciała F.*

(4) *Dla ustalonego dywizora $A = \sum_{P\in\mathbb{P}_F} n_P\cdot P$ jego* **stopniem** *nazywamy liczbę $\deg A := \sum_{P\in\mathbb{P}_F} n_P\cdot \deg P$.*

(5) *W grupie dywizorów $\mathcal{D}_F$ dywizory stopnia zero tworzą podgrupę, którą oznaczać będziemy $\mathcal{D}_F^0$.*

(6) *W zbiorze dywizorów $\mathcal{D}_F$ definiujemy relację częściowego porządku warunkiem:*

$$A \leqslant B \iff \bigwedge_{P\in\mathbb{P}_F} (v_P(A) \leqslant v_P(B))$$

(7) *Dla ustalonego dywizora $A \in \mathcal{D}_F$ zbiór:*

$$\mathcal{L}(A) = \{x \in F : (x) \geqslant -A\} \cup \{0\}$$

okazuje się być przestrzenią liniową nad ciałem K, której wymiar nazywamy **wymiarem dywizora** *i oznaczamy $\dim A$.*

(8) *Dwa dywizory $A, B \in \mathcal{D}_F$ nazwiemy* **równoważnymi**, *co oznaczymy jako $A \sim B$, wtedy i tylko wtedy, gdy dla pewnego elementu $x \in U(F)$ zachodzi równość $A = B + (x)$.*

Potrzebne nam własności dywizorów ujmuje następujące:

TWIERDZENIE 1.1.6. *Niech F/K będzie ciałem funkcji algebraicznych, $A, B \in \mathcal{D}_F$.*

(1) *Jeżeli $A \sim B$, to $\dim A = \dim B$ oraz $\deg A = \deg B$.*

(2) *Dla dowolnego elementu $x \in F$:*

$$(x) = (x)_0 - (x)_\infty$$

oraz:

$$\deg (x)_0 = \deg (x)_\infty = [F : K(x)]$$

Można się przekonać, że dywizory główne tworzą podgrupę grupy dywizorów, która - jako że $\mathcal{D}_F$ jest abelowa - jest też normalna. Jest zatem celowe rozpatrywanie grupy ilorazowej $\mathcal{D}_F/\mathcal{P}_F$. Elementy tej grupy są w istocie klasami abstrakcji relacji równoważności dywizorów (która okazuje się być relacją równoważnościową), co razem z tezą (1) twierdzenia 1.1.6 pozwala zdefiniować wymiar i stopień klasy jako wymiar i stopień dowolnego jej reprezentanta. Podsumujmy więc:

DEFINICJA 1.1.9. *Niech F/K będzie ciałem funkcji algebraicznych, $\mathcal{D}_F$ grupą dywizorów a $\mathcal{P}_F$ podgrupą dywizorów głównych.*

(1) *Grupę $\mathcal{D}_F/\mathcal{P}_F$ nazywamy* **grupą klas dywizorów** *i oznaczamy $\mathcal{C}_F$. Jej elementy oznaczać będziemy jako $[A]$.*

(2) **Stopniem** *klasy $[A] \in \mathcal{C}_F$ nazywamy stopień dowolnego jej reprezentanta i oznaczamy $\deg [A]$.*

(3) **Wymiarem** *klasy $[A] \in \mathcal{C}_F$ nazywamy wymiar dowolnego jej reprezentanta i oznaczamy $\dim [A]$.*

(4) *Klasy dywizorów stopnia zero tworzą podgrupę w grupie $\mathcal{C}_F$, którą oznaczamy przez $\mathcal{C}_F^0$ i nazywamy* **grupą Piccarda**.

2. Ciało funkcji wymiernych

Najprostszym i zarazem bardzo naturalnym przykładem ciała funkcji algebraicznych jest ciało funkcji wymiernych. Zilustrujmy poznane pojęcia na tym właśnie przykładzie. Niech więc K będzie ciałem, x elementem nad nim przestępnym i rozważmy ciało funkcji algebraicznych $K(x)/K$.

Uwaga 1.2.1. *Zbiór:*

$$\mathcal{O}_{p(X)} = \left\{ \frac{f(x)}{g(x)} : f(X), g(X) \in K[X], p(X) \nmid g(X) \right\}$$

gdzie $p(X) \in K[X]$ jest wielomianem nierozkładalnym i unormowanym, jest pierścieniem waluacyjnym w $K(x)$ z ideałem maksymalnym:

$$P_{p(X)} = \left\{ \frac{f(x)}{g(x)} : f(X), g(X) \in K[X], p(X) | f(X), p(X) \nmid g(X) \right\}$$

Stopień punktu $P_{p(X)}$ równy jest stopniowi wielomianu $p(X)$. Przy tym oznaczamy:

$$P_\alpha = P_{X-\alpha}$$

Zbiór:

$$\mathcal{O}_\infty = \left\{ \frac{f(x)}{g(x)} : f(X), g(X) \in K[X], \deg f(X) \leqslant g(X) \right\}$$

jest pierścieniem waluacyjnym w $K(x)$ z ideałem maksymalnym:

$$P_\infty = \left\{ \frac{f(x)}{g(x)} : f(X), g(X) \in K[X], \deg f(X) < \deg g(X) \right\}$$

P_∞ jest punktem stopnia 1.

Powyższa uwaga wraz z następnym twierdzeniem pokazuje nam, że punkty w ciele funkcji wymiernych mają bardzo czytelny opis, z którego wielokrotnie będziemy korzystać.

Twierdzenie 1.2.1. *W ciele funkcji wymiernych nie ma innych punktów niż punkty postaci $P_{p(X)}$ oraz P_∞.*

3. Rodzaj ciała funkcji algebraicznych. Twierdzenie Riemanna - Rocha

W tym paragrafie podamy podstawowe twierdzenie teorii ciał funkcji algebraicznych, wiążące ze sobą pojęcie stopnia i wymiaru dywizora, pochodzące od Riemanna i Rocha. Najpierw jednak zdefiniujmy rodzaj ciała funkcji algebraicznych. Potrzebne będzie nam w tym celu następujące:

Twierdzenie 1.3.1. *Niech F/K będzie ciałem funkcji algebraicznych. Istnieje taka liczba naturalna γ, że:*

$$\bigwedge_{A \in \mathcal{D}_F} (\deg A - \dim A \leqslant \gamma)$$

Definicja 1.3.1. *Niech F/K będzie ciałem funkcji algebraicznych. Najmniejsza spośród takich liczb naturalnych γ, że:*

$$\bigwedge_{A \in \mathcal{D}_F} (\deg A - \dim A \leqslant \gamma)$$

nazywa się **rodzajem** *ciała funkcji algebraicznych F/K i oznaczana jest przez $g(F)$ lub po prostu g.*

Wyznaczenie wymiaru dywizora jest na ogół zajęciem bardzo trudnym - jak widzieliśmy, definicja wymiaru jest mało intuicyjna i niewiele mówi nam o sposobie jego obliczania. Sporym ułatwieniem jest twierdzenie Riemanna - Rocha, które zaraz podamy. Trzeba tu jednak zaznaczyć, że rezultat ten nie rozwiązuje do końca zasygnalizowanych trudności; wyznaczenie rodzaju ciała też nie jest proste, a czasami jest zgoła niemożliwe - podaje się tylko pewne oszacowania, przykładowym wynikiem tej teorii są twierdzenia pochodzące od Castelnuovo. Sam dowód twierdzenia Riemanna - Rocha również do najprostszych nie należy i angażuje dosyć zaawansowany aparat algebraiczny, na który składają się takie pojęcia jak idele, adele, różniczki Weyl'a itp. Przed zacytowaniem twierdzenia musimy więc przybliżyć kilka pojęć niezbędnych dla zrozumienia jego wypowiedzi.

DEFINICJA 1.3.2. *Niech F/K będzie ciałem funkcji algebraicznych o rodzaju g.*

(1) *Dla ustalonego dywizora $A \in \mathcal{D}_F$ jego* **indeksem** *nazywamy liczbę $i(A) = \dim A - 1 + \deg A - g$.*
(2) *Dywizor $A \in \mathcal{D}_F$ nazywamy* **specjalnym**, *jeżeli $i(A) > 0$.*
(3) *Dokładnie jedna klasa $[W] \in \mathcal{C}_F$ [1] taka, że:*

$$\bigwedge_{A \in \mathcal{D}_F} \bigwedge_{W \in [W]} (i(A) = \dim (W - A))$$

nazywana jest **klasą kanoniczną**, *a jej elementy* **dywizorami kanonicznymi**.

TWIERDZENIE 1.3.2. (RIEMANNA - ROCHA) *Niech F/K będzie ciałem funkcji algebraicznych o rodzaju g, $[W] \in \mathcal{C}_F$ klasą kanoniczną o elementach oznaczanych przez W. Przy takich założeniach, dla dowolnego dywizora $A \in \mathcal{D}_F$:*

$$\dim A = \deg A + 1 - g + \dim (W - A)$$

Z twierdzenia tego wypływa szereg ważnych wniosków. Kilka z nich podajemy poniżej.

TWIERDZENIE 1.3.3. *Niech F/K będzie ciałem funkcji algebraicznych o rodzaju g:*

(1) *Dla punktu $P \in \mathbb{P}_F$ i liczby $n \geqslant 2g$ istnieje element $x \in F$ taki, że:*

$$(x)_\infty = nP$$

(2) *Jeżeli A jest dywizorem ciała F stopnia nie mniejszego niż $2g - 1$, to:*

$$\dim A = \deg A + 1 - g$$

(3) *Ciało F/K jest ciałem funkcji wymiernych wtedy i tylko wtedy, gdy:*
F/K ma rodzaj 0 oraz istnieje w nim dywizor stopnia 1
(4) *Dla dywizorów kanonicznych W:*

$$\dim W = g \text{ oraz } \deg W = 2g - 2$$

Jako osobne wnioski podamy następujące dwa twierdzenia: Weierstrassa "o dziurach", opisujące w pewien sposób bieguny funkcji algebraicznej i mocne twierdzenie aproksymacyjne, będące swego rodzaju odpowiednikiem chińskiego twierdzenia o resztach:

[1] Oczywiście istnienie i jedyność tej klasy wymaga dowodu.

TWIERDZENIE 1.3.4. (WEIERSTRASSA "O DZIURACH") *Niech F/K będzie ciałem funkcji algebraicznych o rodzaju g, niech $P \in \mathbb{P}_F$ będzie punktem stopnia 1. Istnieje dokładnie g liczb $i_1 < \ldots < i_g$ takich, że dla wszelkich elementów $x \in F$ $(x)_\infty \neq i_j P$, $j \in \{1, \ldots, g\}$.*

TWIERDZENIE 1.3.5. (MOCNE TWIERDZENIE APROKSYMACYJNE) *Niech F/K będzie ciałem funkcji algebraicznych, a $S \subsetneq \mathbb{P}_F$ właściwym zbiorem punktów tego ciała. Niech $P_1, \ldots, P_r \in S$, niech $x_1, \ldots, x_r \in F$ oraz $n_1, \ldots, n_r \in \mathbb{Z}$. Istnieje wówczas funkcja algebraiczna $x \in F$ taka, że:*

$$v_{P_i}(x - x_i) = n_i$$

dla $i \in \{1, \ldots, r\}$ oraz

$$v_P(x) \geqslant 0$$

dla $P \in S \setminus \{P_1, \ldots, P_r\}$.

ROZDZIAŁ 2

Rozszerzenia ciał funkcji algebraicznych

1. Rozszerzenia algebraiczne

DEFINICJA 2.1.1. *Niech F'/K' oraz F/K będą ciałami funkcji algebraicznych.*

(1) *F'/K' nazywamy* **rozszerzeniem ciała funkcji algebraicznych** *F/K, co oznaczamy $F'/K' \supseteq F/K$, gdy $F' \supseteq F$ oraz $K' \supseteq K$.*
(2) *Rozszerzenie $F'/K' \supseteq F/K$ nazywamy* **algebraicznym**, *jeżeli rozszerzenie $F' \supseteq F$ jest algebraiczne.*
(3) *Rozszerzenie $F'/K' \supseteq F/K$ nazywamy* **rozszerzeniem ciała stałych** *K' o ciało F, jeśli $F' = FK'$.*
(4) *Rozszerzenie $F'/K' \supseteq F/K$ nazywamy* **skończonym**, *gdy $[F' : F] < +\infty$.*

Podstawowe własności rozszerzeń ciał funkcji algebraicznych ujmuje następujące twierdzenie.

TWIERDZENIE 2.1.1. *Niech F'/K' będzie algebraicznym rozszerzeniem ciała F/K. Wówczas:*

(1) *$K' \supset K$ jest rozszerzeniem algebraicznym oraz $F \cap K' = K$*
(2) *F'/K' jest rozszerzeniem skończonym F/K wtedy i tylko wtedy, gdy $[K' : K] < \infty$*
(3) *Jeżeli $F_1 = FK'$, to F_1/K' jest rozszerzeniem ciała stałych F/K oraz F'/K' jest skończonym rozszerzeniem ciała F_1/K' o tym samym ciele stałych.*

Okazuje się być interesującym badanie, jak zachowują się punkty ciała funkcji algebraicznych przy przejściu do rozszerzenia. Ważnym też jest stwierdzenie, w jakim stosunku mają się do siebie punkty ciała i jego rozszerzenia. Wprowadźmy więc kolejną definicję.

DEFINICJA 2.1.2. *Niech $F'/K' \supseteq F/K$ będzie rozszerzeniem algebraicznym, niech $P' \in \mathbb{P}_{F'}$, $P \in \mathbb{P}_F$ będą punktami ciał F' i F, odpowiednio. Jeżeli $P' \supseteq P$, to mówimy, że punkt P' jest* **rozszerzeniem** *punktu P (lub że* **leży nad** *punktem P), zaś punkt P jest* **zwężeniem** *punktu P' (lub* **leży pod** *nim), co oznaczamy $P'|P$.*

Następujące twierdzenie pozwala nam stwierdzić, że każdy punkt rozszerzenia leży nad pewnym punktem ciała wyjściowego oraz - na odwrót - każdy punkt ciała wyjściowego ma skończenie wiele rozszerzeń.

TWIERDZENIE 2.1.2. *Niech F'/K' będzie algebraicznym rozszerzeniem ciała F/K.*

(1) *Dla każdego punktu $P' \in \mathbb{P}_{F'}$ istnieje dokładnie jeden punkt $P \in \mathbb{P}_F$ taki, że $P'|P$.*
(2) *Dla każdego punktu $P \in \mathbb{P}_F$ istnieje co najmniej jeden i zarazem skończenie wiele punktów $P' \in \mathbb{P}_{F'}$ takich, że $P'|P$.*

Kolejne twierdzenie podaje kilka warunków równoważnych na to, aby jeden punkt leżał nad drugim.

TWIERDZENIE 2.1.3. *Niech $F'/K' \supseteq F/K$ będzie rozszerzeniem algebraicznym. Dla punktów $P \in \mathbb{P}_F$ i $P' \in \mathbb{P}_{F'}$ niech $\mathcal{O}_P$ i $\mathcal{O}_{P'}$ będą odpowiednimi pierścieniami waluacyjnymi, zaś v_P oraz $v_{P'}$ waluacjami dyskretnymi. Wówczas każde dwa z następujących trzech warunków są równoważne:*

(1) $P'|P$
(2) $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$
(3) *Istnieje liczba naturalna $e \geqslant 1$ taka, że:*

$$\bigwedge_{x \in F} (v_{P'}(x) = e \cdot v_P(x))$$

Ponadto, jeżeli $P'|P$, to:

$$P = P' \cap F \text{ oraz } \mathcal{O}_P = \mathcal{O}_{P'} \cap F$$

Zdefiniowana w punkcie (3) powyższego twierdzenia liczba e ma swoją nazwę - zwiemy ją indeksem rozgałęzienia. Indeks ten pozwala klasyfikować rozszerzenia punktów oraz wyróżnić pewien szczególny rodzaj rozszerzeń ciał.

DEFINICJA 2.1.3. *Niech $F'/K' \supseteq F/K$ będzie rozszerzeniem algebraicznym, niech $P' \in \mathbb{P}_{F'}$, $P \in \mathbb{P}_F$ będą punktami ciał F' i F, odpowiednio, przy czym $P'|P$, zaś $v_{P'}$ i v_P ich waluacjami dyskretnymi.*

(1) *Liczbę naturalną e taką, że:*

$$\bigwedge_{x \in F} (v_{P'}(x) = e \cdot v_P(x))$$

nazywamy **indeksem rozgałęzienia** *rozszerzenia punktów $P'|P$ i oznaczamy $e(P'|P)$.*
(2) *Rozszerzenie $P'|P$ nazywamy* **nierozgałęzionym**, *gdy $e(P'|P) = 1$. W przeciwnym razie rozszerzenie nazywamy* **rozgałęzionym**.
(3) *Rozszerzenie ciał $F'/K' \supseteq F/K$ nazywamy* **nierozgałęzionym**, *gdy wszystkie rozszerzenia punktów w tym rozszerzeniu są nierozgałęzione.*

Indeks rozgałęzienia w wieży ciał zachowuje sie podobnie jak stopień rozszerzenia, o czym mówi kolejne twierdzenie.

TWIERDZENIE 2.1.4. *Niech F'/K' będzie algebraicznym rozszerzeniem ciała F/K i niech punkty $P \in \mathbb{P}_F$ i $P' \in \mathbb{P}_{F'}$ leżą jeden nad drugim, $P'|P$. Jeżeli F''/K'' będzie algebraicznym rozszerzeniem ciała F'/K' i punkt $P'' \in \mathbb{P}_{F''}$ będzie leżał nad punktem P', $P''|P'$, to:*

$$e(P''|P) = e(P''|P') \cdot e(P'|P)$$

Na koniec tego paragrafu podajmy jeszcze dwie definicje - stopnia względnego punktu i jego konormy.

DEFINICJA 2.1.4. *Niech $F'/K' \supseteq F/K$ będzie rozszerzeniem algebraicznym, niech $P' \in \mathbb{P}_{F'}$, $P \in \mathbb{P}_F$ będą punktami ciał F' i F, odpowiednio, przy czym $P'|P$. Stopień rozszerzenia ciała reszt F_P punktu P do ciała reszt $F'_{P'}$ punktu P', $[F'_{P'} : F_P]$ nazywamy* **stopniem względnym** *rozszerzenia punktów $P'|P$ i oznaczamy $f(P'|P)$.*

DEFINICJA 2.1.5. *Niech $F'/K' \supseteq F/K$ będzie rozszerzeniem algebraicznym, niech $P \in \mathbb{P}_F$ będzie punktem ciała F, a $A \in \mathcal{D}_F$ dywizorem.*

(1) **Konormą punktu** P *nazywamy dywizor ciała F' zdefiniowany następująco:*

$$\mathsf{Con}_{F'/F}(P) = \sum_{P'|P} e(P'|P) \cdot P'$$

(2) **Konormą dywizora** A *nazywamy dywizor ciała F' zdefiniowany następująco:*

$$\mathsf{Con}_{F'/F}(A) = \sum_{P \in \mathbb{P}_F} v_P(A) \cdot \mathsf{Con}_{F'/F}(P)$$

2. Rozszerzenia ciał stałych

Wyróżnijmy w osobnym paragrafie następujące twierdzenie, które podaje nam wszystkie potrzebne w dalszym ciągu własności szczególnego rodzaju rozszerzeń algebraicznych, jakimi są rozszerzenia ciał stałych.

TWIERDZENIE 2.2.1. *Niech rozszerzenie ciała stałych $F' = FK'/K'$ będzie algebraicznym rozszerzeniem ciała F/K. Wówczas:*

(1) *K' jest pełnym ciałem stałych ciała F'.*
(2) *Rozszerzenie $F' \supset F$ jest nierozgałęzione.*
(3) *F'/K' ma ten sam rodzaj co F/K.*
(4) *Dla dowolnego dywizora $A \in \mathcal{D}_F$:*

$$\deg \mathsf{Con}_{F'/F}(A) = \deg A$$

(5) *Ciało reszt $F'_{P'}$ dowolnego punktu $P' \in \mathbb{P}_{F'}$ równe jest kompozytowi:*

$$F'_{P'} = F_P K'$$

gdzie F_P jest ciałem reszt punktu $P = P' \cap F$

3. Rozszerzenia Galois

Szczególną rolę w dowodzie twierdzenia Hasse'go - Weil'a pełnią rozszerzenia Galois i rozszerzenia rozdzielcze. Poświęcimy im ten i następny paragraf, przy czym interesować nas będą wyłącznie rozszerzenia skończone. Zobaczmy, że definiuje się je bardzo podobnie do "zwykłych" rozszerzeń:

DEFINICJA 2.3.1. *Niech $F'/K' \supseteq F/K$ będzie rozszerzeniem skończonym.*

(1) **Grupą Galois** *rozszerzenia $F'/K' \supseteq F/K$ nazywamy grupę Galois rozszerzenia $F' \supseteq F$ i oznaczamy* $\mathsf{Gal}\,(F'/F)$.
(2) *Rozszerzenie $F'/K' \supseteq F/K$ nazywamy* **rozszerzeniem Galois**, *gdy rozszerzenie $F' \supseteq F$ jest Galois.*
(3) *Rozszerzenie $F'/K' \supseteq F/K$ nazywamy* **rozszerzeniem cyklicznym**, *gdy rozszerzenie $F' \supseteq F$ jest cykliczne.*

Bardzo ważną własnością rozszerzeń typu Galois jest, że indeksy rozgałęzienia i stopnie względne rozszerzeń ustalonego punktu są takie same - co więcej, ściśle wiążą się ze stopniem rozszerzenia ciała. Mówi o tym kolejne twierdzenie.

TWIERDZENIE 2.3.1. *Niech F'/K' będzie rozszerzeniem Galois ciała F/K i $P'_1, \ldots, P'_r \in \mathbb{P}_{F'}$ niech będą wszystkimi punktami ciała F' leżącymi nad punktem $P \in \mathbb{P}_F$. Wówczas:*

(1) *Dla wszelkich* $i, j \in \{1, \dots, r\}$*:*
$$e(P'_i|P) = e(P'_j|P) \text{ oraz } f(P'_i|P) = f(P'_j|P)$$
(2) *Jeżeli* $e(P)$ *i* $f(P)$ *oznaczają wspólną wartość, odpowiednio, indeksu rozgałęzienia i stopnia względnego rozszerzeń punktu* P*, to:*
$$e(P) \cdot f(P) \cdot r = [F' : F]$$

Dla rozszerzeń punktów definiuje się specjalne grupy, będące podgrupami grupy Galois rozszerzenia ciała. Są to grupy rozkładu i grupy bezwładności. Wobec zasadniczych twierdzeń teorii Galois, odpowiadają im pewne ciała pośrednie, które tak samo nazywamy ciałami rozkładu i bezwładności. Mianowicie:

DEFINICJA 2.3.2. *Niech* $F'/K' \supseteq F/K$ *będzie rozszerzeniem Galois,* $P' \in \mathbb{P}_{F'}$*,* $P \in \mathbb{P}_F$ *punktami takimi, że* $P'|P$*, a* $v_{P'}$*,* v_P *i* $\mathcal{O}_{P'}$*,* $\mathcal{O}_P$ *waluacjami dyskretnymi i pierścieniami waluacyjnymi im odpowiadającymi.*

(1) *Grupę:*
$$G_Z(P'|P) = \{\sigma \in \mathsf{Gal}\,(F'/F) : \sigma(P') = P'\}$$
nazywamy **grupą rozkładu** *punktu* P' *nad* P*.*
(2) *Grupę:*
$$G_T(P'|P) = \{\sigma \in \mathsf{Gal}\,(F'/F) : v_{P'}(\sigma(z) - z) > 0, \text{dla } z \in \mathcal{O}_{P'}\}$$
nazywamy **grupą bezwładności** *punktu* P' *nad* P*.*
(3) *Ciało* $Z(P'|P)$ *odpowiadające grupie* $G_Z(P'|P)$ *nazywamy* **ciałem rozkładu** *punktu* P' *nad* P*.*
(4) *Ciało* $T(P'|P)$ *odpowiadające grupie* $G_T(P'|P)$ *nazywamy* **ciałem bezwładności** *punktu* P' *nad* P*.*

Potrzebne nam własności grup i ciał rozkładu i bezwładności ujmują następujące dwa twierdzenia:

TWIERDZENIE 2.3.2. *Niech* F'/K' *będzie rozszerzeniem Galois ciała* F/K *i niech* $P' \in \mathbb{P}_{F'}$ *będzie rozszerzeniem punktu* $P \in \mathbb{P}_F$*,* $P'|P$*. Jeżeli oznaczymy przez* $G_Z(P'|P)$ *grupę rozkładu takiego rozszerzenia, przez* $G_T(P'|P)$ *grupę bezwładności, zaś przez* $Z(P'|P)$ *i* $T(P'|P)$ *ciała rozkładu i bezwładności, to:*

(1) $|G_Z(P'|P)| = e(P|P) \cdot f(P'|P)$
(2) $G_T(P'|P) \lhd G_Z(P'|P)$ *oraz* $Gal(F'_{P'}/F_P) \cong G_Z(P'|P)/G_T(P'|P)$
(3) *Jeżeli* $P_Z = P' \cap Z(P'|P)$ *jest punktem ciała* $Z(P'|P)$*, to:*
$$e(P_Z|P) = f(P_Z|P) = 1$$

TWIERDZENIE 2.3.3. *Niech* F'/K' *będzie rozszerzeniem Galois ciała* F/K *i niech* $P' \in \mathbb{P}_{F'}$ *będzie rozszerzeniem punktu* $P \in \mathbb{P}_F$*,* $P'|P$*. Oznaczmy przez* $Z(P'|P)$ *i* $T(P'|P)$ *ciała rozkładu i bezwładności rozszerzenia* $P'|P$ *i dla ciała pośredniego* $F \subseteq M \subseteq F'$ *przez* P_M *punkt* $P_M = P' \cap M$ *ciała* M*. Wówczas:*

(1) $M \subseteq Z(P'|P)$ *wtedy i tylko wtedy, gdy* $e(P_M|P) = f(P_M|P) = 1$*.*
(2) $M \supseteq Z(P'|P)$ *wtedy i tylko wtedy, gdy* P' *jest jedynym punktem ciała* F' *będącym rozszerzeniem punktu* P_M*.*
(3) $M \subseteq T(P'|P)$ *wtedy i tylko wtedy, gdy* $e(P_M|P) = 1$*.*
(4) $M \supseteq T(P'|P)$ *wtedy i tylko wtedy, gdy* P' *jest jedynym punktem ciała* F' *będącym rozszerzeniem punktu* P_M *oraz* $e(P'|P_M) = [F' : M]$*.*

4. Rozszerzenia rozdzielcze

Jedynym twierdzeniem tego paragrafu jest następujące kryterium rozdzielczości, potrzebne nam w dowodzie twierdzenia Hasse'go - Weil'a:

TWIERDZENIE 2.4.1. *Niech F/K będzie ciałem funkcji algebraicznych, dla którego charakterystyka ciała K jest równa $q > 0$, $charK = q$. Jeżeli element $t \in F$ dla pewnego punktu $P \in \mathbb{P}_F$ spełnia warunek:*

$$v_P(t) \not\equiv 0 (\mathsf{mod}\, q)$$

gdzie v_P oznacza waluację dyskretną związaną z punktem P, to rozszerzenie $F \supset K(t)$ jest rozdzielcze i skończone.

ROZDZIAŁ 3

Ciała funkcji algebraicznych nad ciałami skończonymi

1. Funkcja dzeta ciała funkcji algebraicznych

W paragrafie niniejszym zdefiniujemy wszystkie pojęcia potrzebne do wypowiedzenia twierdzenia Hasse'go - Weil'a, w szczególności poznamy funkcję dzeta Riemanna ciała funkcji algebraicznych i zbadamy jej podstawowe własności.

Ustalmy liczbę naturalną (będącą potęgą liczby pierwszej) q i niech $F/\mathbb{F}_q$ będzie ciałem funkcji algebraicznych o rodzaju g.

LEMAT 3.1.1. *Dla każdej liczby $n \in \mathbb{N}$ istnieje tylko skończenie wiele dodatnich dywizorów ciała F stopnia n.*

D o w ó d : Ustalmy liczbę $n \in \mathbb{N}$ i zauważmy, że ponieważ każdy dywizor dodatni można - z definicji - przedstawić w postaci sumy dywizorów pierwszych, wystarczy pokazać, iż zbiór:

$$\mathsf{S} = \{P \in \mathbb{P}_F : \deg P \leqslant n\}$$

dywizorów pierwszych stopnia mniejszego od n jest skończony.

