Silverman – najciekawsze zadania

Rozdział I

1.1

(a) *(przy założeniu $char(K) \neq 3$, upraszczającym obliczenia)*

Niech $F(X,Y,Z) = Y^2Z + AXYZ + BYZ^2 - X^3$. Załóżmy, że dla pary (A,B) istnieje $P = [x : y : z] \in \mathbb{P}^2$ spełniające

$$0 = F(P) = \frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P)$$

czyli równoważnie:

$$\begin{cases} \frac{\partial F}{\partial X}(P) & = AYZ - 3X^2 = 0 \\ \frac{\partial F}{\partial Y}(P) & = 2YZ + AXZ + BZ^2 \\ \frac{\partial F}{\partial Z}(P) & = Y^2 + AXY + 2BZ = 0. \end{cases}$$

Jeżeli $y = 0$, to $3x^2 = 0$, więc $x = 0$. Stąd $z \neq 0$. Ale (z drugiego równania) $Bz^2 = 0$, więc $B = 0$.
Załóżmy, że $y \neq 0$; bez straty ogólności $y = 1$. Wtedy, jeżeli byłoby $z = 0$, to $3x^2 = 0$, więc $x = 0$ i wstawiając $[x : y : z] = [0 : 1 : 0]$ do ostatniego równania dostalibyśmy sprzeczność. Stąd $z \neq 0$. Ale $z \cdot (2 + Ax + Bz) = 0$, więc $2 + Ax + Bz = 0$ oraz $1 + Ax + 2Bz = 0$, co oznacza, że:

$$\begin{cases} Ax = -3 \\ Bz = 1 \end{cases}$$

$$\begin{cases} x = -3/A \\ z = 1/B \end{cases}$$

(w szczególności $A, B \neq 0$). Aby x, z spełniały pierwsze równanie: $A \cdot \frac{1}{B} = 3 \cdot (-\frac{3}{A})^2$, czyli $B = \frac{A^3}{27}$.

Odpowiedź: V jest osobliwa wtw. gdy $B = 0$ (wtedy $[0 : 0 : 1]$ jest osobliwy) lub gdy $B = A^3/27$ dla $A \neq 0$ (wtedy $P = [-3/A : 1 : 27/A^3]$ jest osobliwy).

1.2

(c) $f(X,Y) = Y^2 - X^4 - Y^4$. Aby znaleźć punkty osobliwe w $\mathbb{A}^2$:

$$\begin{cases} Y^2 & = X^4 + Y^4 \\ 2Y & = 4Y^3 \\ -4X^3 & = 0. \end{cases}$$

Jeżeli $char(K) = 2$, to wszystkie punkty są osobliwe (równanie tej krzywej to $(Y - X^2 - Y^2)^2$ – jest ono kwadratem). W przeciwnym wypadku $X = 0$ oraz

$$\begin{cases} Y^2 \cdot (1 - Y^2) & = 0 \\ Y \cdot (1 - 2Y) & = 0 \end{cases}$$

co jest możliwe tylko gdy $Y = 0$ lub $Y^2 = 2Y = 1$, czyli $Y = 2$, $2Y = 1$, co jest niemożliwe w charakterystyce $\neq 3$. Stąd jedyny punkt osobliwy to $(0,0)$ oraz, jeżeli $char(K) = 3$, $(0,2)$.

Znajdźmy teraz punkty osobliwe tej krzywej w $\mathbb{P}^2 \setminus \mathbb{A}^2$. Szukamy punktów postaci $[X : Y : 0]$. Dostajemy układ:

$$\begin{cases} 0 & = X^4 + Y^4 \\ -4X^3 & = 0 \\ -4Y^3 & = 0, \end{cases}$$

który nie ma rozwiązań dla $char(K) \neq 2$. Stąd dla $char(K) \neq 2$ nie ma żadnych punktów osobliwych w nieskończoności.

1.3 Niech $V : f(X_1, \ldots, X_n) = 0$, $P = (p_1, \ldots, p_n)$. Rozważmy przestrzeń styczną do V w punkcie P:

$$\begin{aligned} T_P(V) &:= \{(y_1, \ldots, y_n) \in \mathbb{A}^n : \sum_i \frac{\partial f}{\partial X_i}(P) \cdot y_i\} = \\ &= \{y \in \overline{K}^n : (\nabla f(P), y)\} = \\ &= Span(\nabla f(P))^{\perp}. \end{aligned}$$

Rozważmy parowanie $\langle \cdot, \cdot \rangle : M_P/M_P^2 \times T_P \to \overline{K}$ zadane jako:

$$\langle g, y \rangle := (\nabla g(P), y) = \sum_i \frac{\partial g}{\partial X_i}(P) y_i.$$

Pokażemy, że jest ono doskonałe, tzn. że przyporządkowanie

$$M_P/M_P^2 \ni \quad g \mapsto \langle g, \cdot \rangle \quad \in Hom_{\overline{K}}(T_P(V), \overline{K})$$

jest izomorfizmem:

- **dobrze określone:** jeżeli $g \in \overline{K}[X_1, \ldots, X_n]$ oraz $g \in I(V) = (f)$, to
- zauważmy, że jeżeli $g(P) = 0$, to z rozwinięcia Taylora wokół P:

$$g(X_1, \ldots, X_n) = \sum_i \frac{\partial g}{\partial X_i}(P) \cdot (X_i - p_i) + (\text{element } M^2_{\mathbb{A}^n, P}).$$

Ponadto:

$$M_P = (X_1 - p_1, \ldots, X_n - p_n)$$
$$M_P^2 = \Big((X_i - p_i) \cdot (X_j - p_j) : 1 \leqslant i, j \leqslant n \Big).$$

Stąd $g \in M_P^2$ wtw. gdy

$$\sum_i \frac{\partial g}{\partial X_i}(P) \cdot (X_i - p_i) \in M_P^2$$

??

1.4

1.6

1.7

(a) $S^2T = S^3 = T^3 = 0 \Rightarrow \quad S = T = 0$

(b) $X = S^2T$, $Y = S^3$, $Z = T^3 \Rightarrow \quad [Y : X] = [S^3 : S^2T] = [S : T]$.

$\psi([X : Y : Z]) = [Y : X] \Rightarrow$

$$\psi \circ \phi([S : T]) = \psi([S^2T : S^3 : T^3]) = [S^3 : S^2T] = [S : T]$$

$$\phi \circ \psi([X : Y : Z]) = \phi([X : Y : Z]) = [Y^2X : Y^3 : X^3] = [Y^2X : Y^3 : Y^2Z] = [X : Y : Z].$$

Uwaga: ψ nie jest regularna w $[0 : 0 : 1]$.

(c) $\mathbb{P}^1$ oraz V nie są izomorficzne, bo V ma punkt osobliwy $[0 : 0 : 1]$.

1.9 Załóżmy nie wprost, że $\phi = [\phi_0 : \ldots : \phi_n] : \mathbb{P}^m \to \mathbb{P}^n$ jest niestałym morfizmem, gdzie

$$\phi_0(x_0, \ldots, x_m), \ldots, \phi_n(x_0, \ldots, x_m) \in k[x_0, \ldots, x_n]$$

są jednorodnymi wielomianami tego samego dodatniego stopnia bez wspólnych czynników – wtedy $\phi_0, \ldots, \phi_n$ nie mają wspólnych miejsc zerowych (patrz Remark 3.3, str. 13), czyli $Z(\phi_0) \cap \ldots \cap Z(\phi_n) = \varnothing$.
Ale $\dim Z(\phi_i) = m - 1$, więc korzystając indukcyjnie z Dimension Theorem (Hartshorne, Theorem I.7.2) każda nierozkładalna składowa $Z(\phi_0) \cap \ldots \cap Z(\phi_n)$ ma wymiar $m - n - 1 \geqslant 0$; w szczególności $Z(\phi_0) \cap \ldots \cap Z(\phi_n) \neq \varnothing$ – sprzeczność kończy dowód.

1.10 (a) zauważmy, że jeżeli $p \equiv 3 \pmod 4$, to $V_p(\mathbb{Q}) = \varnothing$, więc w szczególności $V_p \ncong \mathbb{P}^1$ nad $\mathbb{Q}$. Istotnie, załóżmy nie wprost że $X^2 + Y^2 = pZ^2$ dla pewnych $[X, Y, Z] \neq [0, 0, 0]$, $X, Y, Z \in \mathbb{Z}$, $NWD(X, Y, Z) = 1$. Wtedy $p | X^2 + Y^2$. Jeżeli $p \nmid X$, to $(YX^{-1})^2 \equiv -1 \pmod p$, więc -1 jest resztą kwadratową $\pmod p$, co jest niemożliwe – symbol Legendre'a. Stąd $p | X, Y$, więc $p^2 | pZ^2$ oraz $p | Z$, przecząc $NWD(X, Y, Z) = 1$. Stąd $V_p(\mathbb{Q}) = \varnothing$.
Załóżmy teraz, że $p \equiv 1 \pmod 4$ – wtedy $p = a^2 + b^2$ dla pewnych $a, b \in \mathbb{Z}$. Stąd $[a : b : 1] \in V_p(\mathbb{Q})$. Aby dostać izomorfizm, wystarczy zastosować standardową sztuczkę dla stożkowych – przeprowadzanie prostych przez punkt $[a : b : 1]$.
Część afiniczna V_p ma równanie: $C_p : x^2 + y^2 = a^2 + b^2$. Podstawiając $x := x' + a$, $y := y' + b$ dostajemy: $x'^2 + 2ax' + y'^2 + 2by' = 0$. Przeprowadzamy prostą $y' = tx'$ przez $(0, 0)$ oraz szukamy jej punktu przecięcia z V_p różnego od $(0, 0)$. Dostajemy równania:

$$x'^2 + 2ax' + t^2x'^2 + 2btx' = 0$$

$$(1 + t^2) \cdot x' + (2a + 2bt) = 0$$

$$x' = \frac{-2a - 2bt}{1 + t^2}, \qquad y' = tx' = \frac{-2at - 2bt^2}{1 + t^2} = \frac{2b - 2at}{1 + t^2} - 2b$$

Stąd dostajemy izomorfizm $\mathbb{A}^1 \to C_p$:

$$t \mapsto \left[a + \frac{-2a - 2bt}{1 + t^2}, -b + \frac{2b - 2at}{1 + t^2} \right]$$

Łatwo uzyskać morfizm odwrotny – wystarczy wyliczyć t z powyższych wzorów:

$$\frac{2b - 2at}{-2a - 2bt} = \frac{x - a}{y + b} \Rightarrow t = \frac{yb + xa + b^2 - a^2}{ay - xb + 2ab}$$

czyli ten izomorfizm to:

$$[x, y] \mapsto \frac{yb + xa + b^2 - a^2}{ay - xb + 2ab}$$

Podstawiając $t = \frac{T}{U}$ dostajemy izomorfizm $\mathbb{P}^1 \to V_p$ dany przez:

$$[T, U] \mapsto \left[a + \frac{-2aU^2 - 2bTU}{U^2 + T^2}, -b + \frac{2bU^2 - 2aTU}{U^2 + T^2}, 1 \right] =$$

$$= \left[a(U^2 + T^2) - 2aU^2 - 2bTU, -b(U^2 + T^2) + 2bU^2 - 2aTU, U^2 + T^2 \right]$$

Odwrotny morfizm jest analogicznie dany przez:

$$[X, Y, Z] \mapsto \left[\frac{Yb + Xa + Z \cdot (b^2 - a^2)}{aY - bX + 2abZ}, 1 \right] = \left[Yb + Xa + Z \cdot (b^2 - a^2), aY - bX + 2abZ \right]$$

(b) niech $p \neq q, p, q \equiv 3 \pmod 4$. Wtedy z prawa wzajemności reszt kwadratowych: $(\frac{p}{q})(\frac{q}{p}) = (-1)^{(p-1)(q-1)/4} = -1$, więc $-1 \in \{(\frac{p}{q}), (\frac{q}{p})\}$. Bez straty ogólności załóżmy, że $-1 = (\frac{q}{p})$. Wykażemy, że $V_q(\mathbb{Q}(\sqrt{p})) = \varnothing$.