W tym celu wybierzmy taki element $x \in F \backslash \mathbb{F}_q$, że $[F : \mathbb{F}_q(x)] < +\infty$ i rozważmy ciało funkcji wymiernych $\mathbb{F}_q(x)$. Jest to oczywiście ciało funkcji algebraicznych $\mathbb{F}_q(x)/\mathbb{F}_q$. W zbiorze punktów $\mathbb{P}_{\mathbb{F}_q(x)}$ tego ciała weźmy pod uwagę podzbiór:

$$\mathsf{S}_0 = \{P_0 \in \mathbb{P}_{\mathbb{F}_q(x)} : \deg P_0 \leqslant n\}$$

Pokażemy najpierw, że:

$$\bigwedge_{P \in \mathrm{S}} (P \cap \mathbb{F}_q(x) \in \mathsf{S}_0)$$

Istotnie, ustalmy punkt $P \in \mathsf{S}$ i niech $\mathcal{O}_P \subseteq F$ będzie pierścieniem waluacyjnym odpowiadającym punktowi P. Rozszerzenie ciał funkcji algebraicznych $F/\mathbb{F}_q \supseteq \mathbb{F}_q(x)/\mathbb{F}_q$ jest, jako skończone, algebraiczne. Ponadto:

$$\bigwedge_{a \in \mathbb{F}_q(x)} \left(a \in \mathcal{O}_P \vee a^{-1} \in \mathcal{O}_P\right)$$

więc $\mathcal{O}_P \cap \mathbb{F}_q(x) \subseteq \mathbb{F}_q(x)$ jest pierścieniem waluacyjnym zawartym w pierścieniu $\mathcal{O}_P$. Jeżeli oznaczymy przez P_0 punkt ciała $\mathbb{F}_q(x)$ związany z pierścieniem waluacyjnym $\mathcal{O}_P \cap \mathbb{F}_q(x)$, to wobec twierdzenia 2.1.3:

$$P|P_0 \text{ oraz } P_0 = P \cap \mathbb{F}_q(x)$$

Aby przekonać się, że stopień punktu P_0 jest nie większy od n, rozważmy odwzorowania $\kappa : \mathcal{O}_P \to \mathcal{O}_P/P$ dane wzorem:

$$\kappa(x) = x(P), \text{ dla } x \in \mathcal{O}_P$$

oraz $\kappa' : \mathcal{O}_P \cap \mathbb{F}_q(x) \to \mathcal{O}_P/P$ zadane jako $\kappa' = \kappa \restriction_{\mathcal{O}_P \cap \mathbb{F}_q(x)}$. Oczywiście obydwa odwzorowania są homomorfizmami i bez trudu możemy przekonać się, że $\ker \kappa' = P \cap \mathbb{F}_q(x) = P_0$, a zatem wobec twierdzenia o homomorfizmie ciało $\mathcal{O}_P \cap \mathbb{F}_q(x)/P_0$ zanurza się w ciało $\mathcal{O}_P/P$. Skoro $\mathsf{deg}\, P = [\mathcal{O}_P/P : \mathbb{F}_q] \leqslant n$, więc $\mathsf{deg}\, P_0 = [\mathcal{O}_P \cap \mathbb{F}_q(x)/P_0 : \mathbb{F}_q] \leqslant n$.

Dalej, pokażemy, iż każdy punkt ze zbioru S_0 ma tylko skończenie wiele rozszerzeń wśród punktów ciała F. Faktycznie, ustalmy punkt $P_0 \in \mathsf{S}_0$ i niech v_{P_0} oznacza waluację dyskretną z nim związaną. Rozszerzenie ciał funkcji algebraicznych $F/\mathbb{F}_q \supseteq \mathbb{F}_q(x)/\mathbb{F}_q$ jest algebraiczne. Ponadto z tezy (1) twierdzenia 1.3.3 wynika, że istnieje element $a \in \mathbb{F}_q(x)$, którego jedynym zerem jest punkt P_0. Zauważmy więc, że:

$$\bigwedge_{P \in \mathbb{P}_F} (P|P_0 \iff v_P(a) > 0)$$

gdzie v_P oznacza waluację dyskretną związaną z punktem P.

Ustalmy punkt $P \in \mathbb{P}_F$ i załóżmy, że $P|P_0$. Wobec twierdzenia 2.1.3 istnieje liczba naturalna $e \in \mathbb{N}$ taka, że $v_P(a) = e \cdot v_{P_0}(a) > 0$.

Na odwrót, ustalmy punkt $P \in \mathbb{P}_F$ i załóżmy, że $v_P(a) > 0$. Wobec twierdzenia 2.1.2 istnieje punkt $Q \in \mathbb{P}_{\mathbb{F}_q(x)}$ będący zwężeniem punktu P. Jeżeli przez v_Q oznaczymy waluację dyskretną związaną z tym punktem, to stosując twierdzenie 2.1.3 mamy, że $v_Q(a) > 0$. Jednakże punkt P_0 jest jedynym zerem elementu a w ciele $\mathbb{F}_q(x)$, więc $Q = P_0$.

Wobec wniosku 1.1.5 element a ma skończoną liczbę zer w ciele F, czyli na mocy pokazanej równoważności, punkt P_0 ma skończoną liczbę rozszerzeń w ciele F. Z drugiej strony pokazaliśmy, że zwężenie dowolnego punktu $P \in \mathsf{S}$ jest punktem zbioru S_0, tak więc skończoność zbioru S równoważna jest skończoności zbioru S_0. Ale zbiór S_0 jest skończony, gdyż - na mocy twierdzenie 1.2.1 - punktów stopnia nie większego od n w ciele $\mathbb{F}_q(x)$ jest tyle, ile wielomianów z pierścienia $\mathbb{F}_q[X]$ stopnia nie większego od n, a tych jest oczywiście skończona liczba. *QED*

Lemat ten wykorzystamy do dowodu następującego twierdzenia:

TWIERDZENIE 3.1.1. *Grupa Piccarda $\mathcal{C}^0_{\mathbb{F}}$ ciała funkcji algebraicznych $F/\mathbb{F}_q$ jest grupą skończoną.*

D o w ó d : Korzystając z twierdzenia 1.1.5 możemy stwierdzić, że w ciele F istnieje co najmniej jeden punkt, a zatem istnieje też dywizor stopnia nie mniejszego od rodzaju ciała. Niech więc $B \in \mathcal{D}_F$ oraz $\mathsf{deg}\, B = n \geqslant g$. Oznaczmy ponadto przez:

$$\mathcal{C}^n_F = \{[A] \in \mathcal{C}_F : \mathsf{deg}\,[A] = n\}$$

zbiór klas dywizorów stopnia n. Zdefiniujmy odwzorowanie $\Phi : \mathcal{C}^0_F \to \mathcal{C}^n_F$ wzorem:

$$\Phi([A]) = [A + B] \text{ dla } A \in \mathcal{C}^0_F$$

Bez trudu sprawdzamy, że tak określona funkcja jest bijekcją, a zatem dla pokazania skończoności grupy $\mathcal{C}^0_F$ potrzeba i wystarczy wykazać skończoność zbioru $\mathcal{C}^n_F$.

Pokażemy, że dla dowolnie wybranej klasy dywizorów $[C] \in \mathcal{C}^n_F$ istnieje dywizor $A \in [C]$ nieujemny, $A \geqslant 0$. Istotnie, ustalmy klasę $[C] \in \mathcal{C}^n_F$ i niech $C \in [C]$ będzie jej reprezentantem. Wobec twierdzenia 1.3.2:

$$\mathsf{dim}\, C \geqslant \mathsf{deg}\, C + 1 - g$$

Ponieważ stopień klasy dywizorów $\deg[C] = n \geqslant g$ i - z definicji - równy jest stopniowi dywizora $\deg C$, więc $\dim C \geqslant 1$. Zauważmy dalej, że:

$$(\mathcal{L}(C) \neq \{0\}) \Longleftrightarrow \bigvee_{A \in \mathcal{D}_F} (A \sim C \wedge A \geqslant 0)$$

Załóżmy, że $\mathcal{L}(C) \neq \{0\}$. Wobec tego - z definicji przestrzeni $\mathcal{L}(C)$ - istnieje element $x \in F$ taki, że $(x) \geqslant -C$, czyli $(x) + C \geqslant 0$. Zatem dywizor $A = (x) + C$ jest nieujemny i równoważny z dywizorem C.

Na odwrót, niech $A \in \mathcal{D}_F$ będzie nieujemnym dywizorem równoważnym z C. Oznacza to, że istnieje również niezerowy element $x \in F$ taki, że $A = (x) + C$. Skoro A jest nieujemny, to $(x) + C \geqslant 0$, czyli $(x) \geqslant -C$, a zatem $x \in \mathcal{L}(C) \setminus \{0\}$.

Wobec lematu 3.1.1 dywizorów dodatnich stopnia n jest skończenie wiele, a więc również klas $[C] \in \mathcal{C}_F^n$ może być tylko skończona liczba, co w połączeniu z wcześniejszymi spostrzeżeniami kończy dowód. *QED*

Definicja 3.1.1. **Liczbą klas** *ciała funkcji algebraicznych $F/\mathbb{F}_q$ nazywamy rząd grupy Piccarda i oznaczamy symbolem h_F lub po prostu h.*

Zmierzamy do zdefiniowania funkcji dzeta Riemanna ciała funkcji algebraicznych. Będzie to pewien szereg potęgowy o współczynnikach wyrażających moc zbioru nieujemnych dywizorów określonego stopnia. Zanim to zrobimy, musimy sprawdzić, iż faktycznie dywizorów takich jest skończenie wiele i podać jakiś sposób wyznaczania ich liczby. Zdefiniujmy w tym celu liczbę naturalną $\partial > 0$ wzorem:

$$\partial = \min\{\deg A : A \in \mathcal{D}_F \wedge \deg A > 0\}$$

oraz ciąg $(A_n)_{n\in\mathbb{N}} \in \mathbb{N}^{\mathbb{N}}$ o wyrazach:

$$A_n = |\{A \in \mathcal{D}_F : A \geqslant 0 \ \deg A = n\}| \text{ dla } n \in \mathbb{N}$$

Lemat 3.1.2. *Przy powyższych oznaczeniach:*

(1) *Jeśli $\partial \nmid n$, to $A_n = 0$*
(2) *Dla ustalonej klasy dywizorów $[C] \in \mathcal{C}_{\mathbb{F}}$:*

$$|\{A \in [C] : A \geqslant 0\}| = \frac{1}{q-1}(q^{dim[C]} - 1)$$

(3) *Jeśli $\partial | n$ i $n > 2g - 2$, to:*

$$A_n = \frac{h}{q-1}(q^{n+1-g} - 1)$$

D o w ó d : (1) Bez trudu sprawdzamy, że odwzorowanie $\deg : \mathcal{D}_F \to \mathbb{Z}$ jest homomorfizmem grup abelowych. Tak więc dla udowodnienia, że stopień dowolnego dywizora nieujemnego jest wielokrotnością liczby ∂ (a więc w szczególności, że nie istnieją dywizory, których stopień nie byłby podzielny przez liczbę ∂) potrzeba i wystarcza zauważyć, że podgrupa $\deg(\{A \in \mathcal{D}_F : A \geqslant 0\})$ grupy $\mathbb{Z}$ jest cykliczna i generowana przez ∂.

Istotnie, niech $A_0 \in \mathcal{D}_F$ będzie dywizorem nieujemnym stopnia ∂. Ustalmy liczbę $n \in \mathbb{N}$, $n > \partial$ niepodzielną przez ∂ i dla dowodu nie wprost przypuśćmy, że wybraliśmy dywizor nieujemny $A \in \mathcal{D}_F$ stopnia n. Wykonując dzielenie z resztą $\deg A$ przez ∂ otrzymujemy:

$$\deg A = r \cdot \partial + s, \text{ gdzie } r \in \mathbb{N},\ 0 < s < \partial$$

Zatem dywizor $A - r \cdot A_0$ jest dywizorem nieujemnym stopnia s mniejszego od ∂, co jest sprzeczne z definicją liczby ∂.

(2) Ustalmy klasę $[C] \in \mathcal{C}_F$ i niech C będzie jej reprezentantem. Argumentując podobnie jak w dowodzie twierdzenia 3.1.1 stwierdzamy, że:

$$\bigwedge_{A \in [C]} \left((A \geqslant 0) \iff \left(\bigvee_{x \in F} (x \in \mathcal{L}(C) \setminus \{0\} \wedge A = (x) + C) \right) \right)$$

Tak więc dywizory nieujemne z klasy $[C]$ pozostają we wzajemnie jednoznacznej odpowiedniości z dywizorami głównymi elementów niezerowych przestrzeni $\mathcal{L}(C)$. Ponadto moc zbioru $\mathcal{L}(C)\setminus\{0\}$ równa jest $q^{\dim C}-1$ i - z definicji waluacji dyskretnej - dowolne dwa elementy leżą w tym samym dywizorze głównym tylko wtedy, gdy jeden powstaje z drugiego przez pomnożenie przez niezerową stałą z ciała $\mathbb{F}_q$. Zatem dywizorów głównych elementów niezerowych przestrzeni $\mathcal{L}(C)$ jest $\frac{1}{q-1}(q^{\dim [C]}-1)$.

(3) Ustalmy liczbę $n > 2g$ podzielną przez ∂. Znowu argumentując podobnie jak w dowodzie twierdzenia 3.1.1 stwierdzamy, że klas dywizorów stopnia n jest dokładnie h, gdzie h jest liczbą klas ciała F. Oznaczmy przez $[C_1], \ldots, [C_h]$ wszystkie takie klasy. Korzystając z udowodnionej już części twierdzenia oraz tezy (2) twierdzenia 1.3.3 mamy więc:

$$|\{A \in [C_j] : A \geqslant 0\}| = \frac{1}{q-1}(q^{\dim C_j} - 1) = \frac{1}{q-1}(q^{n+1-g} - 1)$$

dla $j \in \{1, \ldots, h\}$. Dalej, ponieważ każdy dywizor stopnia n leży w dokładnie jednej z klas $[C_1], \ldots, [C_h]$, otrzymujemy:

$$A_n = \sum_{j=1}^{h} |\{A \in [C_j] : A \geqslant 0\}| = \frac{h}{q-1}(q^{n+1-g} - 1)$$

co kończy dowód. *QED*

Definicja 3.1.2. *Przy wprowadzonych wcześniej oznaczeniach funkcję* $Z : \mathbb{C} \to \mathbb{C}$ *daną wzorem:*

$$Z(t) = Z_F(t) = \textstyle\sum_{n=0}^{\infty} A_n t^n, \text{ dla } t \in \mathbb{C}$$

zwiemy **funkcją dzeta Riemanna** *ciała funkcji algebraicznych* F.

Przekonaliśmy się, że wszystkie współczynniki A_n są skończone oraz "większość" równa jest zeru, część z nich można zaś - znając rodzaj ciała i jego liczbę klas - stosunkowo łatwo wyliczyć w przypadku odpowiednio dużego n. Problemem może się wydawać policzenie pozostałych współczynników, jednak następne twierdzenia pokażą, iż jest to problem pozorny - w istocie policzenie ich też nie nastręcza większych trudności. Ponadto okaże się, że liczba ∂ równa jest w istocie 1, co w oczywisty sposób uprości dotychczasowe rozważania. W związku z - co trzeba przyznać - dosyć zawikłaną definicją funkcji dzeta pojawia się naturalne pytanie, czy funkcja taka jest dobrze określona, tj. czy definiujący ją szereg jest zbieżny. Odpowiedzi na nie udziela kolejne twierdzenie.

Twierdzenie 3.1.2. *Przy powyższych oznaczeniach funkcja* $Z(t)$ *jest zbieżna dla* $|t| < q^{-1}$. *Dokładniej, dla* $|t| < q^{-1}$*:*

(1) *Jeśli rodzaj ciała* $g = 0$*, to:*

$$Z(t) = \frac{1}{q-1}\left(\frac{q}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}\right)$$

(2) *Jeśli rodzaj ciała $g \geqslant 1$, to:*

$$Z(t) = F(t) + G(t)$$

gdzie:

$$F(t) = \frac{1}{q-1} \sum_{0 \leqslant \deg[C] \leqslant 2g-2} q^{\dim[C]} t^{\deg[C]}$$

oraz:

$$G(t) = \frac{h}{q-1}(q^{1-g}(qt)^{2g-2+\partial} \frac{1}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}})$$

D o w ó d : (1) Załóżmy, że rodzaj ciała równy jest zeru. Zauważmy, że w takim wypadku liczba klas równa jest 1 - dokładniej, każdy dywizor stopnia zero jest dywizorem głównym.

Istotnie, dla ustalonego dywizora A stopnia zero, wobec tezy (2) twierdzenia 1.3.3 mamy:

$$\mathsf{dim}\, A = \mathsf{deg}\, A + 1 - g = 1$$

Zatem z definicji przestrzeni $\mathcal{L}(A)$ istnieje niezerowy element $a \in F$ taki, że $(x) \geqslant -A$. Ponieważ poza tym, wobec tezy (2) twierdzenia 1.1.6, dywizor główny elementu x, (x), jest stopnia zero, więc $A = -(x)$. Korzystając jeszcze z definicji waluacji $A = (x^{-1})$.

Teraz, zakładając, że $|qt| < 1$, wystarczy policzyć:

$$\begin{aligned}
\sum_{n=0}^{\infty} A_n t^n &= \sum_{n=0}^{\infty} A_{\partial n} t^{\partial n} = \sum_{n=0}^{\infty} \frac{1}{q-1}(q^{\partial n+1} - 1)t^{\partial n} = \\
&= \frac{1}{q-1}(q \sum_{n=0}^{\infty} (qt)^{\partial n} - \sum_{n=0}^{\infty} t^{\partial n}) = \\
&= \frac{1}{q-1}(\frac{q}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}})
\end{aligned}$$

(2) Wykonując obliczenia podobne jak w punkcie (1) mamy:

$$\begin{aligned}
\sum_{n=0}^{\infty} A_n t^n &= \sum_{\deg[C] \geqslant 0} |\{A \in [C] : A \geqslant 0\}| t^{\deg[C]} = \\
&= \sum_{\deg[C] \geqslant 0} \frac{q^{\dim[C]} - 1}{q-1} t^{\deg[C]} = \\
&= \frac{1}{q-1} \sum_{0 \leqslant \deg[C] \leqslant 2g-2} q^{\dim[C]} t^{\deg[C]} + \\
&+ \frac{1}{q-1} \sum_{\deg[C] > 2g-2} q^{\deg[C]+1-g} t^{\deg[C]} + \\
&- \frac{1}{q-1} \sum_{\deg[C] \geqslant 0} t^{\deg[C]} = F(t) + G(t)
\end{aligned}$$

gdzie:

$$F(t) = \frac{1}{q-1} \sum_{0 \leqslant \deg[C] \leqslant 2g-2} q^{\dim[C]} t^{\deg[C]}$$

oraz:

$$\begin{aligned}(q-1)G(t) &= \sum_{n=\frac{2g-2}{\partial}+1} hq^{n\partial+1-g}t^{n\partial} - \sum_{n=0}^{\infty} ht^{n\partial} = \\ &= hq^{1-g}(qt)^{2g-2+\partial}\frac{1}{1-(qt)^{\partial}} - h\frac{1}{1-t^{\partial}}\end{aligned}$$

co kończy dowód. *QED*

Wniosek 3.1.1. *Funkcję dzeta można rozszerzyć na całą płaszczyznę zespoloną poprzez dodanie zwykłego bieguna w punkcie* $t = 1$.

D o w ó d : Jest to oczywiste, gdyż taki biegun ma funkcja $\frac{1}{1-t^{\partial}}$. *QED*

Funkcja dzeta już przez swą definicję nasuwa analogie do znanej funkcji ζ Riemanna. Nie jest to oczywiście przypadek - więcej takich podobieństw poznamy później, najważniejsze z nich dotyczy potwierdzenia hipotezy Riemanna. Tymczasem sformułujmy twierdzenie podobne do wyniku Eulera, znanego z teorii funkcji analitycznych. Potrzebne nam będzie pojęcie produktu:

$$\prod_{i=1}^{\infty}(1+a_i)$$

w którym $(a_i)_{i\in\mathbb{N}} \in \mathbb{C}^{\mathbb{N}}$ jest ciągiem liczb zespolonych. Przypomnijmy, że produkt nazywamy **zbieżnym**, jeżeli:

$$\lim_{n\to\infty}\prod_{i=1}^{n}(1+a_i) = a \neq 0$$

oraz **bezwzględnie zbieżnym**, gdy:

$$\sum_{i=1}^{\infty}|a_i| < \infty$$

Pokazuje się, że każdy produkt bezwzględnie zbieżny jest zbieżny (por. [**9**] str. 197 - 199).

Twierdzenie 3.1.3. (o reprezentacji przez produkt Eulera) *Przy wcześniejszych oznaczeniach, dla* $|t| < q^{-1}$ *funkcja dzeta może być przedstawiona jako bezwzględnie zbieżny produkt:*

$$Z(t) = \prod_{P\in\mathbb{P}_F}(1-t^{\deg P})^{-1}$$

W szczególności $Z(t) \neq 0$ *dla* $|t| < q^{-1}$

D o w ó d : Pokażemy najpierw, że produkt $\prod_{P\in\mathbb{P}_F}(1-t^{\deg P})^{-1}$ jest bezwzględnie zbieżny dla $|t| < q^{-1}$. Istotnie, korzystając z twierdzenia 3.1.2, otrzymujemy:

$$\sum_{P\in\mathbb{P}_F}|t|^{\deg P} \leqslant \sum_{n=0}^{\infty} A_n|t|^n < \infty$$

Pozostaje wykazać równość funkcji. Mamy:

$$\prod_{P\in\mathbb{P}_F}(1-t^{\deg P})^{-1} = \prod_{P\in\mathbb{P}_F}\sum_{n=0}^{\infty}t^{\deg(nP)} =$$

$$= \sum_{A\in\mathcal{D}_F, A\geqslant 0} t^{\deg A} = \sum_{n=0}^{\infty} A_n t^n = Z(t)$$

co należało dowieść. QED

Zanim przejdziemy do dalszych rozważań podamy kilka ogólnych własności rozszerzeń ciał stałych w przypadku ciał funkcji algebraicznych nad skończonymi ciałami stałych. Rozważać będziemy następujące rozszerzenia:

$$\overline{F} := F\overline{F}_q \supseteq F \text{ oraz } \overline{\mathbb{F}}_q \supseteq \mathbb{F}_q$$

gdzie $\overline{F}_q$ oznacza algebraiczne domknięcie ciała $\mathbb{F}_q$. Wobec tego możemy mówić o algebraicznym rozszerzeniu ciała funkcji algebraicznych $\overline{F}/\overline{F}_q \supseteq F/\mathbb{F}_q$. Dalej, z kursowego wykładu algebry wiemy, że $\mathbb{F}_{q^r}$ jest jedynym rozszerzeniem stopnia r ciała $\mathbb{F}_q$ (por. [**3**] przykład II.1.4.6), będziemy więc rozważać następujące, jednoznacznie określone wieże ciał:

$$\overline{F} \supseteq F_r = F\mathbb{F}_{q^r} \supseteq F \text{ oraz } \overline{\mathbb{F}}_q \supseteq \mathbb{F}_{q^r} \supseteq \mathbb{F}_q$$

dla $r \geqslant 1$. Możemy zatem mówić o algebraicznym rozszerzeniu ciała funkcji algebraicznych $F_r/\mathbb{F}_{q^r} \supseteq F/\mathbb{F}_q$. Podstawowe własności tak zdefiniowanych rozszerzeń ujmuje następujący lemat.

LEMAT 3.1.3. *Przy powyższych oznaczeniach*

(1) *$F_r \supset F$ jest rozszerzeniem cyklicznym stopnia r. Grupa Galois tego rozszerzenia generowana jest przez automorfizm Frobeniusa $\sigma : \mathbb{F}_r \to \mathbb{F}_r$ dany wzorem:*

$$\sigma(a) = a^q \text{ dla } a \in \mathbb{F}_{q^r}$$

(2) *$\mathbb{F}_{q^r}$ jest ciałem stałych dla F_r.*
(3) *$F_r/\mathbb{F}_{q^r}$ ma ten sam rodzaj co $F/\mathbb{F}_q$.*
(4) *Niech $P \in \mathbb{P}_F$ będzie punktem ciała F stopnia m. Wówczas:*

$$Con_{F_r/F}(P) = P'_1 + \ldots + P'_d$$

gdzie $d = NWD(m, r)$ oraz $P'_1, \ldots, P'_d$ są wszystkimi, parami różnymi punktami ciała F_r leżącymi nad P, stopnia $\frac{m}{d}$.

Dowód lematu poprzedzimy jeszcze jednym lematem:

LEMAT 3.1.4. *Niech F/K będzie ciałem funkcji algebraicznych, a α niech będzie elementem algebraicznym nad K. Wówczas:*

$$[K(\alpha) : K] = [F(\alpha) : F]$$

D o w ó d : Jako, że $F \supseteq K$, nierówność $[K(\alpha) : K] \geqslant [F(\alpha) : F]$ jest oczywista. Aby pokazać nierównośc przeciwną - i tym samym zakończyć dowód - zauważmy, że wielomian minimalny $\phi(X) \in K[X]$ elementu α jest nierozkładalny w pierścieniu $F[X]$.

Istotnie, przypuśćmy dla dowodu nie wprost, że $\phi(X) = f(X) \cdot g(X)$ dla wielomianów $f(X), g(X) \in F[X]$ stopnia nie mniejszego od 1. Możemy przy tym założyć, że $\phi(X), f(X), g(X)$ są wielomianami unormowanymi. Oznaczmy przez Φ ciało algebraicznie domknięte, zawierające ciało F (a więc i K). W takim razie

dowolny pierwiastek wielomianu $f(X)$ lub $g(X)$ jest też pierwiastkiem wielomianu $\phi(X)$, a więc elementem algebraicznym nad ciałem K. Stąd wszystkie współczynniki wielomianów $f(X)$ i $g(X)$ są algebraiczne nad ciałem K, jako że są wartościami wielomianów o współczynnikach algebraicznych. Z drugiej strony wszystkie te współczynniki są elementami ciała F i skoro ciało K jest algebraicznie domknięte w ciele F, to $f(X), g(X) \in K[X]$, co doprowadza nas do sprzeczności. *QED*

D o w ó d l e m a t u 3.1.3 : (1) Pokażemy najpierw, że rozszerzenie $\mathbb{F}_{q^r} \supseteq \mathbb{F}_q$ jest proste, czyli $\mathbb{F}_{q^r} = \mathbb{F}_q(\alpha)$. Istotnie, jak wiadomo grupa multyplikatywna ciała skończonego jest cykliczna (por. [**3**], przykład II.2.4.2). Niech więc:

$$< \alpha >= \{1, 2, \ldots, q^r\}$$

Zauważmy, że $\mathbb{F}_{q^r} = \mathbb{F}_q(\alpha)$. Inkluzja $\mathbb{F}_{q^r} \supseteq \mathbb{F}_q(\alpha)$ jest oczywista, aby zaś przekonać się o prawdziwości inkluzji przeciwnej, ustalmy element $a \in \mathbb{F}_{q^r}$. Jeżeli jest to element zerowy, to naturalnie $a \in \mathbb{F}_q(\alpha)$, a jeżeli nie, to jako element grupy multyplikatywnej jest potęgą elementu α, tym bardziej więc należy do $\mathbb{F}_q(\alpha)$.

Pokażemy, że rozszerzenie $F_r \supseteq F$ jest proste, dokładniej, że $F_r = F(\alpha)$, gdzie α jest zdefiniowanym przed chwilą elementem. Podobnie jak wcześniej, inkluzja $F_r \supseteq F(\alpha)$ jest oczywista, a w celu wykazania inkluzji przeciwnej, ustalmy element $x \in F_r$ wybrany ze zbioru generatorów kompozytu $F\mathbb{F}_q(\alpha)$. Niech więc $x = a \cdot b$, gdzie $a \in F$ i $b \in \mathbb{F}_q(\alpha)$. W takim razie $b = x_0 + x_1\alpha + \ldots + x_r\alpha^r$, gdzie $x_i \in \mathbb{F}_q \subseteq F$, $i \in \{0, \ldots, r\}$, zatem $x = a(x_0 + x_1\alpha + \ldots + x_r\alpha^r) \in F(\alpha)$.