Mamy: $-1 = (\frac{q}{p})$, więc q rozkłada się w $\mathbb{Q}(\sqrt{p})$ na 2 różne czynniki pierwsze stopnia 1:

$$q = \pi\overline{\pi}, \qquad \mathbb{Z}[\sqrt{p}]/(\pi) \cong \mathbb{Z}[\sqrt{p}]/(\overline{\pi}) \cong \mathbb{Z}/(q) \cong \mathbb{F}_q$$

Załóżmy nie wprost, że $[X,Y,Z] \in V_q(\mathbb{Q}(\sqrt{p}))$, $X,Y,Z \in \mathbb{Z}[\sqrt{p}]$, $NWD((X),(Y),(Z)) = 1$. Wtedy: $X^2+Y^2 = qZ^2$, więc $X^2+Y^2 \equiv 0 \pmod{\pi}$. Liczby te są względnie pierwsze, więc $\pi \nmid X,Y$ oraz $(XY^{-1})^2 \equiv -1 \pmod{\pi}$. Oznacza to, że -1 jest kwadratem w $\mathbb{Z}[\sqrt{p}]/(\pi) \cong \mathbb{F}_q$, jest więc kwadratem w $\mathbb{F}_q$. To jest jednak niemożliwe, bo $(\frac{-1}{q}) = (-1)^{(q-1)/2} = -1$.

Wystarczy teraz zauważyć, że $[\sqrt{p},0,0] \in V_p(\mathbb{Q}(\sqrt{p}))$, więc $V_p(\mathbb{Q}(\sqrt{p})) \neq \varnothing$ i V_p, V_q nie mogą być izomorficzne nad $\mathbb{Q}$.

1.12 (a) Niech $f \in \overline{K}[V]$, $\forall_{\sigma \in G_{\overline{K}/K}} \quad f^\sigma = f$, wykażemy, że $f \in K[V]$.
Niech $F \in K[X_1,\ldots,X_n]$, $F \equiv f \pmod{I(V)}$. Zdefiniujmy $\xi : G_{\overline{K}/K} \to K[X_1,\ldots,X_n]$, $\xi(\sigma) = F^\sigma - F$ i zauważmy, że $im\,\xi \subset I(V)$ – istotnie, zgodnie z założeniem, $F^\sigma - F \equiv f^\sigma - f \equiv 0 \pmod{I(V)}$. Oczywiście ξ jest ciągłe w topologii Krulla (bo działanie $G_{\overline{K}/K}$ na $\overline{K}$ jest ciągłe), a ponadto $\xi(\sigma_1\sigma_2) = F^{\sigma_1\sigma_2} - F = (F^{\sigma_1} - F)^{\sigma_2} + (F^{\sigma_2} - F) = \xi(\sigma_1)^{\sigma_2} + \xi(\sigma_2)$, więc $\xi \in Z^1(G_{\overline{K}/K}, I(V))$.

Z addytywnej wersji 90-tego twierdzenia Hilberta $H^1(G_{\overline{K}/K}, \overline{K}^+) = 0$. Ponadto, jako $G_{\overline{K}/K}$-moduły: $I(V) \cong (\overline{K}^+)^t$ (gdzie $t \in \mathbb{N}$). Istotnie, V jest zdefiniowane nad K, więc $G_{\overline{K}/K}$ działa na $I(V)$. Stąd, z **[AEC, II.5, Lemma 5.8.1]**, $I(V)$ ma (jako przestrzeń liniowa nad $\overline{K}$) bazę $G_{\overline{K}/K}$-niezmienniczną, tzn. $I(V) \cong \oplus_{i=1}^{\infty} f_i \overline{K}$ (izomorfizm przestrzenii K-liniowych) dla pewnych $f_i \in K[X_1,\ldots,X_n]$ (warto zauważyć, że jest to przestrzeń przeliczalnie wymiarowa nad $\overline{K}$, jako że $\overline{K}[X_1,\ldots,X_n]$ jest taką przestrzenią). Stąd dostajemy izomorfizm grup addytywnych: $I(V)^+ \cong \oplus_{i=1}^{\infty} f_i \overline{K}^+$, a ponieważ każdy składnik $f_i\overline{K}^+$ jest $G_{\overline{K}/K}$-modułem (ponieważ $f_i \in K[X_1,\ldots,X_n]$), to $I(V)^+ \cong \oplus_{i=1}^{\infty} \overline{K}^+$ jako $G_{\overline{K}/K}$-moduły.
Stąd $H^1(G_{\overline{K}/K}, I(V)) = H^1(G_{\overline{K}/K}, (\overline{K}^+)^t) = \prod H^1(G_{\overline{K}/K}, \overline{K}^+) = 0$, więc ξ jest kobrzegiem, tzn. $\xi(\sigma) = G^\sigma - G$ dla pewnego $G \in I(V)$. Stąd: $F^\sigma - F = G^\sigma - G$, czyli $(F-G)^\sigma = F - G$, więc $F - G \in K[X_1,\ldots,X_n]$ i ostatecznie (ponieważ $G \in I(V)$) $f \equiv F \equiv F - G \pmod{I(V)}$, co kończy dowód.

(b) **Sposób I:** Niech $P = [x_0,\ldots,x_n] \in \mathbb{P}^n$, $\forall_{\sigma \in G_{\overline{K}/K}} P^\sigma = P$. Zdefiniujmy dla każdego $\lambda \in G_{\overline{K}/K}$ liczbę: $\lambda_\sigma \in \overline{K}$ tak, że $x_i^\sigma = \lambda_\sigma x_i$ dla każdego i. Jak łatwo wtedy sprawdzić, $\sigma \mapsto \lambda_\sigma$ jest kocyklem, więc z 90 tw. Hilberta jest też kobrzegiem, tzn. $\lambda_\sigma = \frac{a^\sigma}{a}$ dla pewnego $a \in \overline{K}$. Stąd dla każdego i zachodzi: $(\frac{x_i}{a})^\sigma = \frac{x_i}{a}$, więc $\frac{x_i}{a} \in K$ oraz $P = [\frac{x_0}{a},\ldots,\frac{x_n}{a}] \in \mathbb{A}^n(K)$.

Sposób II: Załóżmy, że $x_i \neq 0$ – wtedy $P = [\frac{x_0}{x_i},\frac{x_1}{x_i},\ldots,\frac{x_n}{x_i}]$ oraz dla każdych i,σ: $(\frac{x_1}{x_i})^\sigma = \frac{x_1}{x_i}$ (co wynika z $P^\sigma = P$), więc $\frac{x_0}{x_i},\frac{x_1}{x_i},\ldots,\frac{x_n}{x_i} \in K$.

(c) Ustalmy i i niech $V_1' = V_1 \cap \{[x_0,x_1,\ldots,x_n] \in \mathbb{P}^n : x_i = 1\}$. Niech też $e_i = [0,0,\ldots,1,0,\ldots,0]$. Wtedy $\forall_\sigma\, \phi(e_i)^\sigma = \phi(e_i)$, więc $\phi(e_i) \in \mathbb{P}^n(K)$. Niech też V_2' będzie przekrojem V_2 z hiperpłaszyzną afiniczną w $\mathbb{P}^n$, zawierającą $\phi(e_i)$. Wtedy $\phi : V_1 \to V_2$ indukuje odwzorowanie rozmaitości afinicznych $\phi' : V_1' \to V_2'$, spełniające $\phi'^\sigma = \phi'$, a więc określone nad K. Ponieważ zachodzi to dla dowolnego i, to ϕ jest określone nad K.

Rozdział II

2.1 ??????

2.2 Niech $f = t_{\phi(P)}^{ord_{\phi(P)}(f)} \cdot g$, $g(\phi(P)) \in \overline{K}^*$. Wtedy $(\phi^* \circ g)(P) = g(\phi(P)) \in \overline{K}^*$, więc $ord_P(\phi^* g) = 0$ i:

$$ord_P(\phi^* f) = ord_P(t_{\phi(P)}^{ord_{\phi(P)}(f)} \cdot g) = ord_{\phi(P)}(f) \cdot ord_P(\phi^* t_{\phi(P)}) + ord_P(\phi^* g) = ord_{\phi(P)}(f) \cdot e_\phi(P)$$

2.3

(a) Niech $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ będzie dowolnym morfizmem. Wtedy $\phi = [g(X/Y), 1]$ dla pewnej funkcji wymiernej $g \in K(t)$. Niech d będzie stopniem g (tzn. maksimum ze stopnia licznika i mianownika). Zauważmy, że wtedy

$$\deg \phi = [K(\mathbb{P}^1) : \phi^* K(\mathbb{P}^1)] = [K(t) : K(g)] = \deg g.$$

(i) Niech $Q = [a : 1]$ (dla $Q = [1 : 0]$ dowód jest podobny). Łatwo zauważyć, że $g(X/Y) - a$ jest ilorazem dwóch wielomianów jednorodnych stopnia d. Rozkładając te wielomiany na czynniki:

$$g(X/Y) - a = \frac{\prod_{i=1}^{s} (\beta_i X - \alpha_i Y)^{n_i}}{\prod_{i=1}^{t} (\gamma_i X - \omega_i Y)^{m_i}},$$

gdzie $\sum_i n_i = \sum_i m_i = d$. Wtedy $\phi^{-1}(Q) = \{[\alpha_i : \beta_i] : i = 1, \ldots, s\}$ oraz:

$$e_\phi([\alpha_i : \beta_i]) = ord_{[\alpha_i : \beta_i]}(f - a) = n_i.$$

Pozostaje zauważyć, że

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \sum_i n_i = d = \deg \phi.$$

(ii) Niech $g(t) = h(t^q)$, gdzie funkcja wymierna h jest rozdzielcza, zaś q jest równe 1 dla $char(K) = 0$ lub jest potęgą p dla $char(K) = p$. Niech $\psi = [h(X/Y), 1] : \mathbb{P}^1 \to \mathbb{P}^1$. Zauważmy, że:

$$\deg_s(\phi) = [K(\mathbb{P}^1) : \phi^*(K(\mathbb{P}^1))]_{sep} = [K(t) : K(g)]_{sep} = [K(t) : K(h)] = \deg h.$$

Niech S będzie zbiorem zer funkcji h' (jest to zbiór skończony – ma co najwyżej $2d$ elementów, bo $h' \not\equiv 0$). Wybierzmy dowolny punkt $P = [a : 1]$, gdzie $a \notin h(S)$ oraz $P \neq \psi([1 : 0])$. Wtedy $h(t) - a$ jest funkcją wymierną stopnia d, która ma w liczniku wielomian stopnia d (zapewnia to warunek $P \neq \psi([1 : 0])$). Równanie $h(t) = a$ ma $\deg h$ pierwiastków, licząc z krotnościami. Zauważmy jednak, że żaden z tych pierwiastków nie może być podwójny – w przeciwnym wypadku $h(t) = a$, $h'(t) = 0$, więc byłoby $t \in S$ oraz $a \in h(S)$, sprzeczność. Stąd dla prawie wszystkich P: $|\psi^{-1}(P)| = \deg h$. Ale Frobenius jest bijekcją, zatem dla prawie wszystkich P:

$$|\#\phi^{-1}(P)| = |\psi^{-1}(P)| = \deg h = \deg_s(\phi).$$

(b) Niech $D = \sum_i a_i(P_i)$, gdzie $\deg D = \sum a_i > 0$ oraz $P_i = [\alpha_i : \beta_i]$. Wtedy:

$$f \in L(D) \quad \Leftrightarrow \quad f = \prod_i (\beta_i X - \alpha_i Y)^{a_i} \cdot g$$

dla pewnego wielomianu jednorodnego g stopnia $\deg D$. Stąd:

$$\dim L(D) = \text{ (wymiar prz. wielomianów jednorodnych st. } \deg D) = \deg D + 1.$$

2.4

(a) oczywiste.

(b) Wykażemy najpierw, że $dim\big(L(D + (P))/L(D)\big) \leqslant 1$. Istotnie, niech r będzie współczynnikiem przy P w D, zaś t_P – uniformizatorem w P. Wtedy

$$\Phi : L(D + (P)) \to K, \qquad \Phi(f) = (t_P^{r+1} \circ f)(P)$$

jest homomorfizmem o jądrze $L(D)$, więc $dim\big(L(D + (P))/L(D)\big) \leqslant dim\, K = 1$.
Oznacza to, że $dim(L(D + (P))) \leqslant dim(L(D)) + 1$ i dalej indukcyjnie: $dim(L(D + (P_1) + \ldots + (P_s))) \leqslant dim(L(D)) + s$.
Niech teraz $deg\, D = d$ i niech $P \in C$. Wtedy $deg(D - (d+1)(P)) < 0$, więc $dim(L(D - (d+1)(P))) = 0$. Stąd: $\dim(L(D)) \leqslant dim(L(D - (d+1)(P))) + (d+1) = d + 1$.