Pokażemy, że grupa Galois rozszerzenia $F_r \supseteq F$ jest cykliczna rzędu r. Jak wiemy z kursowego wykładu algebry (por. [**3**], przykład III.1.4.2), rozszerzenie $\mathbb{F}_{q^r} \supseteq \mathbb{F}_q$ jest rozszerzeniem cyklicznym stopnia r, którego grupa Galois jest generowana przez automorfizm Frobeniusa $\sigma_0 : \mathbb{F}_{q^r} \to \mathbb{F}_{q^r}$ dany wzorem $\sigma_0(a) = a^q$, dla $a \in \mathbb{F}_{q^r}$. Oznaczmy przez $\sigma : F_r \to F_r$ przedłużenie automorfizmu Frobieniusa na ciało F_r:

$$\sigma(x) = \begin{cases} x & \text{jeżeli } x \in F_r \setminus \mathbb{F}_{q^r} \\ \sigma_0(x) & \text{jeżeli } x \in \mathbb{F}_{q^r} \end{cases}$$

Odwzorowanie to również nazywać będziemy automorfizmem Frobeniusa i tam, gdzie nie prowadzi to do sprzeczności, nie będziemy robili rozróżnienia między σ a σ_0. Dla elementu $x \in F_r$, $x = a_0 + a_1\alpha + \ldots + a_r\alpha^r$, gdzie $a_i \in F$, $i \in \{0, \ldots, r\}$ i dowolnego automorfizmu $\phi \in \mathsf{Gal}\,(F_r/F)$ mamy więc:

$$\begin{aligned} \phi(x) &= \phi(a_0 + a_1\alpha + \ldots + a_r\alpha^r) = a_0 + a_1\phi(\alpha) + \ldots + a_r\phi(\alpha^r) = \\ &= a_0 + a_1\sigma^{n_0}(\alpha) + \ldots + a_r\sigma^{n_0}(\alpha^r) = \sigma^{n_0}(a_0 + a_1\alpha + \ldots + a_r\alpha^r) = \\ &= \sigma^{n_0}(x) \end{aligned}$$

gdzie $n_0 \in \{0, \ldots, r\}$ jest pewną liczbą naturalną. Tak więc istotnie grupa $\mathsf{Gal}\,(F_r/F)$ jest cykliczna rzędu r, a jej generatorem jest σ.

Aby przekonać się, że rozszerzenie $F_r \supseteq F$ jest Galois, skorzystamy z lematu 3.1.4:

$$[F_r : F] = [F(\alpha) : F] = [\mathbb{F}_q(\alpha) : \mathbb{F}_q] = [\mathbb{F}_{q^r} : \mathbb{F}_q] = r$$

(2) i (3) wynikają bezpośrednio z tez (1) i (3) twierdzenia 2.2.1.

(4) Ustalmy punkt $P \in \mathbb{P}_F$ stopnia m oraz punkt $P' \in \mathbb{P}_{F_r}$ leżący nad punktem P, $P'|P$. Przyjmijmy też oznaczenie $d = NWD(m, r)$. Ponieważ - wobec tezy (3) twierdzenia 2.2.1 - rozszerzenie $F_r \supseteq F$ jest nierozgałęzione, więc indeks rozgałęzienia $e(P'|P) = 1$. Ponadto - aplikując tezę (5) twierdzenia 2.2.1 - ciało reszt $F_{r\,P'}$ punktu P' jest iloczynem kompozycyjnym $\mathbb{F}_{q^r}$ i ciała reszt F_P punktu P,

$F_{r\,P'} = \mathbb{F}_{q^r} F_P$. Z definicji ciało F_P jest rozszerzeniem stopnia m ciała $\mathbb{F}_q$, a więc jest izomorficzne z ciałem $\mathbb{F}_{q^m}$ (por. [**3**] przykład II.1.4.6). Jeżeli więc oznaczymy przez $l = NWW(m,r)$, to:

$$F_{r\,P'} = \mathbb{F}_{q^r}\,\mathbb{F}_{q^m} = \mathbb{F}_{q^l}$$

Stąd, jako że $l \cdot d = m \cdot r$, otrzymujemy równość:

$$\mathsf{deg}\, P' = [\mathbb{F}_{q^l} : \mathbb{F}_{q^r}] = \frac{m}{d}$$

Korzystając z tezy (4) twierdzenia 2.2.1 widzimy, że $\mathsf{deg}\,(\mathsf{Con}_{F_r/F}(P)) = \mathsf{deg}\, P = m$. Ostatecznie więc:

$$Con_{F_r/F}(P) = P'_1 + \ldots + P'_d$$

gdzie $d = NWD(m,r)$ oraz $P'_1, \ldots, P'_d$ są wszystkimi, parami różnymi punktami ciała F_r leżącymi nad P, stopnia $\frac{m}{d}$. *QED*

Wykorzystamy teraz powyższy lemat do znalezienia związku z funkcją dzeta ciała F i funkcją dzeta ciała F_r. Potrzebna będzie nam do tego pewna tożsamość wielomianowa, którą pozostawimy tu bez dowodu. Mianowicie, jeżeli $m \geqslant 1$ oraz $r \geqslant 1$ są liczbami naturalnymi i d oznacza ich największy wspólny dzielnik, to:

$$(1 - t^{\frac{mr}{d}})^d = \prod_{\xi^r=1} (1 - (\xi t)^m)$$

Twierdzenie 3.1.4. *Jeżeli $Z(t)$ i, odpowiednio, $Z_r(t)$ oznaczają funkcję dzeta ciała F i F_r, to:*

$$Z_r(t^r) = \prod_{\xi^r=1} Z(\xi t)$$

D o w ó d : Ponieważ - zgodnie z twierdzeniem 3.1.2 - szereg definiujący funkcję dzeta zbieżny jest dla $|t| < q^{-1}$, więc wystarczy ograniczyć się do przypadku liczb t wybranych ze wspomnianego koła zbieżności. Bezpośrednio z twierdzeń 3.1.3 i 2.1.2 mamy:

$$Z_r(t^r) = \prod_{P' \in \mathbb{P}_{F_r}} \left(1 - t^{r \deg P'}\right)^{-1} = \prod_{P \in \mathbb{P}_F} \prod_{P' | P} \left(1 - t^{r \deg P'}\right)^{-1}$$

Zajmijmy się wewnętrznym produktem w powyższym wyrażeniu. Ustalmy więc punkt $P \in \mathbb{P}_F$ stopnia m i niech d oznacza największy wspólny dzielnik r i m. Korzystając kolejno z tezy (4) twierdzenia 2.2.1 i tezy (4) lematu 3.1.3 mamy:

$$m = \mathsf{deg}\, P = \mathsf{deg}\, \left(\mathsf{Con}_{F_r/F}(P)\right) = \mathsf{deg}\,(P'_1 + \ldots + P'_d)$$

gdzie $P'_1, \ldots, P'_d$ są wszystkimi, parami różnymi punktami ciała F_r leżącymi nad P, stopnia $\frac{m}{d}$. Wykorzystując wspomnianą tożsamość wielomianową mamy więc:

$$\begin{aligned} \prod_{P' | P} \left(1 - t^{r \deg P'}\right) &= \left(1 - t^{\frac{rm}{d}}\right)^d = \\ &= \prod_{\xi^r=1} (1 - (\xi t)^m) = \\ &= \prod_{\xi^r=1} \left(1 - (\xi t)^{\deg P}\right) \end{aligned}$$

Stąd:

$$Z_r(t^r) = \prod_{P \in \mathbb{P}_F} \prod_{\xi^r=1} \left(1 - (\xi t)^{\deg P}\right)^{-1} = \prod_{\xi^r=1} Z(\xi t)$$

co kończy dowód. *QED*

Teraz możemy bez trudu udowodnić zapowiadane wcześniej dwa twierdzenia, ułatwiające nam opis funkcji dzeta.

TWIERDZENIE 3.1.5. (SCHMIDT'A) *Przy wcześniejszych oznaczeniach* $\partial = 1$

D o w ó d : Na podstawie tezy (1) lematu 3.1.2 ∂ dzieli stopień każdego dywizora ciała F. Wybierzmy liczbę $\xi \in \mathbb{C}$ taką, że $\xi^{\partial} = 1$. Korzystając z twierdzenia 3.1.3 otrzymujemy:

$$Z(\xi t) = \prod_{P \in \mathbb{P}_F} \left(1 - (\xi t)^{\deg P}\right)^{-1} = \prod_{P \in \mathbb{P}_F} \left(1 - t^{\deg P}\right)^{-1} = Z(t)$$

Stosując więc twierdzenie 3.1.4 otrzymujemy:

$$Z_{\partial}(t^{\partial}) = (Z(t))^{\partial}$$

Dalej, dzięki wnioskowi 3.1.1, funkcja $Z_{\partial}(t^{\partial})$ ma zwykły biegun w punkcie $t = 1$. Ponadto funkcja $(Z(t))^{\partial}$ ma biegun rzędu ∂ w punkcie $t = 1$. Dzięki otrzymanej równości funkcji $Z_{\partial}(t^{\partial})$ i $(Z(t))^{\partial}$ widzimy, że $\partial = 1$. *QED*

TWIERDZENIE 3.1.6. *Przy powyższych oznaczeniach;*

(1) *Każde ciało funkcji algebraicznych* $F/\mathbb{F}_q$ *rodzaju 0 jest ciałem funkcji wymiernych o funkcji dzeta:*

$$Z(t) = \frac{1}{(1-t)(1-qt)}$$

(2) *Jeśli* $\mathbb{F}/\mathbb{F}_q$ *jest rodzaju* $g \geqslant 1$*, to:*

$$Z(t) = F(t) + G(t)$$

gdzie:

$$F(t) = \frac{1}{q-1} \sum_{0 \leqslant \deg[C] \leqslant 2g-2} q^{\dim[C]} t^{\deg[C]}$$

oraz:

$$G(t) = \frac{h}{q-1}\left(q^g t^{2g-1} \frac{1}{1-qt} - \frac{1}{1-t}\right)$$

D o w ó d : To, że ciało funkcji algebraicznych o rodzaju zero, posiadające dywizor stopnia 1 jest ciałem funkcji wymiernych, jest treścią tezy (3) twierdzenia 1.3.3. Pozostałe tezy otrzymujemy podstawiając $\partial = 1$ w twierdzeniu 3.1.2. *QED*

Przechodzimy teraz do zdefiniowania ważnego pojęcia L-wielomianu ciała funkcji algebraicznych i poznania kilku jego własności. Pozwala on między innymi dyskutować liczbę punktów stopnia 1 danego ciała funkcji algebraicznych. Wielomian ten odegra kluczową rolę w twierdzeniu Hasse'go - Weil'a, które można wypowiedzieć - i tak też zrobimy - używając wyłącznie pierwiastków L-wielomianu.

DEFINICJA 3.1.3. *Wielomian* $L(t) = L_F(t) = (1-t)(1-qt)Z(t)$ *nazywamy* **L-wielomianem** *ciała* $F/\mathbb{F}_q$*.*

Przed omówieniem własności L-wielomianu podamy jeszcze pomocnicze twierdzenie, przedstawiające równanie funkcyjne spełniane przez funkcję dzeta.

TWIERDZENIE 3.1.7. (RÓWNANIE FUNKCYJNE FUNKCJI DZETA) *Funkcja dzeta ciała funkcji algebraicznych* $F/\mathbb{F}_q$ *spełnia równanie:*

$$Z(t) = q^{g-1} t^{2g-2} Z\left(\frac{1}{qt}\right)$$

D o w ó d : Jeżeli rodzaj ciała g równy jest zeru, to tezę otrzymujemy bezpośrednio z twierdzenia 3.1.6. Załóżmy więc, że rodzaj g jest nie mniejszy od 1 i - na podstawie twierdzenia 3.1.6 - przedstawmy funkcję dzeta w postaci:

$$Z(t) = F(t) + G(t)$$

gdzie:

$$F(t) = \frac{1}{q-1} \sum_{0 \leqslant \deg [C] \leqslant 2g-2} q^{\dim [C]} t^{\deg [C]}$$

oraz:

$$G(t) = \frac{h}{q-1} \left(q^g t^{2g-1} \frac{1}{1-qt} - \frac{1}{1-t} \right)$$

Niech W będzie dywizorem kanonicznym ciała F. Korzystając z twierdzenia 1.3.2 i tezy (4) twierdzenia 1.3.3 otrzymujemy:

$$\begin{aligned}
(q-1)F(t) &= \sum_{0 \leqslant \deg [C] \leqslant 2g-2} q^{\dim [C]} t^{\deg [C]} = \\
&= \sum_{0 \leqslant \deg [C] \leqslant 2g-2} q^{\deg [C]+1-g+\dim [W-C]} t^{\deg [C]} = \\
&= q^{g-1} t^{2g-2} \sum_{0 \leqslant \deg [C] \leqslant 2g-2} q^{\deg [C]-(2g-2)+\dim [W-C]} t^{\deg [C]-(2g-2)} = \\
&= q^{g-1} t^{2g-2} \sum_{0 \leqslant \deg [C] \leqslant 2g-2} q^{\dim [W-C]} \left(\frac{1}{qt} \right)^{\deg [W-C]} = \\
&= q^{g-1} t^{2g-2} (q-1) F(\frac{1}{qt})
\end{aligned}$$

Podobnie dla funkcji $G(t)$:

$$\begin{aligned}
q^{g-1} t^{2g-2} G\left(\frac{1}{qt}\right) &= \frac{h}{g-1} q^{g-1} t^{2g-2} \left(q^g \left(\frac{1}{qt} \right)^{2g-1} \frac{1}{1-q\frac{1}{qt}} - \frac{1}{1-\frac{1}{qt}} \right) = \\
&= \frac{h}{g-1} \left(\frac{1}{t} \frac{1}{1-\frac{1}{t}} - \frac{q^g t^{2g-1}}{qt\left(1-\frac{1}{qt}\right)} \right) = \\
&= G(t)
\end{aligned}$$

Po dodaniu stronami otrzymanych zależności otrzymujemy tezę. QED

Twierdzenie 3.1.8. *Przy powyższych oznaczeniach;*

(1) $L(t) \in \mathbb{Z}(t)$ *oraz* $\deg L(t) = 2g$
(2) $L(t) = q^g t^{2g} L(\frac{1}{qt})$
(3) $L(1) = h$
(4) *Jeśli* $L(t) = a_0 + a_1 t + \ldots + a_{2g} t^{2g}$, *to:*
   (a) $a_0 = 1$ *oraz* $a_{2g} = q^g$
   (b) $a_{2g-i} = q^{g-i} a_i$ *dla* $0 \leqslant i \leqslant g$
   (c) $a_1 = N - (q+1)$, *gdzie* N *oznacza liczbę punktów stopnia 1 ciała* F.
(5) $L(t)$ *ma następujący rozkład w pierścieniu* $\mathbb{C}[t]$*:*

$$L(t) = \prod_{i=1}^{2g} (1 - \alpha_i t)$$

przy czym współczynniki $\alpha_1, \ldots, \alpha_{2g}$ *są liczbami spełniającymi równości:*

$$\alpha_i^{m_i} + c^i_{m_i-1}\alpha_i^{m_i-1} + \ldots + c^i_1\alpha_i + c^i_0 = 0$$

dla $i \in \{1, \ldots, 2g\}$, $m_i \in \mathbb{N}$, $c^i_{m_i-1}, \ldots, c^i_0 \in \mathbb{Z}$, *które ponadto można dobrać w ten sposób, aby:*

$$\alpha_i\alpha_{g+i} = q$$

dla $i \in \{1, \ldots, g\}$

(6) *Jeżeli* $L_r(t)$ *oznacza* $L-$*wielomian ciała* $F_r/\mathbb{F}_{q^r}$, *to* $L_r(t)$ *ma następujący rozkład w pierścieniu* $\mathbb{C}[t]$*:*

$$L_r(t) = \prod_{i=1}^{2g}(1 - \alpha_i^r t)$$

przy czym współczynniki $\alpha_1, \ldots, \alpha_{2g}$ *są liczbami spełniającymi równości:*

$$\alpha_i^{m_i} + c^i_{m_i-1}\alpha_i^{m_i-1} + \ldots + c^i_1\alpha_i + c^i_0 = 0$$

dla $i \in \{1, \ldots, 2g\}$, $m_i \in \mathbb{N}$, $c^i_{m_i-1}, \ldots, c^i_0 \in \mathbb{Z}$, *które ponadto można dobrać w ten sposób, aby:*

$$\alpha_i\alpha_{g+i} = q$$

dla $i \in \{1, \ldots, g\}$

D o w ó d : Na początek zauważmy, że - zgodnie z twierdzeniem 3.1.6 - L faktycznie jest wielomianem, którego stopień nie przekracza dwukrotności rodzaju ciała. Zatem w przypadku, gdy $g = 0$, całe twierdzenie się trywializuje i dlatego zajmiemy się przypadkiem, gdy $g \geqslant 1$.

(1) Jak przed chwilą stwierdziliśmy, stopień L nie przekracza $2g$. Aby stwierdzić, że stopień ten jest równy $2g$ zauważymy, że współczynnik przy t^{2g} równy jest q^g, ale zrobimy to dopiero w punkcie (4).

(2) Teza ta wynika natychmiast z twierdzenia 3.1.7.

(3) Przyjmując notację twierdzenia 3.1.6 możemy napisać:

$$L(t) = (1-t)(1-qt)F(t) + \frac{h}{q-1}\left(q^g t^{2g-1}(1-t) - (1-qt)\right)$$

skąd wynika od razu, że $L(1) = h$.

(4) Niech $L(t) = a_0 + a_1 t + \ldots + a_{2g}t^{2g}$. Korzystając z udowodnionego już punktu (2) mamy:

$$L(t) = q^g t^{2g} L\left(\frac{1}{qt}\right) = \frac{a_{2g}}{q^g} + \frac{a_{2g-1}}{q^{g-1}}t + \ldots + q^g a_0 t^{2g}$$

skąd dostajemy natychmiast:

$$a_{2g-i} = q^{g-i}a_i, \text{ dla } i \in \{0, \ldots, g\}$$

Ponadto rozpisując wielomian L z definicji otrzymujemy:

$$L(t) = (1-t)(1-qt)\sum_{n=0}^{\infty} A_n t^n$$

skąd bez trudu wyliczamy:

$$a_0 = A_0 \text{ oraz } a_1 = A_1 - (q+1)A_0$$

i ponieważ - z definicji - $A_0 = 1$ oraz $A_1 = N$, więc ostatecznie:

$$a_0 = 1 \text{ oraz } a_1 = N - (q+1)$$

Porównując otrzymane wyniki, dostajemy na koniec:

$$a_{2g} = q^g a_0 = q^g$$

(5) Rozważmy pomiocniczy wielomian:

$$L^{\supset}(t) = t^{2g} L\left(\frac{1}{t}\right) = a_0 t^{2g} + a_1 t^{2g-1} + \ldots + a_{2g} = t^{2g} + a_1 t^{2g-1} + \ldots + q^g$$

gdzie $L(t) = a_0 + a_1 t + \ldots + a_{2g} t^{2g}$, przy czym skorzystaliśmy już z punktu (4). $L^{\supset}$ jest wielomianem unormowanym stopnia $2g$ o współczynnikach całkowitych, tak więc jego pierwiastki $\alpha_1, \ldots, \alpha_{2g} \in \mathbb{C}$ spełniają warunek:

$$\alpha_i^{m_i} + c^i_{m_i-1}\alpha_i^{m_i-1} + \ldots + c_1^i \alpha_i + c_0^i = 0$$

dla $i \in \{1, \ldots, 2g\}$, $m_i \in \mathbb{N}$, $c^i_{m_i-1}, \ldots, c^i_0 \in \mathbb{Z}$. Oczywiście $L^{\supset}(t) = \prod_{i=1}^{2g}(t - \alpha_i)$, więc:

$$L(t) = t^{2g} L^{\supset}\left(\frac{1}{t}\right) = \prod_{i=1}^{2g}(1 - \alpha_i t)$$

Tak więc $L(\alpha_i^{-1}) = 0$ dla $i \in \{1, \ldots, 2g\}$, więc pierwiastki wielomianu $L^{\supset}(t)$ są odwrotnościami pierwiastków $L(t)$. Zatem wobec udowodnionego już punktu (2):

$$L^{\supset}(\alpha) = 0 \iff L^{\supset}\left(\frac{q}{\alpha}\right) = 0$$

Pierwiastki $L^{\supset}$ możemy więc przepisać w postaci:

$$\alpha_1, \frac{q}{\alpha_1}, \ldots, \alpha_k, \frac{q}{\alpha_k}, q^{\frac{1}{2}}, \ldots, q^{\frac{1}{2}}, -q^{\frac{1}{2}}, \ldots, -q^{\frac{1}{2}}$$

gdzie $q^{\frac{1}{2}}$ występuje m razy, $-q^{\frac{1}{2}}$ występuje n razy i $m + n + 2k = 2g$. Korzystając z wypisanej jawnie postaci wielomianu $L^{\supset}(t)$ i wzorów Viete'a, dostajemy:

$$\alpha_1 \cdot \frac{q}{\alpha_1} \cdot \ldots \cdot \alpha_k \cdot \frac{q}{\alpha_k} \cdot \left(q^{\frac{1}{2}}\right)^m \cdot \left(-q^{\frac{1}{2}}\right)^n = q^g$$

Zatem n jest parzyste i skoro $n + m + 2k = 2g$, to również m jest parzyste i - zmieniając ewentualnie numerację - możemy założyć, że:

$$\alpha_i \cdot \alpha_{g+i} = q, \text{ dla } i \in \{1, \ldots, g\}$$

(6) Bezpośrednio z definicji L-wielomianu i twierdzenia 3.1.4 wyliczamy:

$$\begin{aligned} L_r(t^r) &= (1-t^r)(1-q^r t^r) Z_r(t^r) = (1-t^r)(1-q^r t^r) \prod_{\xi^r=1} Z(\xi t) = \\ &= (1-t^r)(1-q^r t^r) \prod_{\xi^r=1} \frac{L(\xi t)}{(1-\xi t)(1-q\xi t)} = \prod_{xi^r=1} L(xit) = \\ &= \prod_{i=1}^{2g} \prod_{\xi^r=1} (1 - \alpha_i \xi t) = \prod_{i=1}^{2g} (1 - \alpha_i^r t^r) \end{aligned}$$

co kończy dowód. *QED*

Paragraf ten zakończymy zapowiadanym już wnioskiem, który uściśla, w jaki sposób z postaci L-wielomianu można odczytywać informacje o liczbie punktów stopnia 1 danego ciała. Zdefiniujmy w tym celu liczby:

$$N(F) = N = |\{P \in \mathbb{P}_F : \mathsf{deg}\, P = 1\}|$$

$$N_r = N(F_r)$$

Wniosek 3.1.2. *Dla $r \geqslant 1$:*

$$N_r = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r$$

gdzie $\alpha_1, \ldots, \alpha_{2g} \in \mathbb{C}$ są odwrotnościami pierwiastków $L-$wielomianu, w szczególności:

$$N = q + 1 - \sum_{i=1}^{2g} \alpha_i$$

D o w ó d : Niech $L_r(t) = a_0 + a_1 t + \ldots + a_{2g} t^{2g}$ będzie L-wielomianem ciała F_r. Korzystając z twierdzenia 3.1.8 (4) $a_1 = N_r - (q^r + 1)$ Z drugiej strony, z tezy (6) tego samego twierdzenia, $L_r(t) = \prod_{i=1}^{2g}(1 - \alpha_i^r t)$, skąd bez trudu wyliczamy, że współczynnikiem przy t jest $-\sum_{i=1}^{2} g\alpha_i^r$. Porównując tę liczbę z a_1 otrzymujemy tezę. *QED*

2. Twierdzenie Hasse'go - Weil'a

Udowodnimy teraz najważniejszy rezultat niniejszej pracy, mianowicie twierdzenie Hasse'ego - Weil'a. Zostało ono sformułowane przez Emila Artina, natomiast pierwszy dowód, w przypadku ciał rodzaju 1, opublikował Hasse (por. [**8**]) w 1933 roku. Przypadek ciał dowolnego rodzaju został rozwikłany przez Weil'a (por. [**18**]). Prezentowany tutaj dowód pochodzi od Enrico Bombieri'ego (por. [**1**]).

Ustalmy liczbę naturalną (będącą potęgą liczby pierwszej) q i niech $F/\mathbb{F}_q$ będzie ciałem funkcji algebraicznych o rodzaju g. Niech:

$$\bigwedge_{n \in \mathbb{N}} (A_n = |\{A \in \mathcal{D}_F : A \geqslant 0 \wedge \deg A = n\}|)$$

oraz niech $Z_F : \mathbb{C} \to \mathbb{C}$ będzie funkcją dzeta ciała funkcji algebraicznych $F/\mathbb{F}_q$ daną wzorem:

$$Z_F(t) = \sum_{n=0}^{\infty} A_n t^n$$

zaś:

$$L_F(t) = (1-t)(1-qt)Z_F(t)$$

będzie L-wielomianem ciała funkcji algebraicznych F/F_q. Oznaczmy przez:

$$\alpha_1, \ldots, \alpha_{2g}$$

odwrotności pierwiastków L-wielomianu.

Twierdzenie 3.2.1. (Hasse'go - Weil'a) *Przy powyższych oznaczeniach:*

$$\bigwedge_{i \in \{1,\ldots,2g\}} (|\alpha_i| = \sqrt{q})$$

Zanim przejdziemy do dowodu, pokażemy prawdziwość dwóch lematów. Pierwszy dotyczy ogólnych własności grup i jest potrzebny głównie do wykazania drugiego z nich, przedstawiającego pewną konstrukcję rozszerzeń ciał, która okaże się kluczowym argumentem w dowodzie twierdzenia Hasse'go - Weil'a.

LEMAT 3.2.1. *Rozważmy grupę G' będącą produktem:*

$$G' =< \sigma > \times G$$

grupy cyklicznej $< \sigma >$ rzędu n i grupy G rzędu m, przy czym $m|n$. Niech $H \subseteq G'$ będzie taką podgrupą, że:

$$|H| = n \cdot e \text{ oraz } |H \cap G| = e$$

Wówczas istnieje dokładnie e podgrup $U \subseteq H$ takich, że:

$$U \text{ jest cykliczna rzędu } n \text{ oraz } U \cap G = \{1\}$$

D o w ó d : Na początek zauważmy, że z produktowej struktury grupy G' w oczywisty sposób wynika, iż każdy element λ grupy G' ma jednoznaczne przedstawienie w postaci $\lambda = \sigma^i \rho$, gdzie $i \in \{0, \dots, n\}$ oraz $\rho \in G$.

Teraz pokażemy, że w grupie G' istnieje dokładnie m rozłącznych podgrup cyklicznych U rzędu n takich, że $U \cap G = \{1\}$. Istotnie, ustalmy element $\tau \in G$ i rozważmy grupę cykliczną $< \sigma \cdot \tau > \subseteq G'$. Wobec struktury grupy G' widzimy, że $\tau \cdot \sigma = \sigma \cdot \tau$, rząd $r(\sigma) = n$ i $r(\tau)|m$, tak więc $r(\sigma \cdot \tau) = n$ (korzystamy tu ze znanych z kursu algebry własności rzędu grupy, por. [**16**] zadanie 53.(f)). Ponadto, korzystając z udowodnionego przedstawienia elementów grupy G', $< \sigma \cdot \tau > \cap G = \{1\}$ oraz $< \sigma \cdot \tau > \neq \sigma \cdot \tau'$ dla $\tau \neq \tau'$, $\tau, \tau' \in G$, co - ponieważ $|G| = m$ - kończy tę część dowodu.

W dalszym ciągu pokażemy, że grupa H zawiera dokładnie e podgrup cyklicznych o żądanych własnościach. Korzystając z pokazanej postaci elementów grupy G' oraz dyskutowanego już faktu przemienności elementów podgrupy $< \sigma >$ z elementami podgrupy G, bezpośrednio z definicji zauważamy, że G jest podgrupą normalną G'. Na mocy II twierdzenia Noether o izomorfizmie (por. [**16**] zadanie 144) mamy zatem, że $H/H \cap G \cong HG/G$. Stąd - skoro $|H| = ne$, $|H \cap G| = e$, $|G| = m$ i $|G'| = nm$ - otrzymujemy, iż $HG = G'$ oraz $H/H \cap G \cong G'/G \cong < \sigma >$. Wybierzmy zatem warstwę grupy $H/H \cap G$ rzędu n i niech $\lambda_0 \in H$ będzie jej reprezentantem. Zapiszmy λ_0 w postaci $\lambda_0 = \sigma^a \cdot \tau'$, gdzie $a \in \mathbb{Z}$ oraz $\tau' \in G$. Zauważmy, że $NWD(a, n) = 1$; istotnie, w przeciwnym wypadku istniałaby liczba $d \in \{1, \dots, n-1\}$ równa co do wartości $\frac{n}{NWD(a,n)}$ taka, że $\sigma^{ad} = 1$ i - korzystając z przemienności elementów podgrupy $< \sigma >$ z elementami podgrupy G - dostalibyśmy zależność $\lambda_0^d = \tau'^d \in H \cap G$, co stałoby w sprzeczności z rzędem warstwy $\lambda_0 H \cap G$. Wobec tego (por. [**16**] zadanie 61.(f)) dla pewnej liczby t mamy $\sigma^{a \cdot t} = \sigma$, więc jeszcze raz korzystając z przemienności elementów podgrupy $< \sigma >$ z elementami podgrupy G otrzymujemy, że $\lambda = \lambda_0^t = \sigma \cdot \tau_0$ dla $\tau_0 \in G$. Jeżeli teraz oznaczymy przez $\psi_1, \dots, \psi_e$ wszystkie elementy grupy $H \cap G$, to możemy zdefiniować grupy:

$$U^{(j)} =< \sigma \tau_0 \psi_j > \text{ dla } j \in \{1, \dots, e\}$$

zawarte w H, cykliczne rzędu n, parami rozłączne i na przecięcie z G równe $\{1\}$.

Dla zakończenia dowodu pozostaje wykazać, że w grupie H nie ma innych grup cyklicznych rzędu n równych na przecięcie z G grupie jedynkowej $\{1\}$. Faktycznie, ustalmy grupę cykliczną $U \subseteq H$ rzędu n i niech $U \cap G = \{1\}$. Argumentując podobnie jak przed chwilą możemy w grupie U wskazać generator postaci $\sigma \cdot \tau_1$, gdzie $\tau_1 \in G$. Ponieważ $\sigma \cdot \tau_1 \in H$ oraz, z definicji λ_0, $\sigma \cdot \tau_0 \in H$, korzystając też z przemienności elementów podgrupy $< \sigma >$ z elementami podgrupy G mamy:

$$\tau_0^{-1} \cdot \tau_1 = (\sigma \tau_0)^{-1} (\sigma \tau_1) \in H \cap G = \{\psi_1, \dots, \psi_e\}$$

Stąd $\tau_1 = \tau_0 \cdot \psi_{j_0}$ dla pewnego $j_0 \in \{1, \dots, e\}$ i $U =< \sigma \cdot \tau_1 >=< \sigma \cdot \tau_0 \cdot \psi_{j_0} >= U^{(j_0)}$ co kończy dowód. *QED*

LEMAT 3.2.2. *Niech $L/\mathbb{F}_q$ będzie ciałem funkcji algebraicznych, niech $E/\mathbb{F}_q \supset L/\mathbb{F}_q$ będzie rozszerzeniem Galois i załóżmy, że $\mathbb{F}_q$ jest ciałem stałych zarówno dla E jak i dla L. Oznaczmy przez m stopień rozszerzenia $[E : L]$ i ustalmy dowolną liczbę naturalną $n \in \mathbb{N}$ taką, że $m|n$. Rozważmy rozszerzenia ciał stałych $E' = E\mathbb{F}_{q^n}/\mathbb{F}_{q^n} \supset E/\mathbb{F}_q$ oraz $L' = L\mathbb{F}_{q^n}/\mathbb{F}_{q^n} \supset L/\mathbb{F}_q$ stopnia $n = [\mathbb{F}_{q^n} : \mathbb{F}_q]$. Wówczas:*

(1) *$E' \supset L$ jest rozszerzeniem Galois stopnia $m \cdot n$ o grupie Galois $G' =< \sigma > \times G$, gdzie:*
$$G = \mathsf{Gal}\,(E'/L') \cong \mathsf{Gal}\,(E/L)$$
zaś σ jest automorfizmem Frobeniusa rozszerzenia $E' \supseteq E$.

(2) *G' zawiera dokładnie m podgrup cyklicznych $U_1, \ldots, U_m$ rzędu n takich, że $U_i \cap G = \{1\}$, dla $i \in \{1, \ldots, m\}$.*

(3) *L ma dokładnie m rozszerzeń stopnia m $E_1, \ldots, E_m$ takich, że $[E' : E_i] = n$, $E' \supset E_i$ jest cykliczne oraz $\mathsf{Gal}\,(E'/E_i) \cong U_i$ dla $i \in \{1, \ldots, m\}$. Możemy przy tym założyć, że $E_1 = E$.*

(4) *$\mathbb{F}_q$ jest ciałem stałych dla $E_i/\mathbb{F}_q$.*

(5) *Jeżeli oznaczymy przez $g(E_i)$ rodzaj ciała E_i, $i \in \{1, \ldots, m\}$, a przez $g(E)$ rodzaj ciała E, to:*
$$E' = E_i\mathbb{F}_{q_n}/\mathbb{F}_{q^n} \text{ oraz } g(E_i) = g(E) \text{ dla } i \in \{1, \ldots, m\}$$

(6) *Jeżeli oznaczymy przez $N(L)$ liczbę punktów stopnia 1 ciała L, a przez $N(E_i)$ liczbę punktów stopnia 1 ciała E_i, $i \in \{1, \ldots, m\}$, to:*
$$m \cdot N(L) = \sum_{i=1}^{m} N(E_i)$$

D o w ó d : (1) Pokażemy najpierw, że $\mathsf{Gal}\,(E'/L) \cong \mathsf{Gal}\,(E'/E) \times \mathsf{Gal}\,(E/L)$. Zdefiniujmy w tym celu odwzorowanie $\Phi : \mathsf{Gal}\,(E'/E) \times \mathsf{Gal}\,(E/L) \to \mathsf{Gal}\,(E'/L)$ wzorem:
$$\Phi(\phi, \psi) = \phi \circ \psi_{E'}, \text{ dla } (\phi, \psi) \in \mathsf{Gal}\,(E'/E) \times \mathsf{Gal}\,(E/L)$$
gdzie odwzorowanie $\psi_{E'} : E' \to E'$ określone jest następująco:
$$\psi_{E'}(a) = \begin{cases} a & \text{jeżeli } a \in E' \setminus E \\ \psi(a) & \text{jeżeli } a \in E \end{cases}$$
Bez trudu sprawdzamy, że odwzorowanie Φ jest dobrze określonym homomorfizmem grup (zauważmy tu, że składanie automorfizmów ϕ i $\psi_{E'}$ jest przemienne, jako że ich nośniki są rozłączne). W oczywisty sposób Φ jest bijekcją, a więc również poszukiwanym izomorfizmem grup.

Korzystając z tezy (1) lematu 3.1.3 stwierdzamy, że $\mathsf{Gal}\,(E'/E) =< \sigma >$, gdzie σ jest automorfizmem Frobeniusa rozszerzenia $E' \supset E$. Ponadto $| < \sigma > \times \mathsf{Gal}\,(E/L)| = n \cdot m = [E' : L]$, więc istotnie rozszerzenie $E' \supseteq L$ jest typu Galois o grupie Galois $< \sigma > \times \mathsf{Gal}\,(E/L)$.

Dla zakończenia tej części dowodu wystarczy sprawdzić, że $\mathsf{Gal}\,(E/L) \cong \mathsf{Gal}\,(E'/L')$. Ponieważ $E' = E\mathbb{F}_{q^n} \supseteq L$ jest typu Galois i $L' = L\mathbb{F}_{q^n} \supseteq L$, więc wobec ze znanego z kursu algebry twierdzenia (por. [**3**] twierdzenie III.2.3.11 (3)) rozszerzenie $E\mathbb{F}_{q^n} L\mathbb{F}_{q^n} = E\mathbb{F}_{q^n} = E' \supseteq L'$ jest Galois o grupie Galois $\mathsf{Gal}\,(E'/L')$ izomorficznej z pewną podgrupą grupy $\mathsf{Gal}\,(E/L)$. Ponadto, z równości:
$$m \cdot n = [E' : L] = [E' : L'] \cdot [L' : L] = [E' : L'] \cdot n$$
widzimy, że $|\mathsf{Gal}\,(E'/L')| = m$ i skoro $|\mathsf{Gal}\,(E/L)| = m$, to $\mathsf{Gal}\,(E'/L') \cong \mathsf{Gal}\,(E/L)$.

Teza (2) wynika bezpośrednio z lematu 3.2.1, natomiast teza (3) jest bezpośrednią konsekwencją zasadniczych twierdzeń teorii Galois znanych z kursu algebry (por. [**3**] twierdzenia III.3.1.1 i III.3.1.2).

(4) i (5) Pokażemy - co okaże się głównym argumentem w tej części dowodu - że dla dowolnych $i \in \{1, \dots, m\}$ $E' = E_i\mathbb{F}_{q^n}$. Ustalmy w tym celu liczbę $i \in \{1, \dots, m\}$ i rozważmy dwie wieże ciał: $E' \supseteq E_i \supseteq L$ i $E' \supseteq L' \supseteq L$. Korzystając ze znanego z wykładu algebry twierdzenia (por. [**3**] twierdzenie III.3.1.5 (1)) otrzymujemy:

$$\mathsf{Gal}\,(E'/E_iL') = \mathsf{Gal}\,(E'/E_i) \cap \mathsf{Gal}\,(E'/L') = U_i \cap G = \{1\}$$

A więc $E' = E_iL'$. Stąd od razu otrzymujemy $E' = E_iL' = E_iL\mathbb{F}_{q^n} = E_i\mathbb{F}_{q^n}$, co oznacza, że E' jest rozszerzeniem ciała stałych $\mathbb{F}_{q^n}$ o ciało E_i.

Aby pokazać pozostałe tezy tej części twierdzenia, zauważmy dla ustalonego $i \in \{1, \dots, m\}$, iż $\mathsf{Gal}\,(E_i\mathbb{F}_{q^n}/E_i) = \mathsf{Gal}\,(E'/E_i) = U_i$. Tak więc $E_i\mathbb{F}_{q^n} \supseteq E_i$ jest rozszerzeniem cyklicznym stopnia n i ponieważ - wobec tezy (1) lematu 3.1.3 - rozszerzeniem takim jest $E_i\mathbb{F}_{q^n}/\mathbb{F}_{q^n} \supseteq E_i/\mathbb{F}_q$, więc ciałem stałych dla E_i jest $\mathbb{F}_q$. Ponadto - wobec tezy (3) lematu 3.1.3 - $E' = E_i\mathbb{F}_{q^n}/\mathbb{F}_{q^n}$ ma ten sam rodzaj, co $E_i/\mathbb{F}_q$ i $E' = E\mathbb{F}_{q^n}/\mathbb{F}_{q^n}$ ma ten sam rodzaj co $E/\mathbb{F}_q$, więc $g(E_i) = g(E') = g(E)$

(6) Przechodzimy teraz do ostatniej, najtrudniejszej części lematu. Oznaczmy:

$$X = \{P \in \mathbb{P}_L : \mathsf{deg}\, P = 1\}$$

$$X_i = \{Q \in \mathbb{P}_{E_i} : \mathsf{deg}\, Q = 1\} \text{ dla } i \in \{1, \dots, m\}$$

Ponieważ grupy $U_1, \dots, U_m$ są parami różne, więc na mocy zasadniczych twierdzeń teorii Galois ciała $E_1, \dots, E_m$ są parami różne i zbiory $X_1, \dots, X_m$ są parami rozłączne. Zatem wystarczy pokazać, że:

$$|\bigcup_{i=1}^{m} X_i| = m \cdot |X|$$

Postaramy się nieco uprościć ten warunek tak, aby do zakończenia dowodu wystarczyło pokazać zachodzenie dwóch wzajemnie jednoznacznych odpowiedniości między punktami. Ustalmy zatem punkt $P \in X$ i niech $Q' \in \mathbb{P}_{E'}$ będzie jego rozszerzeniem, $Q'|P$. Zauważmy, że $f(Q'|P) = n$.

W rzeczy samej, oznaczmy też przez $P_1 = Q' \cap E$ punkt ciała E (istnienie stosownych punktów i poprawność określeń uzasadnia twierdzenie 2.1.3). Wobec tezy (2) twierdzenia 2.3.1 $e(P_1|P) \cdot f(P_1|P) \cdot |\{R \in \mathbb{P}_E : R|P\}| = [E : L] = m$, więc w szczególności $f(P_1|P)|m$, a zatem również $f(P_1|P)|n$. Ponadto, wobec tezy (5) twierdzenia 2.2.1, $E'_{Q'} = E_{P_1}\mathbb{F}_{q^n}$ oraz - z definicji - $E_{P_1} \supseteq \mathbb{F}_q$. Tak więc skoro $[E_{P_1} : \mathbb{F}_q] = [E_{P_1} : E_P] \cdot [E_P : \mathbb{F}_q] = f(P_1|P) \cdot \mathsf{deg}\, P|n \cdot 1 = n$ stwierdzamy, że $E'_{Q'} = \mathbb{F}_{q^n}$. Na koniec policzmy:

$$\begin{aligned} f(Q'|P) &= [E'_{Q'} : L_P] = [\mathbb{F}_{q^n} : L_P] = [\mathbb{F}_{q^n} : L_P] \cdot 1 = [\mathbb{F}_{q^n} : L_P] \cdot \mathsf{deg}\, P = \\ &= [\mathbb{F}_{q^n} : L_P] \cdot [L_P : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q] = n \end{aligned}$$

Dokonamy teraz zapowiadanego uproszczenia zagadnienia. Oznaczmy więc przez $e = e(Q'|P)$ dla dowolnego punktu $Q' \in \mathbb{P}_{E'}$, $Q'|P$ (liczba ta jest - wobec tezy (1) twierdzenia 2.3.1 - stała dla dowolnych rozszerzeń punktu P) oraz przez $r = |\{Q' \in \mathbb{P}_{E'} : Q'|P\}|$ (przypomnijmy, iż - wobec tezy (2) twierdzenia 2.1.2 zbiór $\{Q' \in \mathbb{P}_{E'} : Q'|P\}$ jest skończony). Korzystając z tezy (2) twierdzenia 2.3.1 mamy:

$$m \cdot n = [E' : L] = e(Q'|P) \cdot f(Q'|P) \cdot r = e \cdot n \cdot r$$

skąd - dzieląc obustronnie przez n - otrzymujemy równość $m = n \cdot r$. Jeżeli udowodnimy teraz wzajemnie jednoznaczną odpowiedniość między punktami ze zbioru X_i leżącymi nad punktem P i ich rozszerzeniami w ciele E' oraz - z drugiej strony - taką samą odpowiedniość między rozszerzeniami punktu P z ciała E' a każdymi e różnymi rozszerzeniami wybranymi ze zbiorów X_i, to zakończymy dowód.

Po pierwsze więc, pokażemy, że dla każdego punktu $Q \in X_i$ leżącego nad wcześniej ustalonym punktem P istnieje dokładnie jeden punkt $Q' \in \mathbb{P}_{E'}$ taki, że $Q'|Q$, przy czym $i \in \{1, \ldots, m\}$ jest wybrane dowolnie. Weźmy więc pod uwagę punkt $Q \in X_i$ leżący nad punktem P - istnienie takiego punktu wynika z tezy (1) twierdzenia 2.1.2. Podobnie rozważmy punkt $Q' \in \mathbb{P}_{E'}$ rozszerzający punkt Q. Mamy:

$$1 = \deg Q = [E_{iQ} : \mathbb{F}_p] = [E_{iQ} : L_P] \cdot [L_P : \mathbb{F}_q] = f(Q|P) \cdot \deg P = f(Q|P)$$

Zatem:

$$f(Q'|Q) = f(Q'|Q) \cdot f(Q|P) = [E'_{Q'} : E_{iQ}] \cdot [E_{iQ} : L_P] = [E'_{Q'} : L_P] = f(Q'|P) = n$$

Ponieważ jednocześnie $[E' : E_i] = n$, więc po raz kolejny stosując tezę (2) twierdzenia 2.3.1 dostajemy, że:

$$e(Q'|Q) \cdot n \cdot |\{Q' \in \mathbb{P}_{E'} : Q'|Q\}| = e(Q'|Q) \cdot f(Q'|Q) \cdot |\{Q' \in \mathbb{P}_{E'} : Q'|Q\}| = n$$

więc zbiór $\{Q' \in \mathbb{P}_{E'} : Q'|Q\}$ jest jednoelementowy.

Po drugie pokażemy - i to zakończy już dowód - że dla każdego punktu $Q' \in \mathbb{P}_{E'}$ leżącego nad wcześniej ustalonym punktem P istnieje dokładnie e różnych punktów $Q \in \bigcup_{i=1}^{m} X_i$ takich, że $Q'|Q$. Ustalmy więc punkt $Q' \in \mathbb{P}_{E'}$ leżącego nad punktem P i wprowadźmy skrócone oznaczenia $H = G_Z(Q'|P)$, $Z = Z(Q'|P)$. Niech ponadto $P_Z \in \mathbb{P}_Z$ oznacza punkt $Q' \cap Z$.

Zauważmy najpierw, że $|H| = e \cdot n$. W tym celu wystarczy zastosować tezę (1) twierdzenia 2.3.2 i otrzymać:

$$|H| = e(Q'|P) \cdot f(Q'|P) = e \cdot n$$

Zauważmy dalej, że podgrupie $H \cap G$ grupy Galois $\mathsf{Gal}\,(E'/L)$ odpowiada ciało pośrednie ZL' - wynika to wprost ze znanego z kursu algebry twierdzenia (por. [**3**] twierdzenie III.3.1.5 (1)), jako że:

$$H \cap G = \mathsf{Gal}\,(E'/Z) \cap \mathsf{Gal}\,(E'/L') = \mathsf{Gal}\,(E'/ZL')$$

Teraz zauważmy, że $|H \cap G| = e$. Faktycznie, wobec tezy (3) twierdzenia 2.3.2 $f(P_Z|P) = 1$, skąd:

$$[Z_{P_Z} : \mathbb{F}_q] = [Z_{P_Z} : L_P] \cdot [L_P : \mathbb{F}_q] = f(P_Z|P) \cdot \deg P = 1 \cdot 1 = 1$$

a więc $\mathbb{F}_q$ jest ciałem stałych dla Z. Zatem $ZL' = ZL\mathbb{F}_{q^n} = Z\mathbb{F}_{q_n} \supseteq Z\mathbb{F}_q$ jest - wobec tezy (1) lematu 3.1.3 - rozszerzeniem cyklicznym stopnia n i mamy:

$$|H \cap G| = [E' : ZL'] = \frac{[E' : Z]}{[ZL' : Z]} = \frac{|H|}{[ZL' : Z]} = \frac{e \cdot n}{n} = e$$

.

W dalszym ciągu zauważmy, że ZL' jest ciałem bezwładności punktu Q' nad P i tym samym $H \cap G$ jest grupą bezwładności tego samego rozszerzenia. Ustalmy punkt $P'_Z \in \mathbb{P}_{ZL'}$ leżący nad punktem P_Z. Ponieważ - tak jak stwierdziliśmy - ZL' jest rozszerzeniem ciała stałych $\mathbb{F}_{q^n}$ o ciało Z, więc na mocy tezy (2) twierdzenia

2.2.1 zachodzi równość $e(P'_Z|P_Z) = 1$. Ponadto - wobec tezy (3) twierdzenia 2.3.2 - $e(P_Z|P) = 1$, więc korzystając też z twierdzenia 2.1.4 mamy:

$$e(Q'|P'_Z) = e(Q'|P'_Z) \cdot e(P'_Z|P_Z) = e(Q'|P_Z) = e(Q'|P_Z) \cdot e(P_Z|P) = e(Q'|P) = e$$

skąd $e(Q'|P'_Z) = e = |H \cap G| = [E' : ZL']$. Dalej, ponieważ oczywiście $ZL' \supseteq Z$, więc wobec tezy (2) twierdzenia 2.3.3 Q' jest jedynym punktem ciała E' leżącym nad P_Z i - tym razem wobec tezy (4) tego samego twierdzenia - $ZL' \supseteq T(Q'|P)$. Aby wykazać inkluzję przeciwną, zauważmy, że - wobec tezy (2) twierdzenia 2.2.1 i twierdzenia 2.1.4 - $e(P'_Z|P) = e(P'_Z|P_Z) \cdot e(P_Z|P) = 1 \cdot 1 = 1$ i zastosujmy punkt (3) twierdzenia 2.3.3.

Wobec lematu 3.2.1 dokładnie e grup cyklicznych $U_{i_1}, \ldots, U_{i_e}$ rzędu n spośród grup $U_1, \ldots, U_m$ takich, że $U_i \cap G = \{1\}$, $i \in \{1, \ldots, m\}$, jest zawartych w H. Oznaczmy $Q_{i_j} = Q' \cap E_{i_j}$, $j \in \{1, \ldots, e\}$ i ustalmy $j \in \{1, \ldots, e\}$.

Zauważmy, że $Q_{i_j} \in \bigcup_{i=1}^{m} X_i$, czyli że $\deg Q_{i_j} = 1$. Rzeczywiście, ponieważ H jest grupą Galois rozszerzenia $E' \supseteq Z$, U_{i_j} jest grupą Galois rozszerzenia $E' \supseteq E_{i_j}$ oraz U_{i_j} jest podgrupą grupy H, więc $E' \supseteq E_{i_j} \supseteq Z$ i w szczególności $E_{i_j} \supseteq Z$. Teraz wystarczy zastosować punkt (2) twierdzenia 2.3.3 aby przekonać się, że $Q' \in \mathbb{P}_{E'}$ jest jedynym punktem ciała E' leżącym nad Q_{i_j}. Dalej, wobec udowodnionego już punktu (5) niniejszego lematu, E' jest rozszerzeniem ciała stałych $\mathbb{F}_{q^n}$ o ciało E_{i_j}, a więc - na podstawie tezy (2) twierdzenia 2.2.1 - $e(Q'|Q_{i_j}) = 1$. Wykorzystajmy jeszcze raz punkt (2) twierzenia 2.3.1; mamy:

$$f(Q'|Q_{i_j}) = e(Q'|Q_{i_j}) \cdot f(Q'|Q_{i_j}) \cdot |\{Q' \in \mathbb{P}_{E'} : Q'|Q_{i_j}\}| = [E' : E_{i_j}] = n$$

Zatem $n = f(Q'|P) = [E'_{Q'} : L_P] = [E'_{Q'} : E_{i_j Q_{i_j}}] \cdot [E_{i_j Q_{i_j}} : L_P] = f(Q'|Q_{i_j}) \cdot [E_{i_j Q_{i_j}} : L_P] = n \cdot [E_{i_j Q_{i_j}} : L_P]$ skąd $[E_{i_j Q_{i_j}} : L_P] = 1$. Ostatecznie:

$$\deg Q_{i_j} = [E_{i_j Q_{i_j}} : \mathbb{F}_p] = [E_{i_j Q_{i_j}} : L_P] \cdot [L_P : \mathbb{F}_p] = 1 \cdot \deg P = 1$$

Dla zakończenia dowodu pozostaje wykazać, że skonstruowane dla danego Q' e punkty $Q_{i_j} \in \cup_{i=1}^{m} X_i$, $j \in \{1, \ldots, e\}$, takie, że $Q'|Q_{i_j}$, $j \in \{1, \ldots, e\}$, są jedynymi możliwymi punktami o tej własności. Ustalmy więc liczbę $i \in \{1, \ldots, m\}$ i punkt $Q \in X_i$ leżący pod punktem Q'. Wobec tezy (2) twierdzenia 2.3.2:

$$[E'_{Q'} : L_P] = |\mathsf{Gal}\,(E'_{Q'}/L_P)| = \frac{|G_Z(Q'|P)|}{|G_T(Q'|P)|} = \frac{|H|}{|H \cap G|} = \frac{n \cdot e}{e} = n$$

skąd $[E'_{Q'} : \mathbb{F}_p] = [E'_{Q'} : L_P] \cdot [L_P : \mathbb{F}_p] = n \cdot \deg P = n \cdot 1 = n$, a zatem:

$$f(Q'|Q) = [E'_{Q'} : E_Q] = \frac{[E'_{Q'} : \mathbb{F}_p]}{[E_Q : \mathbb{F}_p]} = \frac{n}{1} = n$$

Korzystając ponownie z udowodnionej już części (5) lematu, E' jest rozszerzeniem ciała stałych $\mathbb{F}_{q^n}$ o ciało E_i, tak więc - wobec tezy (2) twierdzenia 2.2.1 - $e(Q'|Q) = 1$. Zatem na podstawie tezy (2) twierdzenia 2.3.1:

$$n \cdot |\{Q' \in \mathbb{P}_{E'} : Q'|Q\}| = f(Q'|Q) \cdot e(Q'|Q) \cdot |\{Q' \in \mathbb{P}_{E'} : Q'|Q\}| = [E' : E_i] = n$$

skąd $Q' \in \mathbb{P}_{E'}$ jest jedynym rozszerzeniem punktu $Q \in \mathbb{P}_{E_i}$. Tym samym - korzystając z tezy (2) twierdzenia 2.3.3 - $E_i \supseteq Z$ i w konsekwencji $E' \supseteq E_i \supseteq Z$. Skoro H jest grupą Galois rozszerzenia $E' \supseteq Z$ i U_i jest grupą Galois rozszerzenia $E' \supseteq E_i$, to U_i jest podgrupą cykliczną rzędu n grupy H taką, że $U_i \cap G = \{1\}$, a więc jest jedną z podgrup $U_{i_1}, \ldots, U_{i_e}$, co kończy dowód całego lematu. *QED*

D o w ó d t w i e r d z e n i a H a s s e ' g o - W e i l ' a : Dowód podzielimy na kilkanaście kroków.

Dla $r \geqslant 1$ niech $F_r = F \cdot \mathbb{F}_{q^r}/\mathbb{F}_{q^r}$ będzie algebraicznym rozszerzeniem ciała funkcji algebraicznych $F/\mathbb{F}_q$. Oznaczmy:

$$\bigwedge_{n\in\mathbb{N}} A_{n,r} = |\{A \in \mathcal{D}_{F_r} : A \geqslant 0 \wedge degA = n\}|$$

$$Z_{F_r}(t) = \sum_{n=0}^{\infty} A_{n,r}t^n$$

$$L_{F_r}(t) = (1-t)(1-qt)Z_{F_r}(t)$$

Krok I: Dla ustalonej liczby $r \geqslant 1$ niech $\beta_1, \ldots, \beta_{2g}$ będą odwrotnościami pierwiastków L-wielomianu L_{F_r}. Wówczas:

$$\bigwedge_{i\in\{1,\ldots,2g\}} |\alpha_i| = \sqrt{q} \Leftrightarrow |\beta_i| = \sqrt{q^r}$$ ❑

Dowód kroku I: Wobec punktu (6) twierdzenia 3.1.8 odwrotnościami pierwiastków L-wielomianu L_{F_r} są liczby $\alpha_1^r, \ldots, \alpha_{2g}^r$, skąd wynika teza. ❑

Tak więc w kroku I stwierdziliśmy, że aby udowodnić twierdzenie Hasse'go - Weil'a dla ciała F, potrzeba i wystarcza udowodnić je dla dowolnie wybranego rozszerzenia ciała stałych $\mathbb{F}_{q^r}$ o ciało F. Pozwoli to nam w znacznym stopniu uprościć dalsze założenia i wprowadzić przygotowany w lematach aparat. W następnym kroku pokażemy, że twierdzenie wynika bezpośrednio z oszacowań liczby punktów stopnia 1 w takich rozszerzeniach. Oznaczmy:

$$\bigwedge_{r\in\mathbb{N}} N_r = |\{P \in \mathbb{P}_{F_r} : degP = 1\}|$$

przy czym zamiast N_1 pisać będziemy N.