2.5

(i) ⇒ (ii): $C \cong \mathbb{P}^1 \Rightarrow$ z Example II.5.6:

$$genus(C) = genus(\mathbb{P}^1) = 0.$$

(ii) ⇒ (iii): niech $P \neq Q$ – dwa dowolne punkty na C. Wtedy z Riemanna-Rocha:

$$l((P) - (Q)) = deg((P) - (Q)) + 1 = 1,$$

więc $div(f) \geqslant (Q) - (P)$ dla pewnego $f \in \overline{K}(C)^*$. Dywizor $div(f) + (P) - (Q)$ jest wtedy efektywny stopnia 0, zatem $div(f) = (Q) - (P)$ oraz $(Q) \sim (P)$.

(iii) ⇒ (i): niech $P \neq Q$, $div(f) = (Q) - (P)$. Wtedy f ma jedno zero (w Q) oraz jeden biegun (w P). Niech $\phi : C \to \mathbb{P}^1$,

$$\phi = \begin{cases} [f(R) : 1], & R \neq P \\ [1 : 0], & R = P. \end{cases}$$

– wtedy ϕ jest morfizmem (krzywe są gładkie), a ponadto:

$$\deg \phi = \sum_{R \in \phi^{-1}([0:1])} e_\phi(R) = e_\phi(Q) = ord_Q(\phi^* t_{[0,1]}) = ord_Q(\phi^* X) = ord_Q(f) = 1.$$

Stąd ϕ ma stopień 1 i musi być izomorfizmem.

2.6

(a) zauważmy najpierw, że jeżeli $(P_1) \sim (P_2)$, to $P_1 = P_2$. Istotnie, gdyby $P_1 \neq P_2$ oraz $div(f) = P_1 - P_2$, to $C \ni P \mapsto [f(P) : 1] \in \mathbb{P}^1$ byłoby morfizmem stopnia 1, czyli izomorfizmem.

Stąd punkt R, jeżeli istnieje, to jest wyznaczony jednoznacznie.

Jeżeli np. $P = P_0$ to wystarczy przyjąć $R := Q$. Załóżmy więc, że $P, Q \neq P_0$. Zauważmy, że z twierdzenia Riemanna–Rocha: $\ell((P) + (Q) - (P_0)) = 1$, więc istnieje funkcja f tże $div(f) \geqslant (P_0) - (P) - (Q)$. Ma ona więc jeden lub dwa bieguny pojedyncze, należące do zbioru $\{P, Q\}$ (jest niestała, więc ma przynajmniej 1 biegun). Gdyby jednak miała jeden biegun, np. P, to $div(f) = (P_0) - (P)$, dając $(P_0) \sim (P)$ – sprzeczność z pierwszym akapitem. Stąd musi mieć dwa bieguny pojedyncze P oraz Q, oraz dwa zera (ilość biegunów = ilość zer): P_0 oraz pewien punkt R. Punkt ten spełnia: $P_0 + R = div(f) + P + Q \sim P + Q$.

(b) jako przykład wykażemy łączność:

$$(\sigma(P, \sigma(Q, R))) \sim (P) + (\sigma(Q, R)) - (P_0) \sim (P) + (Q) + (R) - 2(P_0).$$

Analogicznie

$$(\sigma(\sigma(P, Q), R)) \sim (P) + (Q) + (R) - 2(P_0),$$

zatem $(\sigma(P, \sigma(Q, R))) \sim (\sigma(\sigma(P, Q), R))$ oraz (np. z zadania 2.5) $\sigma(P, \sigma(Q, R)) = \sigma(\sigma(P, Q), R)$.

(c) Wystarczy wykazać, że κ jest surjekcją (bo $\kappa(P_1) = \kappa(P_2)$ implikuje $(P_1) \sim (P_2)$, czyli $P_1 = P_2$ z zadania 2.5). Niech $[D] \in Pic^0(C)$. Wtedy $l(D + (P_0)) = 1$, zatem

$$div(f) \geqslant -(D) - (P_0)$$

dla pewnego $f \in \overline{K}(C)^*$. Stąd dywizor $div(f) + D + (P_0)$ jest efektywny stopnia 1, zatem $div(f) + D + (P_0) = (Q)$. Stąd $D \sim (Q) - (P_0) = \kappa(Q)$.

(d) Wystarczy wykazać, że $\kappa(\sigma(P, Q)) = \kappa(P) + \kappa(Q)$, tzn. że $[(\sigma(P, Q)) - (P_0)] = [(P) - (P_0)] + [(Q) - (Q_0)]$, tzn.

$$(\sigma(P, Q)) - (P_0) \sim ((P) - (P_0)) + ((Q) - (Q_0))$$

– to wynika jednak bezpośrednio z definicji σ.

2.7 **Rozwiązanie I:** (dowód dla $char\, K = 0$)

Niech krzywa gładka C będzie zadana przez wielomian jednorodny $F \in K[X,Y,Z]$ stopnia d. Bez straty ogólności (po ewentualnym zastosowaniu transformacji rzutowej) możemy założyć, że $[0,0,1] \notin C(K)$. Zdefiniujmy krzywą: $\widetilde{C} : \frac{\partial F}{\partial Z} = 0$; wtedy $C(\overline{K}) \cap \widetilde{C}(\overline{K})$ jest na mocy twierdzenia Bézout zbiorem skończonym.

Rozważmy morfizm $\phi : C \to \mathbb{P}^1$, $\phi = [X,Y]$. Zauważmy, że dla dowolnego $Q = [a,b] \in \mathbb{P}^1(\overline{K})$, takiego że $\phi^{-1}(Q) \cap \widetilde{C}(\overline{K}) = \varnothing$ jest: $|\phi^{-1}(Q)| = d$. Istotnie, wielomian $g_{a,b}(z) = F(a,b,z)$ ma stopień d (założyliśmy, że $[0,0,1] \notin C(K)$).
Ponadto $\phi^{-1}(Q) \cap \widetilde{C}(\overline{K}) = \varnothing$, więc równości $g_{a,b}(z) = g'_{a,b}(z) = 0$ nie mogą zajść równocześnie i $g_{a,b}$ nie ma pierwiastków wielokrotnych. Oznacza to, że $|\phi^{-1}(Q)| = \left|\{[a,b,z] \in \mathbb{P}^2(\overline{K}) : g_{a,b}(z) = 0\}\right| = d$, więc ϕ jest stopnia d.