Krok II: Jeżeli:

$$\bigvee_{c\in\mathbb{R}} \bigwedge_{r\in\mathbb{N}} |N_r - (q^r+1)| \leqslant c\sqrt{q^r}$$

to:

$$\bigwedge_{i\in\{1,\ldots,2g\}} |\alpha_i| = \sqrt{q}$$ ❑

Dowód kroku II: Załóżmy, że istnieje stała $c \in \mathbb{R}$ taka, że:

$$\bigwedge_{r\in\mathbb{N}} |N_r - (q^r+1)| \leqslant c\sqrt{q^r}$$

Na podstawie wniosku 3.1.2 $N_r - (q^r+1) = -\sum_{i=1}^{2g} \alpha_i^r$, więc:

$$\bigwedge_{r\in\mathbb{N}} |\sum_{i=1}^{2g} \alpha_i^r| \leqslant c\sqrt{q^r}$$

Zdefiniujmy funkcję $H : \mathbb{C} \to \mathbb{C}$ wzorem:

$$H(t) = \sum_{i=1}^{2g} \frac{\alpha_i t}{1-\alpha_i t} \text{ dla } t \in \mathbb{C}$$

Funkcja ta jest meromorficzna w $\mathbb{C}$ (tj. analityczna w $\mathbb{C}$ poza ewentualnie zbiorem punktów, w których ma bieguny). Niech:

$$\rho = \min\{|\alpha_i^{-1}| : 1 \leqslant i \leqslant 2g\}$$

Wobec tego funkcja H jest analityczna w kole $K(0,\rho)$, ponieważ $\alpha_1^{-1}, \ldots, \alpha_{2g}^{-1}$ są jej jedynymi biegunami. Na podstawie twierdzenia o zmianie kolejności sumowania

wyrazów szeregu zbieżnego jednostajnie (w szczególności szeregu potęgowego) (por. [**9**], str. 18):

$$\bigwedge_{t\in K(0,\rho)} H(t) = \sum_{i=1}^{2g}\frac{\alpha_i t}{1-\alpha_i t} = \sum_{i=1}^{2g}\sum_{r=1}^{\infty}(\alpha_i t)^r = \\ = \sum_{r=1}^{\infty}\left(\sum_{i=1}^{r}\right)t^r$$

Wobec twierdzenia Cauchy'ego - Hadamarda o promieniu zbieżności szeregu potęgowego (por. [**9**], str. 49), promień zbieżności szeregu $\sum_{r=1}^{\infty}\left(\sum_{i=1}^{r}\right)t^r$ jest równy:

$$\frac{1}{\limsup_{r\to\infty}\sqrt[r]{|\sum_{i=1}^{2g}\alpha_i^r|}} = \frac{1}{\limsup_{r\to\infty}\sqrt[r]{c\sqrt{q^r}}} = \frac{1}{\sqrt{q}}$$

Zatem $\frac{1}{\sqrt{q}} \leqslant \rho$ i wobec tego $|\alpha_i| \leqslant \sqrt{q}$ dla wszelkich $i \in \{1,\dots,2g\}$. Aby pokazać równość, zauważmy, iż wobec tezy (5) twierdzenia 3.1.8:

$$\prod_{i=1}^{2g}\alpha_i = \alpha_1\cdot\ldots\cdot\alpha_{2g} = \alpha_1\cdot\alpha_{g+1}\cdot\alpha_2\cdot\alpha_{g+2}\cdot\ldots\cdot\alpha_g\cdot\alpha_{2g} = q^g$$

skąd wynika, że $|\alpha_i| = \sqrt{q}$ dla $i \in \{1,\dots,2g\}$. ❑

Krok III: Warunek:

$$\bigvee_{c\in\mathbb{R}}\bigwedge_{r\in\mathbb{N}}|N_r - (q^r+1)| \leqslant c\sqrt{q^r}$$

jest równoważny warunkom:

$$\bigvee_{c_1\in\mathbb{R}}\bigwedge_{r\in\mathbb{N}} N_r \leqslant q^r + 1 + c_1\sqrt{q^r}$$
$$\bigvee_{c_2\in\mathbb{R}}\bigwedge_{r\in\mathbb{N}} N_r \geqslant q^r + 1 - c_1\sqrt{q^r}$$ ❑

Dowód tego kroku jest oczywisty. Jak więc widzimy, dalszy dowód będzie polegał na znalezieniu dwóch - górnego i dolnego - oszacowania liczby punktów dla odpowiednich rozszerzeń. Pierwsze z nich otrzymamy wykonując pewne dosyć elementarne operacje na odpowiednio zdefiniowanych przestrzeniach liniowych, natomiast drugie wykorzysta subtelną konstrukcję rozszerzeń ciał, przygotowaną w lematach.

Wobec kroku I, twierdzenie Hasse'go - Weil'a wystarczy pokazać dla pewnego ciała F_r/F_{q^r}. Wybierzmy więc takie rozszerzenie, dla którego q^r jest kwadratem i spełnia zależnośc $q^r > (g+1)^4$. Aby uprościć zapis, zamiast q^r pisać będziemy po prostu q i rozważać ciało $F/\mathbb{F}_q$. Niech więc q będzie kwadratem i:

$$q > (g+1)^4$$

Oznaczmy:

$$q_0 = \sqrt{q},\ m = q_0 - 1,\ n = 2g + q_0,\ r = q - 1 + (2g+1)q_0$$

Niech $Q \in \mathbb{P}_F$ będzie punktem stopnia 1. Oznaczmy:

$$T = \{i \in \{0,\dots,m\} : \bigvee_{x\in F}(x)_\infty = iQ\}$$

$$\mathcal{B} = \{u_i \in F : (u_i)_\infty = iQ, i \in T\}$$

i niech:

$$\mathcal{L} = \mathcal{L}(mQ)\cdot\mathcal{L}(nQ)^{q_0}$$

oznacza najmniejszą przestrzeń liniową zawierającą zbiór:

$$\{xy^{q_0} : x \in \mathcal{L}(mQ), y \in \mathcal{L}(nQ)\}$$

Krok IV: Przy powyższych oznaczeniach:

(1) $r = m + nq_0$,
(2) $\mathcal{L} = \{\sum x_\nu y_\nu^{q_0} : x_\nu \in \mathcal{L}(mQ), y_\nu \in \mathcal{L}(nQ)\}$,
(3) Zbiór $\mathcal{B}$ jest bazą przestrzeni $\mathcal{L}(mQ)$,
(4) $\mathcal{L} \subseteq \mathcal{L}(rQ)$ ❑

Dowód kroku IV: (1) Policzmy:

$$\begin{aligned} r &= q - 1 + (2g+1)q_0 = (q_0)^2 - 1 + (2g+1)q_0 = \\ &= (q_0)^2 - 1 + 2gq_0 + q_0 = q_0 - 1 + (2g + q_0)q_0 = \\ &= m + nq_0 \end{aligned}$$

(2) Oznaczmy $\mathcal{L}_1 = \{\sum x_\nu y_\nu^{q_0} : x_\nu \in \mathcal{L}(mQ), y_\nu \in \mathcal{L}(nQ)\}$. Bez trudu sprawdzamy, że $\mathcal{L}_1$ jest przestrzenią liniową i $\mathcal{L}_1 \supseteq \mathcal{L}$. Dla pokazania przeciwnej inkluzji ustalmy $\sum x_\nu y_\nu^{q_0} \in \mathcal{L}_1$, gdzie $x_\nu \in \mathcal{L}(mQ)$, $y_\nu \in \mathcal{L}(nQ)$, dla $\nu \in \mathbb{N}$. Wówczas dla wszystkich $\nu \in \mathbb{N}$ $x_\nu y_\nu^{q_0} \in \mathcal{L}$, a więc i $\sum x_\nu y_\nu^{q_0} \in \mathcal{L}$.

(3) Pokażemy najpierw, że zbiór $\mathcal{B}$ jest liniowo niezależny. Ustalmy więc $u_1, \ldots, u_p \in \mathcal{B}$, $(u_i)_\infty = iQ$ dla $i \in \{1, \ldots, p\}$ i $p \in \mathbb{N}$ oraz $x_1, \ldots, x_p \in \mathbb{F}_q$ nie wszystkie równe zeru. Dla dowodu nie wprost przypuśćmy, że $x_1u_1 + \ldots + x_pu_p = 0$.Wówczas $v_Q(x_1u_1 + \ldots + x_pu_p) = v_Q(0) = \infty$. Z drugiej strony, ponieważ $v_Q(x_iu_i) \neq v_Q(x_ju_j)$ dla $i \neq j$, $i, j \in \{1, \ldots, p\}$, twierdzenie 1.1.3 daje:

$$\begin{aligned} v_Q(x_1u_1 + \ldots + x_pu_p) &= \min\{v_Q(x_1u_1), \ldots, v_Q(x_pu_p)\} = \\ &= \min\{v_Q(u_1), \ldots, v_Q(u_p)\} < \infty \end{aligned}$$

co daje sprzeczność.

Pokażemy teraz, że $|\mathcal{B}| = 1 + m - g$. Istotnie, wobec twierdzenia Weierstrassa o dziurach 1.3.4, istnieje dokładnie g takich liczb i, że $(x)_{infty} \neq iQ$ dla dowolnych $x \in F$. Zatem $|\mathcal{B}| = |T| = 1 + m - g$.

Na koniec pokażemy, że $\mathsf{dim}\, \mathcal{L}(mQ) = 1 + m - g$. Faktycznie, ponieważ $\mathsf{deg}\, Q = 1$, więc $\mathsf{deg}\,(mQ) = m = q_0 - 1 > (g+1)^2 - 1 = g^2 + 2g + 1 - 1 \geqslant 2g - 2$. Zatem stosując tezę (2) twierdzenia 1.3.3 dostajemy $\mathsf{dim}\, \mathcal{L}(mQ) = \mathsf{dim}\,(mQ) = 1 + m - g$.

(4) Rozpiszmy z definicji:

$$\begin{aligned} \bigwedge_{t \in \mathbb{N}} \mathcal{L}(tQ) &= \{x \in F : (x) \geqslant -tQ\} \cup \{0\} = \\ &= \left\{x \in F : \sum_{P \in \mathbb{P}_F} v_P(x) \geqslant -tQ\right\} \cup \{0\} = \\ &= \left\{x \in F : \left(\bigwedge_{P \in \mathbb{P}_F \setminus \{Q\}} v_P(x) \geqslant 0\right) \wedge (v_Q(x) \geqslant -t)\right\} \cup \{0\} \end{aligned}$$

Ustalmy więc $\sum x_\nu y_\nu^{q_0} \in \mathcal{L}$, gdzie $x_\nu \in \mathcal{L}(mQ)$, $y_\nu \in \mathcal{L}(nQ)$, dla $\nu \in \mathbb{N}$. Mamy wówczas:

$$\bigwedge_{\nu \in \mathbb{N}} \left(\bigwedge_{P \in \mathbb{P}_F \setminus \{Q\}} (v_P(x_\nu) \geqslant 0) \wedge (v_Q(x_\nu) \geqslant -m)\right)$$

$$\bigwedge_{\nu\in\mathbb{N}}\left(\bigwedge_{P\in\mathbb{P}_F\setminus\{Q\}}(v_P(y_\nu)\geqslant 0)\wedge(v_Q(y_\nu)\geqslant -n)\right)$$

i wobec tego:

$$\begin{aligned}\bigwedge_{P\in\mathbb{P}_F\setminus\{Q\}} v_P\left(\sum x_\nu y_\nu^{q_0}\right) &\geqslant \min\{v_P(x_\nu y_\nu^{q_0}):\nu\in\mathbb{N}\}=\\ &= \min\{v_P(x_\nu)+q_0v_P(y_\nu):\nu\in\mathbb{N}\}\geqslant\\ &\geqslant 0\end{aligned}$$

oraz:

$$\begin{aligned}v_Q\left(\sum x_\nu y_\nu^{q_0}\right) &\geqslant \min\{v_Q(x_\nu y_\nu^{q_0}):\nu\in\mathbb{N}\}=\\ &= \min\{v_Q(x_\nu)+q_0v_Q(y_\nu):\nu\in\mathbb{N}\}\geqslant\\ &\geqslant -m-q_0n=-r\text{❑}\end{aligned}$$

Krok V: Dowolny element $y\in\mathcal{L}$ ma jednoznaczne przedstawienie postaci:

$$y=\textstyle\sum_{i\in T}u_iz_i^{q^{s_0}},\ u_i\in\mathcal{B},\ z_i\in\mathcal{L}(nQ)\ \text{❑}$$

Dowód kroku V: Pokażemy najpierw istnienie stosownego przedstawienia. Ustalmy więc $y^{(0)}=\sum x_\nu^{(0)}{y_\nu^{(0)}}^{q_0}\in\mathcal{L}$, gdzie $x_\nu^{(0)}\in\mathcal{L}(mQ)$, $y_\nu^{(0)}\in\mathcal{L}(nQ)$, dla $\nu\in\mathbb{N}$ i niech $x_\nu^{(0)}=\sum_{i\in T}a_{\nu,i}u_i$, gdzie $a_{\nu,i}\in\mathbb{F}_q$, $u_i\in\mathcal{B}$, dla $\nu\in\mathbb{N}$. Mamy wtedy:

$$\begin{aligned}y^{(0)} &= \sum\left(\sum_{i\in T}a_{\nu,i}u_i\right){y_\nu^{(0)}}^{q_0}=\sum\sum_{i\in T}a_{\nu,i}u_i{y_\nu^{(0)}}^{q_0}=\\ &= \sum_{i\in T}\sum a_{\nu,i}u_i{y_\nu^{(0)}}^{q_0}=\sum_{i\in T}\left(\sum a_{\nu,i}{y_\nu^{(0)}}^{q_0}\right)u_i\end{aligned}$$

Ponieważ $y^{(0)}\in\mathcal{L}$, $u_i\in\mathcal{L}(mQ)$ oraz $\mathcal{L}=\{\sum x_\nu y_\nu^{q_0}:x_\nu\in\mathcal{L}(mQ),y_\nu\in\mathcal{L}(nQ)\}$, więc dla pewnych $z_i\in\mathcal{L}(nQ)$, $i\in T$, zachodzi równość $z_i^{q_0}=\sum a_{\nu,i}{y_\nu^{(0)}}^{q_0}$. Tak więc:

$$y^{(0)}=\textstyle\sum_{i\in T}u_iz_i^{q_0},\ \text{gdzie}\ u_i\in\mathcal{B},\ z_i\in\mathcal{L}(nQ),\ i\in T$$

Dla dowodu jednoznaczności ustalmy $y^{(0)}\in\mathcal{L}$ i przypuśćmy, że:

$$y^{(0)}=\textstyle\sum_{i\in T}u_ia_i^{q_0},\ \text{gdzie}\ u_i\in\mathcal{B},\ a_i\in\mathcal{L}(nQ),\ i\in T$$
$$y^{(0)}=\textstyle\sum_{i\in T}u_ib_i^{q_0},\ \text{gdzie}\ u_i\in\mathcal{B},\ b_i\in\mathcal{L}(nQ),\ i\in T$$

są dwoma różnymi przedstawieniami $y^{(0)}$. Mamy więc:

$$0=y^{(0)}-y^{(0)}=\sum_{i\in T}u_ia_i^{q_0}-\sum_{i\in T}u_ib_i^{q_0}=\sum_{i\in T}u_i\left(a_i^{q_0}-b_i^{q_0}\right)$$

Ponieważ $0\in\mathcal{L}$, $u_i\in\mathcal{L}(mQ)$ oraz $\mathcal{L}=\{\sum x_\nu y_\nu^{q_0}:x_\nu\in\mathcal{L}(mQ),y_\nu\in\mathcal{L}(nQ)\}$, więc dla pewnych $x_i\in\mathcal{L}(nQ)$, $i\in T$, nie wszystkich równych zeru zachodzi równość $x_i^{q_0}=a_i^{q_0}-b_i^{q_0}$. Zatem $\sum_{i\in T}u_ix_i^{q_0}=0$ i stąd:

$$v_Q\left(\sum_{i\in T}u_ix_i^{q_0}\right)=v_Q(0)=\infty$$

Z drugiej strony, jeżeli $x_i\neq 0$, to $v_Q(u_ix_i^{q_0})=v_Q(u_i)+q_0v_Q(x_i)$, więc skoro $v_Q(u_i)=-i\in\{0,\ldots,-m\}\subseteq\{0,\ldots,-q_0\}$ to $v_Q(u_ix_i^{q_0})\equiv -i(\mathsf{mod}\,q_0)$. Zatem dla $i\neq j$ oraz

$x_i, x_j \neq 0$ mamy $v_Q(u_i x_i^{q_0}) \neq v_Q(u_j x_j^{q_0})$ i stosując mocną nierówność trójkąta 1.1.3 otrzymujemy:

$$\begin{aligned} v_Q\left(\sum_{i\in T} u_i x_i^{q_0}\right) &= v_Q\left(\sum_{i\in\{i\in T: x_i\neq 0\}} u_i x_i^{q_0}\right) = \\ &= \min\{v_Q(u_i x_i^{q_0}) : i \in \{i \in T : x_i \neq 0\}\} < \\ &< \infty \end{aligned}$$

co doprowadza nas do sprzeczności. ❑

Zdefiniujmy odwzorowanie $\lambda : \mathcal{L} \to \mathcal{L}((q_0 m + n)Q)$ wzorem:

$$\lambda(\sum_{i\in T} u_i z_i^{q_0}) = \sum_{i\in T} u_i^{q_0} z_i$$

dla $u_i \in \mathcal{B}$, $z_i \in \mathcal{L}(nQ)$, $i \in T$.

Krok VI: Przy powyższych oznaczeniach:

(1) λ jest homomorfizmem grup addytywnych,
(2) $\ker\lambda \neq \{0\}$ ❑

Dowód kroku VI: To, że λ jest homomorfizmem można sprawdzić bez większych trudności, przejdziemy więc od razu do dowodu punktu (2). Aby wykazać, że λ nie może być różnowartościowe pokażemy, że $\mathsf{dim}\,\mathcal{L} > \mathsf{dim}\,\mathcal{L}((q_0 m + n)Q)$.

W tym celu zauważmy najpierw, że $\mathsf{dim}\,\mathcal{L} \geqslant (m+1-g)\cdot(n+1-g)$. Faktycznie, na podstawie kroku V $\mathsf{dim}\,\mathcal{L} = \mathsf{dim}\,(mQ) \cdot \mathsf{dim}\,(nQ)$, zaś korzystając z tezy (2) twierdzenia 1.3.3 dostajemy:

$$\begin{aligned} \mathsf{dim}\,(mQ) &\geqslant \mathsf{deg}\,(mQ) + 1 - g = m + 1 - g \\ \mathsf{dim}\,(nQ) &\geqslant \mathsf{deg}\,(nQ) + 1 - g = n + 1 - g \end{aligned}$$

Teraz zauważmy, że $(m + 1 - g) \cdot (n + 1 - g) > g + q + 1$. W rzeczy samej, wystarczy przeliczyć:

$$\begin{aligned} & (m+1-g)\cdot(n+1-g) > g+q+1 & \iff \\ \iff\ & (q_0-g)\cdot(2g+q_0+1-g) > g+q+1 & \iff \\ \iff\ & q - g^2 + q_0 - g > g+q+1 & \iff \\ \iff\ & q_0 > g^2 + 2g + 1 & \iff \\ \iff\ & q > (g+1)^4 \end{aligned}$$

co jest prawdą w myśl poczynionych założeń.

Na koniec zauważmy, że $\mathsf{dim}\,\mathcal{L}((q_0 m + n)Q) = g + q + 1$. Istotnie:

$$\begin{aligned} \mathsf{deg}\,((q_0 m + n)Q) &= q_0 m + n = q_0(q_0 - 1) + (2g + q_0) = \\ &= 2g + q > \\ &= 2g - 2 \end{aligned}$$

więc na podstawie tezy (2) twierdzenia 1.3.3:

$$\begin{aligned} \mathsf{dim}\,((q_0 m + n)Q) &= q_0 m + n + 1 - g = \\ &= 2g + q + 1 - g = \\ &= g + q + 1 \text{❑} \end{aligned}$$

Odnotujmy tu, iż przeprowadzone powyżej rozumowanie jest chyba najbardziej pokrętnym spośród znanych autorowi sposobów sprawdzania nietrywialności jądra homomorfizmu.

Krok VII: Jeżeli $P \in \mathbb{P}_F$ jest punktem stopnia 1 różnym od Q, to:

$$\bigwedge_{x \in \ker \lambda \setminus \{0\}} x(P) = 0 \ \square$$

Dowód kroku VII: Ustalmy punkt $P \in \mathbb{P}_F$ różny od punktu Q i stopnia 1. Zauważmy wpierw, iż dla wszelkich $x \in \mathcal{L} \setminus \{0\}$ $x(P) \neq \infty$; faktycznie, dla ustalonego $x \in \mathcal{L} \setminus \{0\}$ $x(P) = \infty$ wtedy i tylko wtedy, gdy $v_P(x) < 0$, czyli gdy $P = Q$, bowiem Q jest jedymym biegunem elementu x.

Dalej, odnotujmy, że dla wszelkich $x \in \mathcal{L} \setminus \{0\}$ $x(P)^q = x(P)$. Rzeczywiście, skoro P jest punktem stopnia 1, to $F_P \cong \mathbb{F}_q$, skąd wynika nasze spostrzeżenie.

Teraz ustalmy $x = \sum_{i \in T} u_i z_i^{q_0} \in \ker \lambda$, gdzie $u_i \in \mathcal{B}$, $z_i \in \mathcal{L}(nQ)$, $i \in T$ i policzmy:

$$\begin{aligned}
x(P)^{q_0} &= \left((\sum_{i \in T} u_i z_i^{q_0})(P) \right)^{q_0} = \\
&= \left(\sum_{i \in T} u_i(P)(z_i(P))^{q_0} \right)^{q_0} = \\
&= \sum_{i \in T} (u_i(P))^{q_0} (z_i(P))^q = \\
&= \sum_{i \in T} u_i^{q_0}(P) z_i(P) = \\
&= \left(\sum_{i \in T} u_i^{q_0} z_i \right)(P) = \\
&= 0(P) = 0
\end{aligned}$$

Tym bardziej więc $x(P)^q = 0$ i $x(P) = 0$. $\square$

Krok VIII: Przy powyższych oznaczeniach zachodzi oszacowanie:

$$N < (q+1) + (2g+1)\sqrt{q} \ \square$$

Dowód kroku VIII: Jak pokazaliśmy w kroku VII, istnieje niezerowy element $x \in \mathcal{L}$ taki, że dla dowolnego punktu stopnia 1 $P \in \mathbb{F}_P$ różnego od Q zachodzi równość $x(P) = 0$. Wobec tego $\mathsf{deg}\,(x)_0 \geqslant N - 1$. Ponadto, ponieważ $x \in \mathcal{L} \subseteq \mathcal{L}(rQ)$, więc wobec tezy (2) twierdzenia 1.1.6 i definicji przestrzeni $\mathcal{L}(rQ)$:

$$\mathsf{deg}\,(x)_0 = \mathsf{deg}\,(x)_\infty \leqslant r = q - 1 + (2g+1)q_0$$

skąd $N - 1 \leqslant q - 1 + (2g+1)\sqrt{q}$, co dowodzi naszej tezy. $\square$

Podsumujmy dotychczasowe dokonania. W kroku I pokazaliśmy, że zamiast dla konkretnego ciała $F/\mathbb{F}_q$ twierdzenia Hasse'go - Weil'a możemy dowodzić dla dowolnie wybranego rozszerzenia $F_r/\mathbb{F}_{q^r}$ tego ciała. Wcześniej udowodniliśmy, iż rodzaj ciała przy przejściu do rozszerzenia ciała stałych nie ulega zmianie. Wybraliśmy więc takie rozszerzenie, dla którego q^r jest kwadratem większym od $(g+1)^4$ i - dla uproszczenia zapisu - ciało takie oznaczali po prostu przez $F/\mathbb{F}_q$. W kroku VIII udowodniliśmy, że dla tak wybranego ciała zachodzi oszacowanie $N < (q+1)+(2g+1)\sqrt{q}$. Zauważmy jednak, że jeśli q jest kwadratem i $q > (g+1)^4$, to również q^r jest kwadratem i $q^r > (g+1)^4$, dla $r \geqslant 1$, tak więc takie samo oszacowanie zachodzi dla

wszelich rozszerzeń F_r/F_{q^r} naszego ciała. Pokazuje to górne oszacowanie z kroku III dla ciał $F/\mathbb{F}_q$, gdzie q jest kwadratem i $q > (g+1)^4$.

Przechodzimy do dowodu dolnego oszacowania. Wróćmy na chwilę do pierwotnych założeń, tzn. chwilowo o liczbie q niczego nie zakładamy.

Krok IX: Istnieje podciało $F_0 = \mathbb{F}_q(t) \subseteq F$ ciała F oraz rozszerzenie $E \supseteq F$ ciała F takie, że rozszerzenie $F \supseteq F_0$ jest skończone i rozdzielcze, zaś $E \supseteq F_0$ jest skończonym rozszerzeniem Galois.

Dowód kroku IX: Korzystając z twierdzenia 1.1.5 stwierdzamy, że w ciele F istnieje co najmniej jeden punkt. Z definicji waluacji istnieje element $t \in F$ taki, że $v_P(t) = 1$, gdzie v_P jest waluacją związaną z punktem P. W szczególności więc $v_P(t) \not\equiv 0(\mathsf{mod}\, q)$ i na podstawie twierdzenia 2.4.1 rozszerzenie $F \supseteq \mathbb{F}_q(t)$ jest rozdzielcze i skończone. Teraz za ciało E wystarczy wziąć domknięcie Galois rozszerzenia $F \supseteq \mathbb{F}_q(t)$ (por. [**3**] twierdzenie III.2.3.10). ❑

Przyjmijmy oznaczenia z kroku IX i dla $r \geqslant 1$ rozważmy wieżę rozszerzeń:

$$E/K_r \supseteq F_r/\mathbb{F}_{q^r} \supseteq F_0\mathbb{F}_{q^r} = \mathbb{F}_{q^r}(t)/\mathbb{F}_{q^r}$$

Krok X: Przy powyższych oznaczeniach, dla wszystkich $r \geqslant 1$:

(1) $K_r = \mathbb{F}_{q^r}$ jest ciałem stałych dla E.
(2) $E \supseteq \mathbb{F}_{q^r}(t)$ jest rozszerzeniem Galois, a $F_r/ \supseteq \mathbb{F}_{q^r}(t)$ jest rozszerzeniem rozdzielczym.

Dowód kroku X: Ustalmy liczbę $r \geqslant 1$. Poprawność doboru ciał stałych wynika z tez (2) i (3) twierdzenia 2.1.1. To, że rozszerzenie $F_r/ \supseteq \mathbb{F}_{q^r}(t)$ jest skończonym rozszerzeniem rozdzielczym sprawdzamy powtarzając argumenty z dowodu kroku IX. W końcu fakt, że $E \supseteq \mathbb{F}_{q^r}(t)$ jest rozszerzeniem Galois wynika ze znanego z wykładu algebry twierdzenia (por. [**3**] twierdzenie III.2.3.11 (3)). ❑

W kroku X stwierdziliśmy, że własności rozszerzeń skonstruowanych w kroku IX zachowają się przy przejściu do rozszerzeń ciał stałych. Możemy więc dalszy dowód prowadzić dla rozszerzenia $F_r/\mathbb{F}_{q^r}$ takiego, że q^r jest kwadratem i $q^r > (g+1)^4$. Podobnie jak wcześniej, zamiast q^r będziemy pisać po prostu q.

Rozważmy rozszerzenie Galois $E/F_q \supseteq F/F_q$ (jest to istotnie rozszerzenie Galois, gdyż F jest ciałem pośrednim rozszerzenia Galois). Niech $[E : F] = m$, $[E : F_0] = n$. Oczywiście $m|n$ i oznaczmy:

$$E' = E\mathbb{F}_{q^n}/\mathbb{F}_{q^n},\ F' = F\mathbb{F}_{q^n},\ F'_0 = F_0\mathbb{F}_{q^n}$$

Krok XI: Przy powyższych oznaczeniach:

(1) $E' \supset F$ jest rozszerzeniem Galois stopnia $m{\cdot}n$ o grupie Galois $\mathsf{Gal}\,(E'/F) =< \sigma > \times \mathsf{Gal}\,(E'/F') \cong < \sigma > \times \mathsf{Gal}\,(E/F)$ gdzie σ jest automorfizmem Frobeniusa rozszerzenia $E' \supseteq E$.
(2) $\mathsf{Gal}\,(E'/F)$ zawiera dokładnie m podgrup cyklicznych $V_1, \ldots, V_m$ rzędu n takich, że $V_i \cap \mathsf{Gal}\,(E'/F') = \{1\}$, dla $i \in \{1, \ldots, m\}$.
(3) F ma dokładnie m rozszerzeń stopnia m $E_1^{(1)}, \ldots, E_m^{(1)}$ takich, że $[E' : E_i^{(1)}] = n$, $E' \supset E_i^{(1)}$ jest cykliczne oraz $\mathsf{Gal}\,(E'/E_i^{(1)}) \cong V_i$ dla $i \in \{1, \ldots, m\}$. Możemy przy tym założyć, że $E_1^{(1)} = E$.
(4) $\mathbb{F}_q$ jest ciałem stałych dla $E_i^{(1)}/\mathbb{F}_q$.
(5) Jeżeli oznaczymy przez $g(E_i^{(1)})$ rodzaj ciała $E_i^{(1)}$, $i \in \{1, \ldots, m\}$, a przez $g(E)$ rodzaj ciała E, to:

$$E' = E_i^{(1)}\mathbb{F}_{q_n}/\mathbb{F}_{q^n} \text{ oraz } g(E_i^{(1)}) = g(E) \text{ dla } i \in \{1, \ldots, m\}$$

(6) Jeżeli oznaczymy przez $N(F)$ liczbę punktów stopnia 1 ciała F, a przez $N(E_i^{(1)})$ liczbę punktów stopnia 1 ciała $E_i^{(1)}$, $i \in \{1, \dots, m\}$, to:

$$m \cdot N(F) = \sum_{i=1}^{m} N(E_i^{(1)})$$

Krok XII: Przy powyższych oznaczeniach:

(1) $E' \supset F_0$ jest rozszerzeniem Galois stopnia $n \cdot n$ o grupie Galois $\mathsf{Gal}\,(E'/F_0) =< \sigma > \times \mathsf{Gal}\,(E'/F_0') \cong < \sigma > \times \mathsf{Gal}\,(E/F_0)$ gdzie σ jest automorfizmem Frobeniusa rozszerzenia $E' \supseteq E$.
(2) $\mathsf{Gal}\,(E'/F_0)$ zawiera dokładnie n podgrup cyklicznych $U_1, \dots, U_m$ rzędu n takich, że $U_i \cap \mathsf{Gal}\,(E'/F_0') = \{1\}$, dla $i \in \{1, \dots, n\}$.
(3) F_0 ma dokładnie n rozszerzeń stopnia n $E_1, \dots, E_m$ takich, że $[E' : E_i] = n$, $E' \supset E_i$ jest cykliczne oraz $\mathsf{Gal}\,(E'/E_i) \cong U_i$ dla $i \in \{1, \dots, n\}$. Możemy przy tym założyć, że $E_1 = E$.
(4) $\mathbb{F}_q$ jest ciałem stałych dla $E_i/\mathbb{F}_q$.
(5) Jeżeli oznaczymy przez $g(E_i)$ rodzaj ciała E_i, $i \in \{1, \dots, n\}$, a przez $g(E)$ rodzaj ciała E, to:

$$E' = E_i\mathbb{F}_{q_n}/\mathbb{F}_{q^n} \text{ oraz } g(E_i) = g(E) \text{ dla } i \in \{1, \dots, n\}$$

(6) Jeżeli oznaczymy przez $N(F_0)$ liczbę punktów stopnia 1 ciała F_0, a przez $N(E_i)$ liczbę punktów stopnia 1 ciała E_i, $i \in \{1, \dots, n\}$, to:

$$n \cdot N(F_0) = \sum_{i=1}^{n} N(E_i)$$

Dowody tych kroków wynikają bezpośrednio z lematu 3.2.2. Przyjmijmy powyższe oznaczenia.

Krok XIII: Zmieniając ewentualnie numerację możemy założyć, że $V_i = U_i$ oraz $E_i^{(1)} = E_i$ dla $i \in \{1, \dots, m\}$.

Dowód kroku XIII: Ustalmy $i \in \{1, \dots, m\}$. Zauważmy, że $E' = E_i^{(1)}\mathbb{F}_{q^n} \subseteq E_i^{(1)}F_0\mathbb{F}_{q^n} = E_i^{(1)}F_0' \subseteq E'E' = E'$, czyli $E' = E_i^{(1)}F_0$. Rozważmy wieże ciał $E' \supseteq E_i^{(1)} \supseteq F \supseteq F_0$ oraz $E' \supseteq F' \supseteq F_0' \supseteq F_0$. Na podstawie wielokrotnie już wykorzystywanego twierdzenia z kursu algebry (por. [**3**] twierdzenie III.3.2.5 (1)) mamy:

$$\{1\} = \mathsf{Gal}\,(E'/E_i^{(1)}F_0') = \mathsf{Gal}\,(E'/E_i^{(1)}) \cap \mathsf{Gal}\,(E'/F_0') = V_i \cap \mathsf{Gal}\,(E'/F_0')$$

więc $V_i \in \{U_1, \dots, U_n\}$ i tym samym $E_i^{(1)} \in \{E_1, \dots, E_n\}$. ❑

Krok XIV: Przy powyższych oznaczeniach i założeniach:

$$N(F) \geqslant q + 1 - \tfrac{n-m}{m}(2g(E) + 1)\sqrt{q}$$ ❑

Dowód kroku XIV: Na podstawie rezultatów z kroków XI - XIII możemy napisać:

$$m \cdot N(F) = \sum_{i=1}^{m} N(E_i)$$

oraz:

$$n \cdot N(F_0) = \sum_{i=1}^{n} N(E_i)$$

Dalej, ponieważ dla wszystkich $i \in \{1, \dots, n\}$ rodzaje ciał E_i oraz E są równe, a także ciałem stałych dla wszelkich E_i jest $\mathbb{F}_q$ to - skoro, zgodnie z poczynionym założeniem, q jest kwadratem i $q > (g+1)^4$ - na podstawie kroku VIII:

$$\bigwedge_{i \in \{1,\dots,n\}} N(E_i) \leqslant q + 1 + (2g(E) + 1)\sqrt{q}$$

Ponadto, na podstawie uwagi 1.2.1 i twierdzenia 1.2.1 punkty stopnia 1 ciała F_0 są - jako punkty ciała funkcji wymiernych - we wzajemnie jednoznacznej odpowiedniości ze zbiorem $\mathbb{F}_q \cup \{\infty\}$, tak więc $N(F_0) = q + 1$. Ostatecznie:

$$\begin{aligned} m \cdot N(F) &= \sum_{i=1}^{m} N(E_i) + n\dot{N}(F_0) - \sum_{i=1}^{n} N(E_i) = \\ &= n(q+1) - \sum_{i=m+1}^{n} N(E_i) \geqslant \\ &= n(q+1) - (n-m)(q+1) - (n-m)(2g(E)+1)\sqrt{q} = \\ &= m(q+1) - (n-m)(2g(E)+1)\sqrt{q} \end{aligned}$$

skąd:

$$N(F) \geqslant q + 1 - \tfrac{n-m}{m}(2g(E)+1)\sqrt{q} \ \square$$

Podsumujmy dotychczasowe rezultaty. W kroku XIV pokazaliśmy, iż dla ciała $F/\mathbb{F}_q$ dla którego q jest kwadratem większym od $(g+1)^4$ zachodzi oszacowanie $N \geqslant q + 1 - c_1\sqrt{q}$. Oczywiście przy takich założeniach $F_r/\mathbb{F}_{q^r}$, $r \geqslant 1$, q^r także jest kwadratem i $q^r > (g+1)^4$. Tak więc $N_r \geqslant q^r + 1 - c_1\sqrt{q^r}$ dla wszelkich $r \geqslant 1$. To, w połączeniu z wynikiem kroku VIII, pozwala stwierdzić, że dla ciał $F/\mathbb{F}_q$ dla których q jest kwadratem większym od $(g+1)^4$ zachodzą oszacowania:

$$\bigvee_{c_1 \in \mathbb{R}} \bigwedge_{r \in \mathbb{N}} N_r \leqslant q^r + 1 + c_1\sqrt{q^r}$$
$$\bigvee_{c_2 \in \mathbb{R}} \bigwedge_{r \in \mathbb{N}} N_r \geqslant q^r + 1 - c_1\sqrt{q^r}$$

a zatem - wobec kroków II i III - twierdzenie Hasse'go - Weil'a jest prawdziwe dla takiego rodzaju ciał. Ale ciałami takimi są też rozszerzenia ciał stałych dowolnych ciał $F/\mathbb{F}_q$, co na mocy kroku I dowodzi twierdzenia w pełnej ogólności. To definitywnie kończy dowód. *QED*

3. Hipoteza Riemanna dla ciał funkcji algebraicznych

Twierdzenie Hasse'go - Weil'a bywa też nazywane hipotezą Riemanna dla ciał funkcji algebraicznych. W tym paragrafie postaramy się w kilku słowach wyjaśnić dlaczego. Tak jak wcześniej ustalmy liczbę naturalną (będącą potęgą liczby pierwszej) q i niech $F/\mathbb{F}_q$ będzie ciałem funkcji algebraicznych o rodzaju g. Niech:

$$\bigwedge_{n \in \mathbb{N}} (A_n = |\{A \in \mathcal{D}_F : A \geqslant 0 \wedge \deg A = n\}|)$$

oraz niech $Z_F : \mathbb{C} \to \mathbb{C}$ będzie funkcją dzeta ciała funkcji algebraicznych $F/\mathbb{F}_q$ daną wzorem:

$$Z_F(t) = \sum_{n=0}^{\infty} A_n t^n$$

zaś:

$$L_F(t) = (1-t)(1-qt)Z_F(t)$$

będzie L-wielomianem ciała funkcji algebraicznych F/F_q. Oznaczmy przez:

$$\alpha_1, \ldots, \alpha_{2g}$$

odwrotności pierwiastków L-wielomianu. Wprowadźmy dwie nowe definicje:

DEFINICJA 3.3.1. *Niech $A \in \mathcal{D}_F$. Liczbę $\mathfrak{N}(A) = q^{\deg A}$ nazywamy* **bezwzględną normą** *dywizora.*

DEFINICJA 3.3.2. *Funkcję $\zeta_F : \mathbb{C} \to \mathbb{C}$ daną wzorem:*

$$\zeta_F(t) = Z_F(q^{-t}),\ dla\ t \in \mathbb{C}$$

nazywamy **funkcją ζ-Riemanna** *ciała funkcji algebraicznych $F/\mathbb{F}_q$.*

Funkcja ζ_F jest - można tak powiedzieć - stuprocentową analogią "zwykłej" funkcji Riemanna $\zeta(t) = \sum_{n=0}^{\infty} n^{-t}$ - zauważmy, że można ją zapisać w formie:

$$\zeta_F(t) = \sum_{n=0}^{\infty} A_n q^{-sn} = \sum_{n=0}^{\infty} A_n (q^n)^{-s} = \sum_{A \in \mathcal{D}_F, A \geqslant 0} \mathfrak{N}(A)^{-s}$$

Pokażemy następujące twierdzenie, łatwo wynikające z twierdzenia Hasse'go - - Weil'a, które jest naturalnym analogonem klasycznej hipotezy Riemanna:

TWIERDZENIE 3.3.1. *Przy powyższych oznaczeniach wszystkie zera funkcji ζ_F leżą na prostej* $\mathsf{Re}\,(t) = \frac{1}{2}$

D o w ó d : Faktycznie, z definicji i z twierdzenia Hasse'go - Weil'a mamy:

$$\begin{aligned}
\zeta_F(t) = 0 \quad &\iff \quad Z_F(q^{-t}) = 0 \iff \\
&\iff \quad q^t \text{jest odwrotnością pierwiastka } L\text{-wielomianu} \implies \\
&\implies \quad |q^t| = \sqrt{q} \implies \\
&\implies \quad q^{\mathrm{Re}\, t} = q^{\frac{1}{2}} \implies \\
&\implies \quad \mathsf{Re}\, t = \frac{1}{2}
\end{aligned}$$

co kończy dowód twierdzenia. *QED*

ROZDZIAŁ 4

Krzywe algebraiczne

1. Rozmaitości afiniczne i rzutowe

W tym paragrafie zdefiniujemy podstawowe pojęcia geometrii algebraicznej, w szczególności powiemy, co to są zbiory algebraiczne i rozmaitości algebraiczne. Podamy też pewne ogólnie znane fakty tej teorii, które w większości pozostawimy bez dowodu, odsyłając tylko do odpowiedniej literatury - autor posługiwał się głównie podręcznikiem Fultona [**7**], choć symbolika użyta w tej pracy różni się istotnie od stosowanej w literaturze i dopasowana jest do przyjętych wcześniej oznaczeń.

Niech F będzie dowolnym ciałem, niech $\overline{F}$ będzie jego domknięciem algebraicznym. Symbolem $\mathbb{A}^n(F)$ oznaczać będziemy n-wymiarową przestrzeń afiniczną nad ciałem F, a symbolem $\mathbb{P}^n(F)$ $n-$wymiarową przestrzeń rzutową nad ciałem F. Przestrzenie dwuwymiarowe nazywać będziemy po prostu płaszczyznami. Podstawową dla nas definicją będzie:

DEFINICJA 4.1.1. (1) **Zbiorem algebraicznym afinicznym** V *nazywamy zbiór:*

$$V = \{(a_1, \ldots, a_n) \in \mathbb{A}^n(\overline{F}) : f(a_1, \ldots, a_n) = 0, f \in M\}$$

gdzie M jest zbiorem wielomianów z pierścienia $\overline{F}[X_1, \ldots, X_n]$.

(2) **Zbiorem algebraicznym rzutowym** V^* *nazywamy zbiór:*

$$V^* = \{(a_1 : \ldots : a_{n+1}) \in \mathbb{P}^n(\overline{F}) : f(a_1, \ldots, a_{n+1}) = 0, f \in M\}$$

gdzie M jest zbiorem wielomianów jednorodnych z pierścienia $\overline{F}[X_1, \ldots, X_{n+1}]$.

Ogólnie przestrzegać będziemy następującej zasady: wszystkie obiekty związane z przestrzenią rzutową wyróżniać będziemy symbolem "$*$". Mając dany jeden zbiór algebraiczny można zastanawiać się, czy zbiór M wielomianów ją definiujących można jakoś powiększyć. Okazuje się, że tak - zbiór wszystkich wielomianów, które zerują się na danym zbiorze algebraicznym tworzy - o czym nietrudno się przekonać - ideał w pierścieniu wielomianów. Uprawomocnia to wprowadzenie kolejnej definicji:

DEFINICJA 4.1.2. (1) *Niech $V \subseteq \mathbb{A}^n(\overline{F})$ będzie afinicznym zbiorem algebraicznym. Ideał:*

$$\mathcal{I}(V) = \{f \in \overline{F}[X_1, \ldots, X_n] : f(a_1, \ldots, a_n) = 0, (a_1, \ldots, a_n) \in V\}$$

nazywamy **ideałem stowarzyszonym** *ze zbiorem V.*

(2) *Niech $V^* \subseteq \mathbb{P}^n(\overline{F})$ będzie rzutowym zbiorem algebraicznym. Ideał:*

$$\mathcal{I}(V^*) = \{f \in \overline{F}[X_1, \ldots, X_{n+1}] : f(a_1, \ldots, a_{n+1}) = 0, (a_1 : \ldots : a_{n+1}) \in V^*, f \text{ jednorodny}\}$$

nazywamy **ideałem stowarzyszonym** *ze zbiorem* V^*.

Zmierzamy teraz do zdefiniowania pojęcia rozmaitości algebraicznej i podania pewnej jej charakteryzacji. Najpierw jednak powiemy, co to są zbiory nierozkładalne.

DEFINICJA 4.1.3. (1) *Afiniczny zbiór algebraiczny nazywamy* **zbiorem nierozkładalnym**, *jeżeli nie jest sumą dwóch właściwych, różnych od niego afinicznych zbiorów algebraicznych.*
(2) *Rzutowy zbiór algebraiczny nazywamy* **zbiorem nierozkładalnym**, *jeżeli nie jest sumą dwóch właściwych, różnych od niego rzutowych zbiorów algebraicznych.*

Rozmaitość algebraiczną określa się teraz w całkowicie naturalny sposób:

DEFINICJA 4.1.4. (1) *Afiniczny zbiór algebraiczny nazywamy* **rozmaitością afiniczną**, *jeżeli jest nierozkładalnym afinicznym zbiorem algebraicznym.*
(2) *Rzutowy zbiór algebraiczny nazywamy* **rozmaitością rzutową**, *jeżeli jest nierozkładalnym rzutowym zbiorem algebraicznym.*

Przydatne będzie następujące kryterium rozstrzygające, czy dany zbiór algebraiczny jest, czy też nie jest rozmaitością:

TWIERDZENIE 4.1.1. (1) *Warunkiem koniecznym i wystarczającym na to, by afiniczny zbiór alebraiczny* V *był rozmaitością jest, iżby ideał* $\mathcal{I}(V)$ *był ideałem pierwszym.*
(2) *Warunkiem koniecznym i wystarczającym na to, by rzutowy zbiór alebraiczny* V^* *był rozmaitością jest, iżby ideał* $\mathcal{I}(V^*)$ *był ideałem pierwszym.*

D o w ó d : (por. [**15**] twierdzenie 6.2.1 dla wersji afinicznej i [**7**] str. 91 dla wersji rzutowej).

Można pokazać, że każdy zbiór algebraiczny jest sumą odpowiedniej liczby rozmaitości. W dalszym ciągu będziemy się więc zajmować wyłącznie rozmaitościami algebraicznymi. W pierwszej kolejności wprowadzimy pewne struktury algebraiczne na rozmaitości - mianowicie pierścień współrzędnych i ciało funkcji wymiernych.

DEFINICJA 4.1.5. (1) *Niech* $V \subseteq \mathbb{A}^n(\overline{F})$ *będzie rozmaitością afiniczną. Pierścień:*

$$\overline{F}[V] = \overline{F}[X_1, \ldots, X_n]/\mathcal{I}(V)$$

nazywamy **pierścieniem współrzędnych** *na rozmaitości* V.
(2) *Niech* $V^* \subseteq \mathbb{P}^n(\overline{F})$ *będzie rozmaitością rzutową. Pierścień:*

$$\overline{F}_h[V^*] = \overline{F}[X_1, \ldots, X_{n+1}]/\mathcal{I}(V^*)$$

nazywamy **pierścieniem współrzędnych** *na rozmaitości* V^*.

W literaturze spotyka się też określenie "pierścień funkcji regularnych", wydaje się jednak, że nazwanie tego pierścienie pierścieniem współrzędnych jest bardziej trafne, nie sugeruje bowiem o jaki rodzaj regularności nam chodzi. Wobec znanego z kursu algebry twierdzenia (por. [**2**] twierdzenie I.2.4.6) jasne jest, że pierścienie współrzędnych tak rozmaitości afinicznych jak i rzutowych są pierścieniami całkowitymi, można więc rozpatrywać ich ciała ułamków.

DEFINICJA 4.1.6. (1) *Niech $V \subseteq \mathbb{A}^n(\overline{F})$ będzie rozmaitością afiniczną. Ciało ułamków pierścienia współrzędnych nazywamy* **ciałem funkcji wymiernych** *na rozmaitości i oznaczamy $\overline{F}(V)$.*

(2) *Niech $V^* \subseteq \mathbb{P}^n(\overline{F})$ będzie rozmaitością rzutową. Ciało ułamków pierścienia współrzędnych nazywamy* **ciałem homogenicznych funkcji wymiernych** *na rozmaitości i oznaczamy $\overline{F}_h(V^*)$.*

(3) *Niech $V^* \subseteq \mathbb{P}^n(\overline{F})$ będzie rozmaitością rzutową oraz $\overline{F}_h(V^*)$ ciałem homogenicznych funkcji wymiernych na rozmaitości. Podciało:*

$$\overline{F}(V^*) = \{z \in \overline{F}_h(V^*) : z = \frac{f}{g}, f, g \in \overline{F}_h[V^*], \deg f = \deg g, f, g \text{ są formami}\}$$

nazywamy **ciałem funkcji wymiernych** *na rozmaitości, przy czym stopień elementu pierścienia współrzędnych rozumiemy jako stopień dowolnego reprezentanta warstwy, czyli wielomianu.*

Bez trudu sprawdzamy poprawność przyjętych definicji. Jest dosyć oczywistym spostrzeżeniem, że ciała funkcji wymiernych na rozmaitości są rozszerzeniami ciał $\overline{F}$. Z konieczności też muszą być to rozszerzenia przestępne. Pozwala to wprowadzić nam pojęcie wymiaru rozmaitości.

DEFINICJA 4.1.7. (1) *Niech $V \subseteq \mathbb{A}^n(\overline{F})$ będzie rozmaitością afiniczną. Stopień przestępny rozszerzenia $\overline{F}(V) \supseteq \overline{F}$ nazywamy* **wymiarem rozmaitości**.

(2) *Niech $V^* \subseteq \mathbb{P}^n(\overline{F})$ będzie rozmaitością rzutową. Stopień przestępny rozszerzenia $\overline{F}(V^*) \supseteq \overline{F}$ nazywamy* **wymiarem rozmaitości**.

Wśród podpierścieni ciał funkcji wymiernych na rozmaitościch będziemy chcieli wyróżnić pewne szczególne pierścienie związane geometrycznie z punktami rozmaitości.

DEFINICJA 4.1.8. (1) *Niech $V \subseteq \mathbb{A}^n(\overline{F})$ będzie rozmaitością afiniczną, niech $P \in V$. Funkcję wymierną na rozmaitości $z \in \overline{F}(V)$ nazywamy* **określoną w punkcie** *P wtedy i tylko wtedy, gdy istnieje przedstawienie $z = \frac{f}{g}$, $f, g \in \overline{F}[V]$ dla którego $g(P) \neq 0$. Zbiór wszystkich funkcji określonych w danym punkcie oznaczamy $\overline{F}_P[V]$ i nazywamy* **pierścieniem lokalnym** *punktu P.*

(2) *Niech $V^* \subseteq \mathbb{P}^n(\overline{F})$ będzie rozmaitością rzutową, niech $P \in V^*$. Funkcję wymierną na rozmaitości $z \in \overline{F}(V^*)$ nazywamy* **określoną w punkcie** *P wtedy i tylko wtedy, gdy istnieje przedstawienie $z = \frac{f}{g}$, $f, g \in \overline{F}_h[V^*]$ dla którego $g(P) \neq 0$. Zbiór wszystkich funkcji określonych w danym punkcie oznaczamy $\overline{F}_P[V^*]$ i nazywamy* **pierścieniem lokalnym** *punktu P.*

Bez kłopotu sprawdzamy, że dla danego punktu $P \in V$ ($P \in V^*$) $\overline{F}_P[V]$ ($\overline{F}_P[V^*]$) faktycznie jest pierścieniem. Można się też przekonać, że istotnie jest to pierścień lokalny (por. [**7**] str. 44 dla przypadku afinicznego i str. 93 dla przypadku rzutowego). Tak więc pierścień lokalny punktu ma dokładnie jeden ideał maksymalny, dzięki czemu możemy podać kolejną definicję.

DEFINICJA 4.1.9. (1) *Niech $V \subseteq \mathbb{A}^n(\overline{F})$ będzie rozmaitością afiniczną, niech $P \in V$. Jedyny ideał maksymalny pierścienia lokalnego punktu P, $\overline{F}_P[V]$, oznaczamy $M_P(V)$ i nazywamy* **punktem** *ciała funkcji wymiernych $\overline{F}(V)$.*

(2) *Niech $V^* \subseteq \mathbb{P}^n(\overline{F})$ będzie rozmaitością rzutową, niech $P \in V^*$. Jedyny ideał maksymalny pierścienia lokalnego punktu P, $\overline{F}_P[V^*]$, oznaczamy $M_P(V^*)$ i nazywamy* **punktem** *ciała funkcji wymiernych $\overline{F}(V^*)$.*

Pojawia się tutaj pewien kłopot z dualnością oznaczeń. Mianowicie z jednej strony punktami nazywamy pewne obiekty geometryczne, a z drugiej - pewne konstrukcje algebraiczne. Kłopot ten znika w literaturze anglojęzycznej, gdzie punkty na rozmaitości to po prostu *points*, a punkty ciała funkcji wymiernych to *places* - my, niestety, będziemy musieli jakoś przyzwyczaić się do tej drobnej niedogodności. Pod koniec tego rozdziału okaże się jednak, że w pewnych przypadkach pojęcia te można utożsamiać.

2. Krzywe algebraiczne

Niech, tak jak wcześniej, F będzie dowolnym ciałem, niech $\overline{F}$ będzie jego domknięciem algebraicznym.

Definicja 4.2.1. (1) **Afiniczną krzywą algebraiczną** *nazywamy rozmaitość afiniczną $C \subseteq \mathbb{A}^n(\overline{F})$ wymiaru 1. Jeżeli ponadto jest to rozmaitość na płaszczyźnie afinicznej, to nazywamy ją* **afiniczną krzywą algebraiczną płaską.**

(2) **Rzutową krzywą algebraiczną** *nazywamy rozmaitość rzutową $C^* \subseteq \mathbb{P}^n(\overline{F})$ wymiaru 1. Jeżeli ponadto jest to rozmaitość na płaszczyźnie rzutowej, to nazywamy ją* **rzutową krzywą algebraiczną płaską.**

Definicja ta odbiega nieco od naszej intuicji, wyobrażamy sobie bowiem krzywe na ogół jako miejsca zerowe wielomianów wielu zmiennych w ciele algebraicznie domkniętym (na przykład $\mathbb{C}$). Okazuje się jednak, że w tym wypadku intuicja nas nie zawodzi, ponieważ możemy podać elegancką charakteryzację krzywych algebraicznych:

Twierdzenie 4.2.1. (1) *Na to, aby rozmaitość $C \subseteq \mathbb{A}^2(\overline{F})$ była afiniczną krzywą algebraiczną płaską potrzeba i wystarcza, iżby $C = \{(a,b) \in \mathbb{A}^2(\overline{F}) : f(a,b) = 0\}$, gdzie $f \in \overline{F}[X,Y]$ jest wielomianem nierozkładalnym.*

(2) *Na to, aby rozmaitość $C^* \subseteq \mathbb{P}^2(\overline{F})$ była rzutową krzywą algebraiczną płaską potrzeba i wystarcza, iżby $C^* = \{(a:b:c) \in \mathbb{P}^2(\overline{F}) : f(a,b,c) = 0\}$, gdzie $f \in \overline{F}[X,Y,Z]$ jest wielomianem nierozkładalnym i jednorodnym.*

D o w ó d : (por. [**7**] str. 150). Twierdzenie to uogólnia się na wszystkie rodzaje krzywych, można bowiem pokazać, że dowolna krzywa jest biwymiernie równoważna z pewną krzywą płaską - nie będziemy jednak definiować tu pojęcia biwymiernej równoważności i wchodzić w szczegóły tej teorii.

W świetle powyższego twierdzenia wprowadzamy następującą notację; mianowicie symbol:

$$C : f(X,Y) = 0$$

oznaczać będzie afiniczną krzywą płaską $C = \{(a,b) \in \mathbb{A}^2(\overline{F}) : f(a,b) = 0\}$, gdzie $f \in \overline{F}[X,Y]$ jest wielomianem nierozkładalnym, zaś

$$C^* : f(X,Y,Z) = 0$$

oznaczać będzie rzutową krzywą płaską $C^* = \{(a:b:c) \in \mathbb{P}^2(\overline{F}) : f(a,b,c) = 0\}$, gdzie $f \in \overline{F}[X,Y,Z]$ jest wielomianem nierozkładalnym i jednorodnym.

Wśród punktów na krzywych wyróżnimy teraz dwie ważne klasy:

DEFINICJA 4.2.2. (1) *Niech $C : f(X,Y) = 0$ będzie krzywą afiniczną. Punkt $P \in C$ nazywamy* **nieosobliwym**, *jeżeli:*

$$\frac{\partial f}{\partial X}(X,Y) \restriction_P \neq 0 \text{ lub } \frac{\partial f}{\partial Y}(X,Y) \restriction_P \neq 0$$

Punkt nazywamy **osobliwym**, *gdy nie jest nieosobliwy. Krzywą, której wszystkie punkty są nieosobliwe, nazywamy* **krzywą nieosobliwą**.

(2) *Niech $C^* : f(X,Y,Z) = 0$ będzie krzywą rzutową. Punkt $P \in C^*$ nazywamy* **nieosobliwym**, *jeżeli:*

$$\frac{\partial f}{\partial X}(X,Y,Z) \restriction_P \neq 0 \text{ lub } \frac{\partial f}{\partial Y}(X,Y,Z) \restriction_P \neq 0 \text{ lub } \frac{\partial f}{\partial Z}(X,Y,Z) \restriction_P \neq 0$$

Punkt nazywamy **osobliwym**, *gdy nie jest nieosobliwy. Krzywą, której wszystkie punkty są nieosobliwe, nazywamy* **krzywą nieosobliwą**.

Jasne jest, że w powyższej definicji symbol różniczkowania oznacza formalne różniczkowanie wielomianów i nie ma nic wspólnego z różniczkowaniem rozumianym w sensie analizy matematycznej - tutaj $\overline{F}$ jest, najogólniej, dowolnym ciałem, w związku z czym nie sposób wprowadzać w przestrzeniach $\mathbb{A}^2(\overline{F})$ tudzież $\mathbb{P}^2(\overline{F})$ jakichkolwiek topologii i mówić o ciągłości.