Wykażemy teraz, że $e_\phi(P) = 1 + I(C \cap \widetilde{C}, P)$. Bez straty ogólności załóżmy, że $Y(P) \neq 0$ (założyliśmy, że $[0,0,1] \notin C(K)$) i oznaczmy $x = \frac{X}{Y}$, $z = \frac{Z}{Y}$, $f(x,z) = F(x,1,z)$. Z definicji:

$$e_\phi(P) = \mathrm{ord}_P\left(\phi^* t_{\phi(P)}\right) = \mathrm{ord}_P(x - x(P))$$

Jeżeli $P \notin \widetilde{C}(\overline{K})$, to równość jest prawdziwa: $\frac{\partial f}{\partial z}(P) \neq 0$, więc $x - x(P)$ nie jest styczną do C w punkcie P i musi być uniformizatorem w P, czyli $e_\phi(P) = 1 = 1 + I(C \cap \widetilde{C}, P)$. Możemy więc w dalszym ciągu założyć, że $P \in C(\overline{K}) \cap \widetilde{C}(\overline{K})$.

Zauważmy, że

$$0 = df = \frac{\partial f}{\partial x}dx + \frac{\partial f}{\partial z}dz$$

Rozważmy formę różniczkową:

$$\omega = \frac{dx}{\frac{\partial f}{\partial z}} = -\frac{dz}{\frac{\partial f}{\partial x}}$$

Zauważmy, że punkt P jest gładki, więc ponieważ $\frac{\partial f}{\partial z}(P) = 0$, to $\frac{\partial f}{\partial x}(P) \neq 0$, tak więc $z - z(P)$ jest uniformizatorem w P.
Oznacza to, że $\mathrm{ord}_P(\omega) = \mathrm{ord}_P\left(-\frac{d(z-z(P))}{\frac{\partial f}{\partial x}}\right) = 0$.
Korzystając ze wzoru [**Silverman, AEC, Proposition II 4.3(d), str. 31**]:

$$0 = \mathrm{ord}_P(\omega) = \mathrm{ord}_P\left(\frac{d(x - x(P))}{\frac{\partial f}{\partial z}}\right) = \mathrm{ord}_P\left(x - x(P)\right) - 1 - \mathrm{ord}_P\left(\frac{\partial f}{\partial z}\right)$$

Z własności indeksu przecięcia ([**Fulton, Algebraic Curves, 3.3, (8)**]):

$$e_\phi(P) = \mathrm{ord}_P\left(x - x(P)\right) = 1 + \mathrm{ord}_P\left(\frac{\partial f}{\partial z}\right) = 1 + I(C \cap \widetilde{C}, P)$$

To pozwala nam na obliczenie stopnia dywizora ramifikacji za pomocą twierdzenia Bézout:

$$\sum_{P \in C(\overline{K})} (e_\phi(P) - 1) = \sum_{P \in C(\overline{K})} I(C \cap \widetilde{C}, P) = \deg C \cdot \deg \widetilde{C} = d \cdot (d-1)$$

więc za pomocą wzoru Riemanna – Hurwitza dostajemy wzór na genus:

$$2 \cdot \mathrm{genus}(C) - 2 = -2d + d \cdot (d-1),$$

czyli $\mathrm{genus}(C) = \frac{(d-1)(d-2)}{2}$.

Rozwiązanie II: (na podstawie [**Hindry, Silverman, Diophantine Geometry, Theorem A.4.2.6**])

2.8

(a) Niech $g_i = genus(C_i)$. Jeżeli $g_2 = 0$, to teza jest oczywista. Jeżeli $g_2 \geqslant 1$, to z twierdzenia Hurwitza:

$$2(g_1 - 1) = (\deg \phi) \cdot 2(g_2 - 1) + \sum_P (e_\phi(P) - 1) \geqslant (\deg \phi) \cdot 2(g_2 - 1) \geqslant 2(g_2 - 1),$$

co daje $g_1 \geqslant g_2$.

(b) jeżeli $g = 1$, to z tego, że $e_\phi(P) \geqslant 1$ oraz z nierówności Hurwitza $0 \leqslant \sum_P (e_\phi(P) - 1) \leqslant 0$, więc $e_\phi(P) = 1$ dla każdego P oraz ϕ jest nierozgałęzione.

Jeżeli $g \geqslant 2$, to

$$2g - 2 \geqslant (\deg \phi) \cdot (2g - 2) + \sum_P (e_\phi(P) - 1) \geqslant (\deg \phi) \cdot (2g - 2)$$

więc $1 \geqslant \deg \phi$ oraz $\deg \phi = 1$, czyli ϕ jest izomorfizmem.

2.10 Na podstawie **[Galbraith - Mathematics of Public Key Cryptography]** - rozdział 8.2 Theorem 8.3.8 (4), Lemma 8.3.13.

Niech $\varphi : C_1 \to C_2$ – morfizm gładkich krzywych, oznaczmy: $L = \phi^* K(C_2)$, $M = K(C_1)$.
Niech $Q \in C_2$ i rozważmy pierścień funkcji regularnych w Q: $\mathcal{O}_Q \subset K(C_2)$, jego ideał maksymalny $\mathfrak{m}_Q$ oraz ich obrazy: $A = \phi^*(\mathcal{O}_Q) \subset L$, $\mathfrak{m} = \phi^*(\mathfrak{m}_Q) \subset A$. Wtedy A jest lokalną dziedziną Dedekinda z ciałem ułamków L, ideałem maksymalnym $\mathfrak{m}$ oraz waluacją v indukowaną przez $\mathfrak{m}$ (spełniającą $v(\phi^* f) = ord_Q(f)$). Niech B będzie domknięciem całkowitym A w M. Wtedy B jest również dziedziną Dedekinda i $\mathfrak{m}$ rozkłada się na iloczyn ideałów postaci $\mathfrak{m}_P$, gdzie $P \in \phi^{-1}(Q)$ (indukują one waluacje $ord_P^{C_1}$). Wszystkie one mają stopień 1 (tzn. $[B/\mathfrak{m}_P : A/\mathfrak{m}] = 1$).