Wprowadzone pojęcia pozwalają nam podać teraz kilka przykładów krzywych algebraicznych.

`Przykłady:`

(1) **Krzywe stożkowe**. Krzywymi stożkowymi nazywamy krzywe afiniczne (lub rzutowe) $C : f(X,Y) = 0$ ($C^* : f(X,Y,Z) = 0$, odpowiednio), gdzie f jest wielomianem stopnia 2. Szczegółowa dyskusja dotycząca właściwości takich krzywych wraz z pełną ich klasyfikacją przeprowadzana jest na kursowym wykładzie algebry liniowej.

(2) **Krzywe sześcienne**. Krzywymi sześciennymi nazywamy krzywe afiniczne (lub rzutowe) $C : f(X,Y) = 0$ ($C^* : f(X,Y,Z) = 0$, odpowiednio), gdzie f jest wielomianem stopnia 3.

(3) **Krzywe eliptyczne**. Krzywymi eliptycznymi nazywamy nieosobliwe krzywe postaci $C : Y^2 - f(X) = 0$, gdzie f jest wielomianem stopnia 3 mającym 3 różne miejsca zerowe w $\overline{F}$. Istnieje wiele równoważnych definicji krzywej eliptycznej, my podaliśmy tu jedną z nich. Krzywe eliptyczne odgrywają szczególnie ważną rolę w teorii liczb; posługując się zaawansowanymi metodami teorii krzywych eliptycznych udowodniono między innymi Wielkie Twierdzenie Fermata oraz podano warunek konieczny i dostateczny na to, aby dana liczba naturalna była liczbą kongruentną. Także wiele algorytmów faktoryzacyjnych (na przykład algorytmy Pollarda, Lenstry) wykorzystuje techniki krzywych eliptycznych.

(4) **Krzywe hipereliptyczne.** Krzywymi hipereliptycznymi nazywamy nieosobliwe krzywe postaci $C : Y^2 - f(X) = 0$, gdzie f jest wielomianem rozdzielczym dowolnego stopnia. Jest to pewne uogólnienie pojęcia krzywej eliptycznej.

W przypadku krzywych algebraicznych istnieje bardzo prosta zależność między przypadkiem afinicznym i rzutowym.

DEFINICJA 4.2.3. (1) *Niech $C^* : f(X,Y,Z) = 0$ będzie krzywą rzutową, gdzie $f \in \overline{F}[X,Y,Z]$.* **Dehomogenizacją** *krzywej C^* nazywamy krzywą afiniczną $C : f(X,Y,1) = 0$.*

(2) *Niech $C : f(X,Y) = 0$ będzie krzywą afiniczną, gdzie $f \in \overline{F}[X,Y]$.* **Homogenizacją** *(lub* **ujednorodnieniem** *czy też* **domknięciem rzutowym***)*

krzywej C nazywamy krzywą rzutową C^*, której dehomogenizacją jest krzywa C.

Krzywe algebraiczne afiniczne i ich domknięcia rzutowe są do siebie bardzo "podobne" w następującym sensie:

TWIERDZENIE 4.2.2. *Niech $C^* : f(X,Y,Z) = 0$ będzie krzywą rzutową, a $C : f(X,Y,1) = 0$ jej dehomogenizacją. Wówczas ciała funkcji wymiernych tych krzywych są izomorficzne, $\overline{F}(C) \cong \overline{F}(C^*)$.*

D o w ó d : Istotnie, wystarczy zdefiniować odwzorowanie $\alpha : \overline{F}(C^*) \to \overline{F}(C)$ wzorem:

$$\alpha(\frac{h^*}{g^*}) = \frac{h}{g}$$

gdzie jeśli $h* = H^* + \mathcal{I}(C^*), g* = G^* + \mathcal{I}(C^*) \in \overline{F}_h[C^*]$, tj. $H^*, G^* \in \overline{F}[X,Y,Z]$ są formami tego samego stopnia, to $h = H + \mathcal{I}(C), g = G + \mathcal{I}(C) \in \overline{F}[C]$, przy czym H i G są dehomegenizacjami wielomianów H^* i G^*, odpowiednio. Bez trudu można się przekonać, że takie odwzorowanie jest dobrze określonym bijektywnym homomorfizmem. *QED*

3. Punkty F-wymierne na rozmaitościach

Niech, tak jak wcześniej, F będzie dowolnym ciałem, niech $\overline{F}$ będzie jego domknięciem algebraicznym.

DEFINICJA 4.3.1. (1) *Niech $V \subseteq \mathbb{A}^n(\overline{F})$ będzie rozmaitością afiniczną. Powiemy, że rozmaitość ta jest* **zdefiniowana** *nad ciałem F wtedy i tylko wtedy, gdy ideał z nią stowarzyszony $\mathcal{I}(V) \lhd \overline{F}[X_1, \ldots, X_n]$ jest generowany przez wielomiany $f_1, \ldots, f_r \in F[X_1, \ldots, X_n]$.* [1)]

(2) *Niech $V^* \subseteq \mathbb{P}^n(\overline{F})$ będzie rozmaitością rzutową. Powiemy, że rozmaitość ta jest* **zdefiniowana** *nad ciałem F wtedy i tylko wtedy, gdy ideał z nią stowarzyszony $\mathcal{I}(V^*) \lhd \overline{F}[X_1, \ldots, X_{n+1}]$ jest generowany przez wielomiany $f_1, \ldots, f_r \in F[X_1, \ldots, X_{n+1}]$.*

Interesować nas będą punkty na rozmaitościach, których współrzędne pochodzą z ciała F. W tym celu wprowadźmy kolejną definicję:

DEFINICJA 4.3.2. (1) *Niech $V \subseteq \mathbb{A}^n(\overline{F})$ będzie rozmaitością afiniczną. Punkt $(a_1, \ldots, a_n) \in V$ nazwiemy* **punktem F-wymiernym**, *jeżeli $a_1, \ldots, a_n \in F$. Zbiór wszystkich punktów $F-$wymiernych na rozmaitości V oznaczać będziemy symbolem $V(F)$.*

(2) *Niech $V^* \subseteq \mathbb{P}^n(\overline{F})$ będzie rozmaitością rzutową. Punkt $(a_1 : \ldots : a_{n+1}) \in V^*$ nazwiemy* **punktem F-wymiernym**, *jeżeli $a_1, \ldots, a_{n+1} \in F$. Zbiór wszystkich punktów $F-$wymiernych na rozmaitości V^* oznaczać będziemy symbolem $V^*(F)$.*

Znaczna część wprowadzonych wcześniej definicji przenosi się w pewien sposób na zbiór punktów F-wymiernych na rozmaitości. Przeprowadzimy krótką dyskusję tych zagadnień.

[1)] Ideał ten zawsze jest skończenie generowany, jako że pierścień $\overline{F}[X_1, \ldots, X_n]$ jest noetherowski.

DEFINICJA 4.3.3. (1) *Niech $V \subseteq \mathbb{A}^n(\overline{F})$ będzie rozmaitością afiniczną, a $\mathcal{I}(V)$ ideałem z nią stowarzyszonym. Ideał:*

$$\mathcal{I}(V/F) = \mathcal{I}(V) \cap F[X_1, \ldots, X_n]$$

nazywać będziemy **F-wymiernym ideałem stowarzyszonym** *z rozmaitością V, a pierścień*

$$F[V] = F[X_1, \ldots, X_n]/\mathcal{I}(V/F)$$

pierścieniem współrzędnych $F-$wymiernych.

(2) *Niech $V^* \subseteq \mathbb{P}^n(\overline{F})$ będzie rozmaitością rzutową, a $\mathcal{I}(V^*)$ ideałem z nią stowarzyszonym. Ideał:*

$$\mathcal{I}(V^*/F) = \mathcal{I}(V^*) \cap F[X_1, \ldots, X_{n+1}]$$

nazywać będziemy **F-wymiernym ideałem stowarzyszonym** *z rozmaitością V^*, a pierścień*

$$F_h[V^*] = F[X_1, \ldots, X_{n+1}]/\mathcal{I}(V^*/F)$$

pierścieniem współrzędnych $F-$wymiernych.

Jest trywialną obserwacją, że ideał $F-$wymierny stowarzyszony z rozmaitością jest ideałem pierwszym. Można wobec tego mówić o jego ciele ułamków i tym samym wprowadzić definicje ciał funkcji $F-$wymiernych:

DEFINICJA 4.3.4. (1) *Niech $V \subseteq \mathbb{A}^n(\overline{F})$ będzie rozmaitością afiniczną. Ciało ułamków pierścienia współrzędnych $F-$wymiernych nazywamy* **ciałem funkcji $F-$wymiernych** *na rozmaitości i oznaczamy $F(V)$.*

(2) *Niech $V^* \subseteq \mathbb{P}^n(\overline{F})$ będzie rozmaitością rzutową. Ciało ułamków pierścienia współrzędnych $F-$wymiernych nazywamy* **ciałem homogenicznych funkcji $F-$wymiernych** *na rozmaitości i oznaczamy $F_h(V^*)$.*

(3) *Niech $V^* \subseteq \mathbb{P}^n(\overline{F})$ będzie rozmaitością rzutową oraz $F_h(V^*)$ ciałem homogenicznych funkcji $F-$wymiernych na rozmaitości. Podciało:*

$$F(V^*) = \{z \in F_h(V^*) : z = \frac{f}{g}, f, g \in F_h[V^*], \deg f = \deg g, f, g \text{ są formami}\}$$

nazywamy **ciałem funkcji $F-$wymiernych** *na rozmaitości, przy czym stopień elementu pierścienia współrzędnych rozumiemy jako stopień dowolnego reprezentanta warstwy, czyli wielomianu.*

Nietrudno się przekonać, że wprowadzone definicje są poprawne. Dla zachowania pełnej analogii z wcześniej rozważanymi pojęciami, zdefiniujemy jeszcze odpowiedniki pierścieni lokalnych punktów $F-$wymiernych oraz ich ideałów maksymalnych:

DEFINICJA 4.3.5. (1) *Niech $V \subseteq \mathbb{A}^n(\overline{F})$ będzie rozmaitością afiniczną, niech $P \in V$. Funkcję $F-$wymierną na rozmaitości $z \in F(V)$ nazywamy* **określoną w punkcie** *P wtedy i tylko wtedy, gdy istnieje przedstawienie $z = \frac{f}{g}$, $f, g \in F[V]$ dla którego $g(P) \neq 0$. Zbiór wszystkich funkcji określonych w danym punkcie oznaczamy $F_P[V]$ i nazywamy* **pierścieniem lokalnym** *punktu $F-$wymiernego P. Jego jedyny ideał maksymalny $M_P(V/F)$ nazywamy* **punktem** *ciała funkcji $F-$wymiernych $F(V)$.*

(2) *Niech* $V^* \subseteq \mathbb{P}^n(\overline{F})$ *będzie rozmaitością afiniczną, niech* $P \in V^*$. *Funkcję* $F-$*wymierną na rozmaitości* $z \in F(V^*)$ *nazywamy* **określoną w punkcie** P *wtedy i tylko wtedy, gdy istnieje przedstawienie* $z = \frac{f}{g}$, $f, g \in F_h[V^*]$ *dla którego* $g(P) \neq 0$. *Zbiór wszystkich funkcji określonych w danym punkcie oznaczamy* $F_P[V^*]$ *i nazywamy* **pierścieniem lokalnym** *punktu* $F-$*wymiernego* P. *Jego jedyny ideał maksymalny* $M_P(V^*/F)$ *nazywamy* **punktem** *ciała funkcji* $F-$*wymiernych* $F(V^*)$.

Odnotujmy tu jeszcze, że w interesującym nas przypadku gdy $V = C$ jest krzywą, zachodzi następujące twierdzenie, wynikające natychmiast z twierdzenia 4.2.2:

TWIERDZENIE 4.3.1. *Niech* $C^* : f(X, Y, Z) = 0$ *będzie krzywą rzutową, a* $C : f(X, Y, 1) = 0$ *jej dehomogenizacją. Wówczas ciała funkcji* $F-$*wymiernych tych krzywych są izomorficzne,* $F(C) \cong F(C^*)$.

4. Punkty F-wymierne na krzywych płaskich

W tym paragrafie przyjrzmy się nieco bliżej punktom $F-$wymiernym na krzywych algebraicznych. Pokażemy, że zarówno ciało funkcji $F-$wymiernych jak i ciało funkcji wymiernych na krzywej są ciałami funkcji algebraicznych. Możemy dzięki temu zdefiniować hipotezę Riemanna dla krzywych algebraicznych w terminach punktów na krzywej i do jej rozstrzygnięcia wykorzystać twierdzenie Hasse'go - Weil'a. Ponadto twierdzenie to można użyć też do oszacowania liczby punktów $F-$wymiernych na krzywej, co szczegółowo przedyskutujemy na przykładzie krzywych eliptycznych - zajmieny się tym jednak w kolejnych paragrafach.

Tak jak zwykle, F niech będzie dowolnym ciałem, a $\overline{F}$ jego domknięciem algebraicznym. W całym tym paragrafie zakładać będziemy, że $C : f(X, Y) = 0$, gdzie $f \in F[X, Y]$ jest wielomianem nierozkładalnym, jest nieosobliwą płaską krzywą algebraiczną, a C^* jej homogenizacją.

UWAGA 4.4.1. (1) *Krzywa* C *jest zdefiniowana nad ciałem* F; *dokładniej, ideał z nią stowarzyszony* $\mathcal{I}(C)$ *jest ideałem głównym generowanym przez wielomian* f.
(2) *Krzywa* C^* *jest zdefiniowana nad ciałem* F.

D o w ó d : Punkt (2) wynika bezpośrednio z (1), ograniczymy się więc do wykazania pierwszej tezy. Oczywiście $(f) \subseteq \mathcal{I}(C)$. Dla dowodu przeciwnej inkluzji przypuśćmy nie wprost, że istnieje wielomian $g(X, Y) \in \mathcal{I}(C)$ taki, że $g(X, Y) \notin (f)$, tj. $f \nmid g$. Rozważmy układ równań:

$$f(X, Y) = 0,\ g(X, Y) = 0$$

Zauważmy, że ma on skończenie wiele rozwiązań. Jeżeli $g_1(X, Y), \ldots, g_r(X, Y)$ są wszystkimi czynnikami nierozkładalnymi w rozkładzie wielomianu $g(X, Y)$, to zbiór rozwiązań rozważanego układu równań równy jest zbiorowi rozwiązań układów:

$$f(X, Y) = 0,\ g_1(X, Y) = 0$$

$$\vdots$$

$$f(X, Y) = 0,\ g_r(X, Y) = 0$$

przy czym $f \nmid g_1, \ldots, f \nmid g_r$. Możemy więc założyć, że $g(X,Y)$ jest nierozkładalny. Dalej, jeżeli $\deg_X f(X,Y) = 0$, to $f(a,b) = 0$ dla skończonej liczby elementów $b \in \overline{F}$. Wówczas dla tych samych (ale niekoniecznie wszystkich) $b \in \overline{F}$ mamy $f(a,b) = 0$. Możemy więc założyć także, że $\deg_X f(X,Y) \geqslant 1$. Rozważmy $f(X,Y)$ jako element pierścienia $\overline{F}(Y)[X]$. Bez trudu sprawdzamy, że $f(X,Y)$ i $g(X,Y)$ są nierozkładalne w $\overline{F}(Y)[X]$ i $f \nmid g$ w pierścieniu $\overline{F}(Y)[X]$. Pierścień $\overline{F}(Y)[X]$ jest euklidesowy, więc skoro $NWD(f,g) = 1$, to istnieją elementy $\alpha(X,Y), \beta(X,Y) \in \overline{F}(Y)[X]$ takie, że:

$$\alpha(X,Y) \cdot f(X,Y) + \beta(X,Y) \cdot g(X,Y) = 1$$

Zatem - wracając z pierścienia wielomianów jednej zmiennej nad ciałem funkcji wymiernych do pierścienia wielomianów dwóch zmiennych - istnieją wielomiany $A(X,Y), B(X,Y) \in \overline{F}[X,Y]$ oraz $H(Y) \in \overline{F}[Y]$ takie, że:

$$A(X,Y) \cdot f(X,Y) + B(X,Y) \cdot g(X,Y) = H(Y)$$

Więc jeżeli $f(a,b) = g(a,b) = 0$ to również $H(b) = 0$, zatem $f(a,b) = g(a,b) = 0$ dla skończonej liczby $b \in \overline{F}$. Ustalmy więc $b \in \overline{F}$ takie, że dla pewnych $a, b \in \overline{F}$ mamy $f(a,b) = g(a,b) = 0$. Jeżeli $f(X,b) \in \overline{F}[X]$ jest niezerowy, to z $b \in \overline{F}$ związanych jest skończenie wiele elementów $a \in \overline{F}$ takich, że $f(a,b) = g(a,b) = 0$, więc układ ma skończenie wiele rozwiązań i dowód tej części twierdzenia jest zakończony. Przypuśćmy więc, że $f(X,b) \in \overline{F}[X]$ jest tożsamościowo równy zeru. Ponieważ wielomian $f(X,Y) \in \overline{F}[X,Y]$ nie jest tożsamościowo równy zeru, nie jest też więc tożsamościowo zerowy w pierścieniu $\overline{F}(X)[Y]$. Wobec twierdzenia Bezout:

$$f(X,Y) = (Y - b) \cdot h(Y)$$

gdzie $h(Y) \in \overline{F}(X)[Y]$, a więc $h(Y) = \frac{C(X,Y)}{D(X)}$, gdzie $C(X,Y) \in \overline{F}[X,Y]$, $D(Y) \in \overline{F}[X]$. Stąd:

$$D(X) \cdot f(X,Y) = (Y - b) \cdot C(X,Y)$$

Porównując stopnie wielomianów widzimy, że $f \nmid (Y - b)$, a więc $f | C$. Zatem:

$$D(X) = (Y - b)\frac{C(X,Y)}{f(X,Y)}$$

co jest sprzecznością, bo po lewej stronie występuje wielomian zmiennej X, a po prawej wielomian zmiennej Y.

Wobec tego rozważany układ ma skończenie wiele rozwiązań. Jest to sprzecznością, gdyż skoro $f(X,Y), g(X,Y) \in \mathcal{I}(C)$ i $\overline{F}$ jest algebraicznie domknięte, to krzywa C ma nieskończenie wiele punktów, więc wielomiany $f(X,Y)$ i $g(X,Y)$ zerują się równocześnie w nieskończenie wielu punktach. *QED*

Zdefiniumy teraz następujące elementy pierścienia współrzędnych $F-$wymiernych:

$$x = X + \mathcal{I}(C/F) \text{ oraz } y = Y + \mathcal{I}(C/F)$$

Jasne jest, że jeżeli $g(X,Y) \in F[C]$, to $g(X,Y) + \mathcal{I}(C/F) = g(x,y)$, zatem $F[C] = F[x,y]$ i tym samym $F(C) = F(x,y)$. Pokażemy przy tych oznaczeniach niezmiernie ważne dla dalszych rozważań twierdzenie:

TWIERDZENIE 4.4.1. (1) *$F(C)/F$ jest ciałem funkcji algebraicznych; dokładniej:*

- *x jest elementem przestępnym nad F,*
- *$F(x,y)$ jest skończonym rozszerzeniem ciała $F(x)$.*

(2) $\overline{F}(C)/\overline{F}$ *jest ciałem funkcji algebraicznych, dokładniej rozszerzeniem ciała stałych ciała* $F(C)/F$.
(3) $F(C^*)/F$ *jest ciałem funkcji algebraicznych.*
(4) $\overline{F}(C^*)/\overline{F}$ *jest ciałem funkcji algebraicznych.*

D o w ó d : Tezy (3) i (4) wynikają natychmiast z tez (1) i (2) oraz twierdzeń 4.2.2 i 4.3.1. Z kolei warunek (2) jest oczywisty, o ile udowodnimy warunek (1).

Pokażmy więc najpierw, że element x jest przestępny nad F. Przypuśćmy dla dowodu nie wprost, że jest elementem algebraicznym. Oznaczmy:

$$\overline{x} = X + \mathcal{I}(C) \text{ oraz } \overline{y} = Y + \mathcal{I}(C)$$

Tak jak wcześniej jest oczywiste, iż jeśli $g(X,Y) \in \overline{F}[C]$, to $g(X,Y) + \mathcal{I}(C) = g(\overline{x},\overline{y})$, zatem $\overline{F}[C] = \overline{F}[\overline{x},\overline{y}]$ i tym samym $\overline{F}(C) = \overline{F}(x,y)$. Zauważmy, że $\overline{x}$ jest przestępny nad $\overline{F}$.

Załóżmy a *contrario*, że $\overline{x}$ jest algebraiczny. Wówczas istnieje wielomian $g(X) \in \overline{F}[X]$ taki, że $g(\overline{x}) = 0$ oraz $g \neq 0$. Wówczas $g(X) \in \mathcal{I}(C)$, ale zgodnie z uwagą 4.4.1 $\mathcal{I}(C) = (f)$, więc $f|g$ co doprowadza nas do sprzeczności, gdyż $f(X,Y)$ jest wielomianem dwóch zmiennych, zaś $g(X)$ - jednej.

Wobec tego $\overline{x}$ jest przestępny nad ciałem $\overline{F}$. Niech $\phi : F \to \overline{F}$ będzie zanurzeniem danym wzorem $\phi(x) = x$, zaś $\phi_r : F[x,y] \to \overline{F}[\overline{x},\overline{y}]$ jedynym jego przedłużeniem o tej własności, że $\phi_r(x) = \overline{x}$ oraz $\phi_r(y) = \overline{y}$. Ponieważ przypuściliśmy, że x jest algebraiczny, więc dla pewnych $a_0, \ldots, a_n \in F$ nie wszystkich równych zeru zachodzi warunek $a_0 + a_1x + \ldots + a_nx^n = 0$. W takim razie:

$$\begin{aligned} 0 &= \phi_r(a_0 + a_1x + \ldots + a_nx^n) = a_0 + a_1\phi_r(x) + \ldots + a_n(\phi_r(x))^n = \\ &= a_0 + a_1\overline{x} + \ldots + a_n\overline{x}^n \end{aligned}$$

co daje sprzeczność z założeniem, że $\overline{x}$ jest przestępny nad $\overline{F}$, a więc i nad F.

Dla zakończenia dowodu pozostaje sprawdzić, że rozszerzenie $F(x,y) \supseteq F(x)$ jest skończone. W tym celu wystarczy zauważyć, że y jest elementem algebraicznym nad $F(x,y)$. Istotnie, zapiszmy $f(X,Y)$ w postaci:

$$f(X,Y) = a_0(X)Y^n + a_1(X)Y^{n-1} + \ldots + a_n(X) \in F[X,Y]$$

gdzie $a_i(X) \in F[X]$ dla $i \in \{0, \ldots, n\}$. Niech:

$$h(Y) = a_0(x)Y^n + a_1(x)Y^{n-1} + \ldots + a_n(x) \in F(x)[Y]$$

Wówczas, skoro x jest elementem przestępnym, $a_i(x) \neq 0$ dla tych $i \in \{0, \ldots, n\}$, dla których $a_i(X) \neq 0$, a więc $h(Y) \neq 0$ i oczywiście $h(y) = 0$. *QED*

Będziemy teraz zmierzali do udowodnienia, że pierścień współrzędnych F-wymiernych nieosobliwej krzywej algebraicznej jest pierścieniem Dedekinda. Udowodnimy w tym celu dwa lematy i wykorzystamy mocne twierdzenie aproksymacyjne.

Lemat 4.4.1. (Lemat uniformizacyjny) *Niech P będzie punktem nieosobliwym krzywej C. Wówczas istnieje funkcja $t \in F_P[C]$ taka, że:*

(1) $t(P) = 0$
(2) *Dla każdej funkcji wymiernej $\varphi \in F(C)$, $\varphi \neq 0$, istnieje dokładnie jedno przedstawienie postaci:*

$$\varphi = t^l v$$

gdzie $v \in U(F_P[C])$ i l jest pewną liczbą całkowitą. Ponadto:

$$\varphi \in F_P[C] \iff l \geqslant 0$$

D o w ó d : Załóżmy dodatkowo - zmieniając ewentualnie układ współrzędnych - że $P = (0,0)$. Dla uproszczenia zapisu wszystkie rachunki wykonujemy na reprezentantach warstw. Dowolny wielomian $f \in F[X,Y]$ możemy zapisać w postaci:

$$f(X,Y) = aX + bY + g(X,Y)$$

przy czym każdy jednomian w $g(X,Y)$ ma stopień nie mniejszy od 2. Ponadto, skoro punkt P jest nieosobliwy, stosując wzor Taylora (dla formalnych pochodnych wielomianów) mamy, że $a = \frac{\partial f}{\partial X}(X,Y) \restriction_P \neq 0$ lub $b = \frac{\partial f}{\partial Y}(X,Y) \restriction_P \neq 0$. Dla ustalenia uwagi załóżmy, że $b \neq 0$. Jeżeli teraz zapiszemy $g(X,Y)$ w postaci $g(X,Y) = X \cdot f_1(X) + Y \cdot f_2(X,Y)$ to dostaniemy:

$$f(X,Y) = X(a + f_1(X)) + Y(b + f_2(X,Y))$$

Ponieważ dla każdego punktu $(x,y) \in C$ mamy $f(x,y) = 0$, więc z powyższego związku $y = \frac{-(a+f_1(x))}{b+f_2(x,y)}x$. Połóżmy więc $v(X,Y) = \frac{-(a+f_1(X))}{b+f_2(X,Y)}$. Zauważmy, że $v \in F_P[C]$; istotnie $b + f_2(0,0) = b \neq 0$. Pokazaliśmy więc, iż istnieje $v \in K_P[C]$ taka, że dla każdego punktu $(x,y) \in C$ $y = x \cdot v$.

Połóżmy $t(X,Y) = X$. Oczywiście funkcja t spełnia warunek (1) i pozostało nam pokazać, że spełnia warunek (2). Ustalmy więc $0 \neq \varphi \in F(C)$. Rozważmy najpierw przypadek, gdy φ jest określona w punkcie P. Jeżeli $\varphi(P) \neq 0$, to kładziemy $\varphi = x^0\varphi$. Załóżmy więc, że $\varphi(P) = 0$. Natenczas $\varphi(x,y) = \frac{p(x,y)}{q(x,y)}$, gdzie $p, q \in F[X,Y]$, dla wszelkich $(x,y) \in C$, przy czym $p(0,0) = 0$ i $q(0,0) \neq 0$. W połączeniu z uzyskaną wcześniej zależnością między x a y dla $(x,y) \in C$ otrzymujemy:

$$\varphi(x,y) = \frac{p(x,y)}{q(x,y)} = \frac{p(x, x \cdot v)}{q(x,y)} = x \cdot \frac{r(x,y)}{q(x,y)}$$

dla wszelkich $(x,y) \in C$, przy czym $v \in F_P[C]$ i $r \in F[X,Y]$. Kładąc więc $u_1(X,Y) = \frac{r(X,Y)}{q(X,Y)}$ otrzymujemy związek $\varphi = X \cdot u_1$, $u_1 \in F_P[C]$. Jeżeli $u_1(P) \neq 0$, to dostajemy przedstawienie, o jakie chodziło. Jeżeli $u_1(P) = 0$, to zastępując φ przez u_1 otrzymamy, że $u_1 = X \cdot u_2$, gdzie $u_2 \in F_P[C]$ - i dalej kontynuujemy postępowanie indukcyjne. Pokażemy obecnie, że procedura ta musi się zakończyć.

Zauważmy najpierw, że $f \nmid p$ w $F[X,Y]$. Istotnie, gdyby $f|p$, to dla wszelkich $Q \in C$ byłoby, że $p(Q) = 0$, gdyż $p = f \cdot h$ dla pewnego $h \in F[X,Y]$. Wówczas φ byłaby tożsamościowo równa zeru, wbrew uprzednim założeniom.

Skonstruujemy teraz liczbę l z warunku (2) lematu. Ponieważ f jest nierozkładalny w $F[X,Y]$, więc jest też nierozkładalny w $F(X)[Y]$ i skoro $F(X)[Y]$ jest pierścieniem euklidesowym, to istnieją wielomiany $\alpha(X,Y), \beta(X,Y) \in F(X)[Y]$ takie, że $\alpha(X,Y) \cdot f(X,Y) + \beta(X,Y) \cdot p(X,Y) = 1$, a tym samym istnieją wielomiany $A(X,Y), B(X,Y) \in F[X,Y]$ oraz $H(X) \in F[X]$ takie, że:

$$A(X,Y) \cdot f(X,Y) + B(X,Y) \cdot p(X,Y) = H(X)$$

Wybierzmy więc nieujemną liczbę $l \in \mathbb{Z}$ tak, aby $X^l | H$ i $X^{l+1} \nmid H$. Pokażemy, że przeprowadzona konstrukcja jest poprawna.