Dowód zadania w przypadku, gdy M/L jest Galois:

(a) Zgodnie z definicją musimy udowodnić, że $N_{M/L}(f)(Q) = \prod_{P \in \phi^{-1}(Q)} f(P)^{e_\phi(P)}$. Niech $\phi^{-1}(Q) = \{P_1, \ldots, P_g\}$. Rozszerzenie jest Galois, więc dla każdego $P \in \phi^{-1}(Q)$: $e_\phi(P) = e$. Niech $c_P = f(P) \in K$, wtedy oczywiście $c_P \in L$. Zauważmy, że dla każdego i istnieje dokładnie e takich $\sigma \in Gal(M/L)$, że $\sigma(\mathfrak{m}_{P_i}) = \mathfrak{m}_{P_1}$. Ponadto, jeżeli $\sigma(\mathfrak{m}_{P_i}) = \mathfrak{m}_{P_1}$, to ponieważ $f \equiv f(P_i) \equiv c_{P_i} \pmod{\mathfrak{m}_{P_i}}$, to $\sigma(f) \equiv c_{P_i} \pmod{\sigma(\mathfrak{m}_{P_i})}$, (bo $\sigma(c_{P_i}) = c_{P_i}$) tzn. $\sigma(f) \equiv c_{P_i} \pmod{\mathfrak{m}_{P_1}}$.
Stąd:

$$N_{L/M}(f) = \prod_{\sigma \in Gal(M/L)} \sigma(f) \equiv \prod_i c_i^e \pmod{\mathfrak{m}_{P_1}}$$

Ale $\mathfrak{m}_{P_1} \cap A = \mathfrak{m}$, zaś obie strony kongruencji należą do A, więc $N_{L/M}(f) \equiv \prod_i c_i^e \pmod{\mathfrak{m}}$, co oznacza po prostu, że

$$\phi_* f(Q) = N_{L/M}(P_1) = \prod_i c_i^e$$

(b) Zgodnie z definicją wystarczy udowodnić, że $\sum_{P \in \phi^{-1}(Q)} ord_P^{C_1}(f) = ord_Q^{C_2}(\phi_*(f))$.
Rozłóżmy ideał główny $(f) = fA$ na ideały pierwsze: $(f) = \prod_{P \in \phi^{-1}(Q)} \mathfrak{m}_P^{ord_P(f)}$.
Rozważmy normę na ideałach: $N_{M/L}(I) = \prod_{\sigma \in Gal(M/L)} \sigma(I)$.
Wtedy $N_{M/L}(\mathfrak{m}_P) = \mathfrak{m}^{[B/\mathfrak{m}_P : A/\mathfrak{m}]} = \mathfrak{m}$, więc $N_{M/L}((f)) = \prod_{P \in \phi^{-1}(Q)} N_{M/L}(\mathfrak{m}_P)^{ord_P(f)} = \mathfrak{m}^{\sum ord_P(f)}$. Z drugiej strony,

$$N_{M/L}((f)) = (N_{M/L}(f)) = \mathfrak{m}^{v(N_{M/L}(f))} = \mathfrak{m}^{v(N_{M/L}(f))}$$

więc porównując wykładniki: $\sum ord_P(f) = v(N_{M/L}(f)) = ord_Q(\phi_* f)$

2.11

(a) niech $f(X,Y)=\prod_P(\beta_P X-\alpha_P Y)^{n_P}$, gdzie $P=[\alpha_P:\beta_P]$ oraz $g(X,Y)=\prod_P(\gamma_P X-\omega_P Y)^{m_P}$, gdzie $P=[\omega_P:\gamma_P]$. Wtedy:

$$f(div(g))=f(\sum_Q m_Q(Q))=\prod_Q f(Q)^{m_Q}=\prod_Q\prod_P(\beta_P\omega_Q-\gamma_Q\alpha_P)^{n_P m_Q}.$$

Analogicznie:

$$g(div(f))=\prod_P\prod_Q(\gamma_Q\alpha_P-\beta_P\omega_Q)^{n_P m_Q}=(-1)^{\sum_{P,Q} m_Q n_P}\cdot f(div(g))=(-1)^{\sum_P m_Q\cdot\sum_Q m_Q}\cdot f(div(g))=f(div(g)).$$

(przypomnijmy, że $\sum_P n_P=\sum_Q n_Q=0$).

(b) niech $\phi=[g:1]:C\to\mathbb{P}^1$. Niech też $x(P)=X/Y$ (dla $P=[X:Y]$) będzie funkcją pierwszej współrzędnej na $\mathbb{P}^1$. Wtedy korzystając z zadania 2.10 oraz z podpunktu (a):

$$\begin{aligned} f(div(g)) &= f(div(\phi^* x))=f(\phi^*(div(x)))\overset{\text{zad. 2.10}}{=}(\phi_* f)(div(x))= \\ &\overset{\text{(a)}}{=} x(div(\phi_* f))=x(\phi_*(div(f)))\overset{\text{zad. 2.10}}{=}(\phi^* x)(div(f))=g(div(f)).\end{aligned}$$

2.12 Analogicznie jak w **[AEC, Lemma 5.8.1]** wystarczy pokazać, że każdy wektor $v\in V$ jest $\overline{K}$–kombinacją wektorów z $V^{G_{\overline{K}/K}}$.

Zauważmy, że wektor v leży w pewnej $G_{\overline{K}/K}$–niezmienniczej skończenie wymiarowej podprzestrzenii W, np. $W=lin\{v^\sigma:\sigma\in G_{\overline{K}/K}\}$ (z ciągłości działania $G_{\overline{K}/K}$ wynika, że każdy wektor ma skończenie wiele "sprzężeń"). Chcemy wykazać, że W ma $\overline{K}$–bazę $G_{\overline{K}/K}$–niezmienniczą.

Wybierzmy dowolną bazę $E=(e_1,\dots,e_n)$ przestrzeni W. Dla każdego $\sigma\in G_{\overline{K}/K}$ określmy $A_\sigma\in Aut(W)\cong Gl_n(\overline{K})$ przez wartości na bazie jako:

$$\forall_i\quad A_\sigma e_i=e_i^\sigma$$

(dla dowolnego σ ciąg $(e_1^\sigma,\dots,e_n^\sigma)$ też jest bazą, więc A_σ jest odwracalne).