Przypuśćmy bowiem, że istnieje przedstawienie:

$$\varphi = X^m \cdot u$$

gdzie $u \in U(F_P[C])$ i m jest pewną liczbą całkowitą ostro większą od l. Zgodnie z definicją liczby l, $H(X) = X^l \cdot D(X)$, gdzie $D(X) \in F[X]$ i $D(0) \neq 0$. Zatem:

$$A(X,Y) \cdot f(X,Y) + B(X,Y) \cdot p(X,Y) = X^l \cdot D(X)$$

więc dla dowolnie ustalonego punktu $(x, y) \in C$:

$$B(x, y) \cdot p(x, y) = x^l \cdot D(x)$$

Dzieląc obustronnie przez $q(x, y)$ dostajemy:

$$B(x, y)\frac{p(x, y)}{q(x, y)} = \frac{x^l D(x)}{q(x, y)}$$

i ponieważ $\varphi = \frac{p}{q} = x^m \cdot u$ dostajemy:

$$B(x, y) \cdot x^m \cdot u = \frac{x^l D(x)}{q(x, y)}$$

ale skoro $u = \frac{u_1}{u_2}$, $u_1, u_2 \in F[C]$, więc:

$$B(x, y) \cdot x^m \cdot u_1(x, y) \cdot q(x, y) = x^l \cdot D(x) \cdot u_2(x, y)$$

co oznacza, że:

$$B(X, Y) \cdot X^m \cdot u_1(X, Y) \cdot q(X, Y) \equiv X^l \cdot D(X) \cdot u_2(X, Y)(\mod f(X, Y)) \text{ w } F[X, Y]$$

a zatem:

$$B(X, Y) \cdot X^{m-l} \cdot u_1(X, Y) \cdot q(X, Y) - \cdot D(X) \cdot u_2(X, Y) = f(X, Y) \cdot H(X, Y)$$

dla pewnego $H(X, Y) \in F[X, Y]$. Kładąc więc $X = 0$ i $Y = 0$ otrzymujemy sprzeczność, jako że prawa strona się zeruje, a lewa nie.

Rozważmy teraz przypadek, gdy φ nie jest określona w punkcie P, a więc dla wszelkich przedstawień $\varphi = \frac{u_1}{u_2}$ zawsze jest $u_2(P) = 0$. Weźmy więc $\varphi^{-1} = \frac{u_2}{u_1}$ i - stosując poprzednie rozumowanie - uzyskamy, że $\varphi^{-1} = X^l \cdot u$, gdzie $u(P) \neq 0$. Zatem $\varphi = X^{-l} \cdot u^{-1}$.

Zobaczymy teraz, że wybór stosownego przedstawienia jest jednoznaczny. Przypuśćmy więc, że mamy dwa różne przedstawienia $\varphi = t^l \cdot v = t^m \cdot u$, $v(P) \neq 0$, $u(P) \neq 0$. Gdyby $l > m$, to $t^{l-m} \cdot v = u$, co byłoby sprzecznością, bo w punkcie P lewa strona by się zerowała, a prawa nie. Zatem $l = m$, ale wtedy automatycznie $v = u$, więc też dostajemy sprzeczność, gdyż - zgodnie z założeniem - rozpatrywaliśmy dwa różne rozkłady.

Dla zakończenia dowodu pozostało sprawdzić prawdziwość ostatniego zdania lematu. Niech więc $\varphi \in F_P[C]$ i niech $\varphi = t^l \cdot v$, gdzie $v(P) \neq 0$. Gdyby $l < 0$, to wówczas $\varphi = \frac{1}{t^{-l}} \cdot v$, co byłoby sprzeczne z tym, że $\varphi \in F_P[C]$. Analogiczny rachunek prowadzony w drugą stronę pokazuje równoważność. *QED*

LEMAT 4.4.2. *Pierścień lokalny punktu nieosobliwego na krzywej afinicznej jest pierścieniem waluacyjnym ciała $F(C)$.*

D o w ó d : Ustalmy funkcję $0 \neq \varphi \in F(C)$. Na podstawie poprzedniego lematu:

$$\varphi = t^l v$$

gdzie $v \in U(F_P[C])$ i l jest pewną liczbą całkowitą. Jeżeli $l \geqslant 0$, to φ jest określona w punkcie P, w przeciwnym wypadku $\varphi^{-1} = t^{-1} \cdot v^{-1}$, zatem $\varphi^{-1} \in F_P[C]$. *QED*

Podamy i udowodnimy teraz zapowiadane wcześniej twierdzenie.

TWIERDZENIE 4.4.2. *Pierścień współrzędnych F-wymiernych na nieosobliwej afinicznej krzywej algebraicznej płaskiej jest dziedziną Dedekinda.*

D o w ó d : Rozważmy następujący zbiór punktów ciała $F(x,y)$:

$$S = \{Q \in \mathbb{P}_{F(x,y)} : Q = M_P(C/F) \text{ dla pewnego } P \in C\}$$

Na podstawie wcześniejszych dwóch lematów, zbiór ten jest dobrze zdefiniowany. Niech teraz:

$$\mathbb{P}_\infty = \{Q \in \mathbb{P}_{F(x,y)} : Q \text{ jest biegunem } x\text{'a lub } y\text{'a}\}$$

Pokażemy, że S jest właściwym podzbiorem $\mathbb{P}_{F(x,y)}$. Istotnie, jako że krzywa jest nieosobliwa, jest niepusty. Aby się przekonać, że $S \subsetneq \mathbb{P}_{F(x,y)}$ zauważmy, że $\mathbb{P}_\infty \nsubseteq S$.

Istotnie, przypuśćmy, że dla pewnego punktu $P \in C$, punkt $Q = M_P(C/F)$ jest biegunem - dla przykładu - x'a, czyli że $v_Q(x) < 0$. W świetle lematu uniformizacyjnego istnieją $t \in F_P[C]$, $u \in U(F_P[C])$ i liczba całkowita l takie, że $x = t^l u$. Wobec twierdzenia 1.1.4 $v_Q(x) = l < 0$, a więc - stosując ponownie lemat uniformizacyjny - stwierdzamy, że $x \notin F_P[C]$, co jest oczywistą sprzecznością, gdyż funkcja x jest określona w każdym punkcie na krzywej.

W dalszym ciągu oznaczmy:

$$\mathcal{O}_S = \{z \in F(x,y) : v_Q(z) \geqslant 0, Q \in S\} = \bigcap_{P \in C} F_P[C]$$

Oczywiście $\mathcal{O}_S$ jest pierścieniem. [2)] Pokażemy, że $\mathcal{O}_S = F[x,y]$.

Ponieważ $F \subseteq \mathcal{O}_S$, $x \in \mathcal{O}_S$ i $y \in \mathcal{O}_S$, więc inkluzja $\mathcal{O}_S \supseteq F[x,y]$ jest oczywista. Dla wykazania inkluzji przeciwnej ustalmy $\phi \in \mathcal{O}_S$. Wówczas $v_Q(\phi) \geqslant 0$ dla $Q \in S$. Dla każdego $Q_i \in S$ istnieje punkt $P_i \in C$ taki, że $Q = M_{P_i}(C/F)$, zaś wobec lematu uniformizacyjnego istnieją $t_{P_i} \in F_{P_i}[C]$, $u_{P_i} \in U(F_{P_i}[C])$ oraz $l_{P_i} \in \mathbb{Z}$ takie, że $\phi = t^{l_{P_i}} u_{P_i}$. Wobec twierdzenia 1.1.4 $v_{Q_i}(\phi) = l_{p_i} \geqslant 0$ dla każdego $Q_i \in S$, a więc korzystając raz jeszcze z lematu uniformizacyjnego mamy, że $\phi \in F_{P_i}[C]$ dla wszystkich $P_i \in C$.

Pozostaje więc wykazać, że funkcja $F-$wymierna określona w każdym punkcie $F-$wymiernym jest elementem pierścienia współrzędnych $F-$wymiernych. Niech:

$$I = \{\phi_2 \in F[x,y] : \phi = \frac{\phi_1}{\phi_2}\} \cup \{0\}$$

Bez trudu stwierdzamy, że I jest ideałem pierścienia $F[x,y]$. Pokażemy jednak, że nie jest to ideał właściwy, a mianowicie $I = F[x,y]$.

Przypuśćmy zatem, że $I \subsetneq F[x,y]$. Niech $\mathfrak{m}$ będzie ideałem maksymalnym zawierającym I, niech $\kappa : F[x,y] \to F[x,y]/\mathfrak{m}$ będzie homomorfizmem kanonicznym. W punkcie $(\kappa(x), \kappa(y))$ wszystkie mianowniki występujące w przedstawieniach ϕ w postaci $\frac{\phi_1}{\phi_2}$ są więc równe zeru, a zatem funkcja ϕ nie jest w tym punkcie określona - co jest sprzecznością.

Tak więc $I = F[x,y]$ i tym samym w pewnym przedstawieniu $\phi = \frac{\phi_1}{\phi_2}$, $\phi_2 = 1$, a zatem $\phi \in F[x,y]$, co kończy dowód inkluzji przeciwnej.

Niech teraz:

$$\Phi = \{v_Q : F(x,y) \to \mathbb{Z} \cup \{\infty\} : v_Q \text{ jest waluacją związaną z punktem } Q,\ Q \in S\}$$

O rodzinie waluacji Ψ powiemy, że jest **prawie skończona**, gdy w dowolnym punkcie z ciała, na którym są określone, tylko dla skończonej ich liczby $v(z) \neq 0$, $v \in \Psi$. Wobec twierdzenia 1.1.5 rodzina Φ jest prawie skończona. Dalej, powiemy że właściwa (tj. niepusta i różna od rodziny wszystkich waluacji określonych na danym ciele) rodzina waluacji Ψ ciała F ma własność **silnej aproksymacji**, gdy spełnia

[2)] Pierścienie tego typu nazywamy **dziedzinami Hasse'go**.

następujący warunek: dla $v_1, \dots, v_r \in \Psi$, $x_1, \dots, x_r \in F$ oraz $n_1, \dots, n_r \in \mathbb{Z}$ istnieje element $x \in F$ taki, że:

$$v_i(x - x_i) = n_i$$

gdy $i \in \{1, \dots, r\}$ oraz

$$v(x) \geqslant 0$$

gdy $v \in \Psi \setminus \{v_1, \dots, v_r\}$; oczywiście - na podstawie mocnego twierdzenia aproksymacyjnego - rodzina Φ czyni zadość tej własności. Na podstawie znanego z teorii pierścieni Dedekinda twierdzenia (por. [**2**] twierdzenie V.3.2.3) przekrój pierścieni waluacyjnych odpowiadających prawie skończonej rodzinie waluacji o własności silnej aproksymacji jest pierścieniem Dedekinda, skąd otrzymujemy tezę. *QED*

5. Punkty F-wymierne na krzywych eliptycznych

Skonstruowany w poprzednim paragrafie aparat można wykorzystać do oszacowania liczby punktów F-wymiernych na krzywych płaskich. Podamy teraz przykład takiego zastosowania studiowanej teorii - ograniczając się wszakże tylko do szczególnego rodzaju krzywych, do krzywych eliptycznych. Przeprowadzone tu rozumowanie nie podaje oczywiście metody oszacowania liczby punktów na dowolnej krzywej, ale ze względu na swą prostotę godne jest poświęcenia mu uwagi. Stosunkowo łatwo można je przenieść na przypadek krzywych hipereliptycznych, czego nie będziemy tu jednak robić. Dodatkowo założymy, że ciało F ma charakterystykę różną od 2. Dla ciał charakterystyki 2 trochę inaczej definiuje się ciało funkcji F-wymiernych - musielibyśmy wprowadzić tu pojęcie ciała funkcji eliptycznych i poświęcić nieco miejsca teorii rozszerzeń Galois typu Artina - Schreiera, co zbytnio odbiegałoby od głównego nurtu niniejszej pracy.

Niech F będzie dowolnym ciałem charakterystyki różnej od 2, a $\overline{F}$ jego domknięciem algebraicznym. Niech $E : Y^2 = f(X)$ będzie krzywą eliptyczną (tj. krzywą nieosobliwą i taką, że wielomian f jest rozdzielczy), a E^* jej homogenizacją. Niech:

$$x = X + \mathcal{I}(E/F) \text{ oraz } y = Y + \mathcal{I}(E/F)$$

i tym samym niech $F(x, y)$ oznacza ciało funkcji F-wymiernych na krzywej E. [3)] Jest dobrze znanym faktem, że w przypadku krzywych eliptycznych domknięcie rzutowe E^* można rozpatrywać jako zbiór $E \cup \{\mathcal{O}\}$, gdzie E jest częścią afiniczną krzywej E, a $\{\mathcal{O}\}$ punktem w nieskończoności, którego współrzędne oznaczać będziemy przez (∞, ∞). Aby zbytnio nie komplikować oznaczeń, stosować będziemy terminologię afiniczną, a w razie konieczności o punkcie (∞, ∞) będziemy mówili jak o pewnym "dodatkowym" punkcie krzywej.

Uwaga 4.5.1. *Niech $f(X) = c\prod_{i=1}^{r} p_i(X)$, gdzie $0 \neq c \in F$ oraz $p_i(X) \in F[X]$, $i \in \{1, \dots, r\}$, będzie rozkładem wielomianu f na czynniki nierozkładalne. Niech P_i oznacza punkt ciała $F(x)$ odpowiadający wielomianowi $p_i(X)$ a P_∞ biegun elementu x w ciele $F(x)$ (por. uwaga 1.2.1). Wówczas:*

1. *$F(x, y) \supseteq F(x)$ jest rozszerzeniem Galois stopnia 2.*
2. *Każdy z punktów $P_1, \dots, P_r, P_\infty$ ma dokładnie jedno rozszerzenie $Q_1, \dots, Q_r, Q_\infty$ w ciele $F(x, y)$, przy czym $e(Q_j|P_j) = e(Q_\infty|P_\infty) = 2$, $\deg Q_j = \deg P_j$ oraz $\deg Q_\infty = 1$. Ponadto $Q_1, \dots, Q_r, Q_\infty$ są jedynymi punktami rozgałęzionymi w $F(x, y)$.*

[3)] Ciała o własnościach takich jak to ciało nazywamy **ciałami funkcji eliptycznych.**

D o w ó d : (por. [**14**] Proposition VI.1.3) Dowód tezy (1) jest bardzo prosty - wystarczy zauważyć, że wielomian $Y^2 - f(X) \in F(X)[Y]$ jest rozdzielczy, a więc element y jest rozdzielczy i tym samym rozszerzenie $F(x,y) \supseteq F(x)$ jest rozdzielcze. Jest też oczywiście kwadratowe, a więc normalne, skąd wynika, że jest rozszerzeniem Galois (por. [**2**] zadanie II.2.1.1 i twierdzenie II.2.3.1). Dla dowodu tezy (2) wykorzystujemy fakt, że dla rozszerzeń Galois zachodzi twierdzenie 2.3.1, skąd łatwo wydedukować jedyność punktów rozszerzających $P_1, \ldots, P_r, Q_\infty$. Wszelako aby udowodnić wszystkie zachodzące między punktami odpowiedniości, musielibyśmy zagłębić się nieco w teorię rozszerzeń typu Kummera, co wydaje się zanadto odbiegać od dyskutowanej tu tematyki.

Udowodnimy teraz kluczowe dla tego paragrafu twierdzenie. Dla walucji $v : F(x,y) \to \mathbb{Z} \cup \{\infty\}$ przez Q_v oznaczać będziemy odpowiadający jej punkt ciała $F(x,y)$.

TWIERDZENIE 4.5.1. *Niech $E : Y^2 = f(X)$ będzie krzywą eliptyczną zdefiniowaną nad ciałem F charakterystyki różnej od 2, a $F(x,y)$ jej ciałem funkcji $F-$wymiernych. Niech $v : F(x,y) \to \mathbb{Z} \cup \{\infty\}$ będzie waluacją tego ciała. Wówczas:*

(1) *Waluacja v i punkt Q_v są jednoznacznie wyznaczone przez wartości funkcji algebraicznych x i y w punkcie Q_v.*
(2) *$(x(Q_v), y(Q_v)) \in E(F_{Q_v}) \supseteq E(F)$, przy czym punkt (∞,∞) interpretujemy jako punkt w nieskończoności $\mathcal{O}$.*

W szczególności odwzorowanie:

$$Q_v \mapsto (x(Q_v), y(Q_v))$$

ustala wzajemnie jednoznaczną odpowiedniość między zbiorem punktów stopnia 1 ciała $F(x,y)$ a zbiorem punktów $F-$wymiernych krzywej E, $E(F)$.

D o w ó d : Niech $Q_1, \ldots, Q_r, Q_\infty$ będą punktami opisanymi w poprzedniej uwadze i niech v_∞ oznacza waluację odpowiadającą punktowi Q_∞. Ponieważ jest to jedyna waluacja rozszerzająca waluację ciała $F(x)$ odpowiadającą biegunowi x'a, więc jest to jedyna waluacja, której pierścień waluacyjny nie zawiera pierścienia współrzędnych $F[x,y]$. Punktowi temu przyporządkowujemy punkt (∞,∞). Dla wszelkich innych waluacji, punkty im odpowiadające nie są biegunami x'a ani y'a.

Ustalmy więc dowolną waluację v różną od v_∞ odpowiadającą punktowi stopnia 1. Wówczas $x, y \in \mathcal{O}_{Q_v}$. Niech $\Phi : F(x,y) \to F_{Q_v}$ będzie dane wzorem $\Phi(z) = z(Q_v)$, $z \in F(x,y)$. Bez trudu sprawdzamy, że Ψ jest homomorfizmem $F-$algebr. Zatem:

- $(x(Q_v), y(Q_v)) \in E(F_{Q_v})$
- $z(Q_v)$ jest jednoznacznie wyznaczone przez wartości $x(P_v)$ i $y(P_v)$.

Niech $M = \ker \Phi \restriction_{F[x,y]}$. Ponieważ $F[x,y]/M$ jest podpierścieniem ciała, więc M jest ideałem pierwszym pierścienia $F[x,y]$. Jednak ponieważ $F[x,y]$ jest pierścieniem Dedekinda, więc M jest też maksymalny. Niech $F[x,y]_M$ będzie lokalizacją pierścienia $F[x,y]$ względem ideału M. Korzystając ponownie z tego, że $F[x,y]$ jest pierścieniem Dedekinda mamy, że $F[x,y]_M = \mathcal{O}_{Q_v}$ (por. [**2**] wniosek z lematu V.3.2.6). To dowodzi, że nasze odwzorowanie jest różnowartościowe.

Ustalmy teraz $(a,b) \in E(F) \setminus \{(\infty,\infty)\}$. Niech $M = (x-a, y-b) \lhd F[x,y]$. Bez trudu sprawdzamy, że jest to ideał maksymalny i niech $F[x,y]_M$ będzie lokalizacją pierścienia $F[x,y]$ względem ideału M. Wówczas $F[x,y]_M = \mathcal{O}_{Q_v}$ (por. [**2**] wniosek z lematu V.3.2.6) dla pewnej waluacji v. Ponadto - z określenia ideału M - $x(Q_v) =$

1 oraz $y(Q_v) = b$, skąd $\deg Q_v = 1$. To dowodzi, że rozpatrywana funkcja jest surjekcją. *QED*

Udowodnione twierdzenie wykorzystamy teraz do oszacowania liczby punktów na rzutowej krzywej eliptycznej E^* zdefiniowanej nad ciałem skończonym charakterystyki różnej od 2. Niech więc q będzie potęgą pewnej liczby pierwszej $p \neq 2$ i rozważmy ciało funkcji algebraicznych $F/\mathbb{F}_q$ o rodzaju g. Wyprowadźmy następujący prosty wniosek z twierdzenia Hasse'go - Weil'a:

TWIERDZENIE 4.5.2. (OSZACOWANIE HASSE'GO -WEIL'A) *Liczba N punktów ciała $F/\mathbb{F}_q$ stopnia 1 może być oszacowana w następujący sposób:*

$$|N - (q+1)| \leqslant 2g\sqrt{q}$$

D o w ó d : W rzeczy samej, jeżeli $\alpha_1, \ldots, \alpha_{2g}$ oznaczają odwrotności pierwiastków L-wielomianu ciała $F/\mathbb{F}_q$, to wobec wniosku 3.1.2:

$$N - (q+1) = -\sum_{i=1}^{2g} \alpha_i$$

skąd - na podstawie twierdzenia Hasse'go - Weil'a - natychmiast wynika teza. *QED*

Tak więc wobec twierdzenia 4.5.1 $N = \mathsf{card}\, E^*(\mathbb{F}_q)$.

6. Hipoteza Riemanna dla krzywych algebraicznych

Rozważmy krzywą afiniczną $C : f(X,Y) = 0$ zdefiniowaną nad ciałem $\mathbb{F}_q$ dla pewnej liczby q będącej potęgą liczby pierwszej p i niech x, y będą - tak jak wcześniej - warstwami elementów X i Y względem ideału $\mathcal{I}(C/\mathbb{F}_q)$. Zdefiniujmy funkcję $\zeta_C : \mathbb{C} \to \mathbb{C}$ wzorem:

$$\zeta_C(t) = \textstyle\sum_{\mathfrak{p}} \mathfrak{N}(\mathfrak{p})^{-t} \text{ dla } \mathsf{Re}\,(t) > 1$$

gdzie suma przebiega po wszystkich ideałach pierwszych pierścienia współrzędnych $\mathbb{F}_q$-wymiernych krzywej C, zaś $\mathfrak{N}(\mathfrak{p})$ oznacza moc ciała $\mathbb{F}_q[x,y]/\mathfrak{p}$ (jest to istotnie ciało, gdyż $\mathbb{F}_q[x,y]$ jest pierścieniem Dedekinda, a w nim każdy ideał pierwszy jest maksymalny, jest to też ciało skończone). Korzystając z tego, że $\mathbb{F}_q[x,y]$ jest pierścieniem Dedekinda możemy wywnioskować - rozumując tak jak w dowodzie twierdzenia 4.5.1 - że funkcja ζ_C jest równa funkcji ζ_F zdefiniowanej w rozdziale 3 - jest więc dla niej spełniona hipoteza Riemanna. W tym sensie hipoteza Riemanna została potwierdzona dla krzywych algebraicznych. Zauważmy przy tym, że jest to jedno z owych "porządnych" uogólnień funkcji ζ Riemanna, o których mowa była we wstępie.

7. Uogólnienia i przypadki szczególne

Przestudiowane w toku pracy zagadnienia pozwalają nam teraz z właściwym zrozumieniem spojrzeć na rozwój twierdzenia Hasse'go - Weil'a i pospekulować na temat możliwych jego uogólnień. Problem znajdowania liczby rozwiązań kongruencji zadanych przez wielomian jednorodny po raz pierwszy był szerzej dyskutowany - podobnie jak większość znanych problemów w teorii liczb - przez Gaussa. Artykuł 358 jego *Disquisitiones Arithmeticae* zawiera dowód następującego twierdzenia:

TWIERDZENIE 4.7.1. (GAUSS'A) *Niech M_q oznacza liczbę rzutowych rozwiązań równania:*

$$x^3 + y^3 + z^3 = 0$$

gdzie x, y, z są elementami ciała skończonego $\mathbb{F}_q$.

(1) *Jeżeli* $q \not\equiv 1 (\mathsf{mod}\, 3)$*, to* $M_q = q + 1$
(2) *Jeżeli* $q \equiv 1 (\mathsf{mod}\, 3$*, to wówczas istnieją liczby całkowite* A *i* B *takie, że:*

$$4q = A^2 + 27B^2$$

oraz wyznaczone jednoznacznie z dokładnością do znaku. Ustalając znak A *w ten sposób, aby* $A \equiv 1 (\mathsf{mod}\, 3)$ *mamy:*

$$M_q = q + 1 + A$$

Odwołujący się tylko do elementarnych pojęć, acz mimo to dosyć skomplikowany dowód tego twierdzenia znaleźć można w [**13**] na stronach 111 - 118. Można pokazać (por. [**14**] str. 186 - 193) że w przypadku, gdy krzywa C^* jest krzywą eliptyczną, rodzaj ciała funkcji wymiernych nad tą krzywą równy jest 1. Wspomniany wcześniej dowód Hasse'go z roku 1933 dotyczył takich właśnie ciał. W tym przypadku dowód ten można w pewien sposób zelementaryzować tak, aby nie odwoływać się do zaawansowanych pojęć teorii ciał funkcji algebraicznych (por. [**10**] str. 95 - 97 lub [**4**] paragrafy 24 i 25). Inne spojrzenie na twierdzenie Hasse'go - Weil'a, skupiające się wyłącznie na jego aspekcie teorioliczbowym, znaleźć można w [**12**].

O wiele ciekawsze wydaje się jednak patrzenie na twierdzenie Hasse'go - Weil'a z aspektu hipotezy Riemanna. Pokazaliśmy, że twierdzenie to można zinterpretować jako jej potwierdzenie w przypadku ciał funkcji algebraicznych jednej zmiennej nad skończonymi ciałami stałych. Wyłożona w tym rozdziale teoria pozwala spojrzeć na twierdzenie Hasse'go - Weil'a jako na potwierdzenie hipotezy Riemanna dla ciał funkcji wymiernych nad krzywymi algebraicznymi nad ciałami skończonymi. Naturalne pytanie, które powinno się w tym momencie pojawić, brzmi: czy w podobny sposób hipotezę Riemanna można potwierdzić też dla ciał funkcji wymiernych na, najogólniej, dowolnej rozmaitości? Intuicyjnie czujemy, że zastosowany wcześniej aparat nie zda w tym przypadku egzaminu - analizując bowiem dowód twierdzenia 4.4.1 widzimy, że stopień przestępny ciała funkcji wymiernych na dowolnie wybranej rozmaitości będzie większy od 1, nie będzie to więc ciało funkcji algebraicznych jednej zmiennej. Tym nie mniej hipotezę Riemanna dla rozmaitości można sformułować - po raz pierwszy na doniosłość takiego uogólnienia zwrócił uwagę Weil w roku 1949 (por. [**17**]) - a nawet udowodnić - co udało się w roku 1974 Deligne (por. [**6**]), za co otrzymał medal Fieldsa.

Spis literatury

[1] E. Bombieri, *Counting Points on Curves over Finite Fields*, Séminaire Bourbaki, 25e anneé, no. 430, 1972/73

[2] J. Browkin, *Teoria ciał*, PWN, Warszawa 1977

[3] J. Browkin, *Wybrane zagadnienia algebry*, PWN, Warszawa 1968

[4] J. Cassels, *Lectures on Elliptic Curves*, LMS, Student Texts 24, London 24

[5] I. Connell, *Elliptic Curve Handbook*

[6] P. Deligne, *La Conjecture de Weil I*, Publ. Math. IHES 43 (1974), 273 - 307

[7] W. Fulton, *Algebraic Curves. An Introduction to Algebraic Geometry*, W.A. Benjamin, Inc., New York 1969

[8] H. Hasse, *Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F.K. Schmidtschen Kongruenzzetafunktionen in gewissen elliptischen Fällen*, Nachr. Ges. Wiss. Göttingen, Math.-Phys. K. (1933), 253-262

[9] F. Leja, *Funkcje zespolone*, PWN, Warszawa 1979

[10] J. Milne, *Elliptic Curves*, http://www.dpmms.cam.ac.uk/Number-Theory-Web/N4.html

[11] B. Riemann, *Ueber die Anzahl der Primazahlen unter eine gegebener Grosse*, Monastber. Akad. Berlin, November 1859

[12] W. Schmidt, *Equations over Finite Fields. An Elementary Approach*, Lecture Notes in Mathematics vol. 536, Springer-Verlag, New York 1980

[13] J. Silverman, J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, New York 1992

[14] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin 1993

[15] K. Szymiczek, *Algebra. Wykłady dla studiów doktoranckich*, http://www.ux1.math.us.edu.pl

[16] K. Szymiczek, *Zbiór zadań z teorii grup*, Uniwesytet Śląski, Katowice 1979

[17] A. Weil, *Number of solutions od equations over finite fields*, Bull. Amer. Math. Soc. 55 (1949), 497 - 508

[18] A. Weil, *Sur les Courbes Algébriques et les Variétés qui s'en Déduisent*, Hermann, Paris 1948