Zauważmy, że $\sigma\mapsto A_\sigma$ jest kocyklem. Istotnie,

$$A_\sigma^\tau A_\tau e_i=A_\sigma^\tau e_i^\tau=(A_\sigma e_i)^\tau=e_i^{\sigma\tau}=A_{\sigma\tau}$$

więc $A_\sigma^\tau A_\tau=A_{\sigma\tau}$. Stąd, ponieważ $H^1(G_{\overline{K}/K},Aut(W))=H^1(G_{\overline{K}/K},Gl_n(\overline{K}))=0$, to A_σ jest również kocyklem, oraz $A_\sigma=B^\sigma B^{-1}$ dla pewnego $B\in Aut(W)$.

Niech $f_i=B^{-1}e_i$ – wtedy $f_i^\sigma=(B^{-1})^\sigma e_i^\sigma=(B^{-1})^\sigma A_\sigma e_i=B^{-1}e_i=f_i$, więc baza $(f_1,\dots,f_n)$ jest $G_{\overline{K}/K}$–niezmiennicza.

2.13 (a) oczywiste.

(b) Ustalmy $\mathcal{O}\in C(K)$. Z zadania 2.6 wynika, że dla każdego $[D]\in Pic_0(C)$ istnieje dokładnie jeden punkt P dla którego $[D]=[(P)-(\mathcal{O})]$. Stąd, jeżeli $[D]\in Pic_K^0(C)$, $[D]=[(P)-(\mathcal{O})]$ to

$$\forall_\sigma\quad [D]=[D]^\sigma\Leftrightarrow[(P)-(\mathcal{O})]=[(P^\sigma)-(\mathcal{O})]\Leftrightarrow P=P^\sigma\Leftrightarrow P\in C(K)$$

Reasumując: $[D]=[\underbrace{(P)-(\mathcal{O})}_{\in Div_K^0(C)}]$.

2.14 *(błąd w treści – rozpatrywane przekształcenie to:* $[1,x,\dots,x^{g+1},y]:C_0\to\mathbb{P}^1$*)*

Niech $C\subset\mathbb{P}^{g+1}$ dane będzie przez układ równań:

$$\begin{cases} Y^2=\sum_{i=0}^{g+1}a_{d-i}X_0X_i+\sum_{i=0}^{g+1}a_{d-g-1-i}X_iX_{g+1} & & (1a)\\ X_t^2=X_{t-1}X_{t+1} & \text{dla } t=1,2,\dots,g & (1b)\\ X_1^j=X_0^{j-1}X_j & \text{dla } j=1,2,\dots,g+1 & (1c)\\ X_g^{g+1-j}=X_{g+1}^{g-j}X_j & \text{dla } j=0,1,\dots,g & (1d)\end{cases} \tag{1}$$

(w razie potrzeby przyjmujemy $a_{-1}=0$). Jasne jest, że obraz C_0 jest zawarty w C.

Rozważmy ponadto podprzestrzenie afiniczne $H:X_0\neq 0$, $H':X_{g+1}\neq 0$. Zauważmy najpierw, że $C\subset H\cup H'$ – istotnie, jeżeli $[0,X_1,\dots,X_{g+1},Y]\in C\setminus H$, to z równań (1b) dostajemy $X_1=X_2=X_3=\ldots=X_g$. Jeżeli ponadto byłoby $X_{g+1}=0$, to z równości (1a) byłoby $Y=0$, co jest niemożliwe.

Niech $x_j = \frac{X_j}{X_0}$, $y = \frac{Y}{X_0}$ i oznaczmy $x = x_1$ – wtedy z równania (1c) $x_j = x_1^j$ i wstawiając te równości do pozostałych równań otrzymujemy równania zerowe (z równań (1b), (1c)), oraz równanie $y^2 = f(x)$. Stąd $C \cap H \cong C_0$.

Niech teraz $v_j = \frac{X_j}{X_{g+1}}$, $w = \frac{Y}{X_{g+1}}$ i oznaczmy $v = v_g$ – wtedy z równania (1d) otrzymujemy $v_j = v_g^{g+1-i}$ i wstawiając te równości do (1) dostajemy równania zerowe oraz równość: $w^2 = f^*(u_g)$, wyznaczającą krzywą C_1. Ponadto $v = \frac{X_g}{X_{g+1}} = \frac{X_0}{X_1} = \frac{1}{x}$, $v = \frac{Y}{X_{g+1}} = \frac{Y}{X_0}\frac{X_0^{g+1}}{X_1^{g+1}} = \frac{y}{x^{g+1}}$ i analogicznie $x = \frac{1}{v}$, $y = \frac{w}{v^{g+1}}$.

Sprawdzimy teraz, że C jest gładka; w tym celu wystarczy sprawdzić, że krzywe afiniczne C_0, C_1 są gładkie, co wynika łatwo z warunku $disc(f) \neq 0$.

Genus (sposób I – stopień dywizora kanonicznego):
Zastanówmy się, dla jakich $P \in C_0$ jest $ord_P(\frac{dx}{y}) \neq 0$ – jest to możliwe tylko, gdy $y = 0$ lub $x - x(P)$ nie jest uniformizatorem w P. Zauważmy, że styczna do punktu $P = (x_0, y_0) \in C_0$ dana jest przez: $-f'(x_0)(x - x_0) + 2y_0(y - y_0) = 0$. Wszystkie proste, poza styczną są uniformizatorami, więc w szczególności $x - x(P)$ nie jest uniformizatorem tylko dla $y_0 = 0$. Niech α będzie dowolnym pierwiastkiem f; obliczymy $ord_{(\alpha,0)}(dx/y)$. Zauważmy, że $0 = \frac{\partial}{\partial x}(y^2 - f(x))dx + \frac{\partial}{\partial y}(y^2 - f(x))dy$, więc $\frac{dx}{y} = \frac{2\,dy}{f'(x)}$. Stąd, jako że y jest uniformizatorem (nie jest styczną), to: $ord_{(\alpha,0)}(dx/y) = ord_{(\alpha,0)}(\frac{2\,dy}{f'(x)}) = 0$. Rozpatrzmy teraz dwa przypadki:

- jeżeli $2 \nmid d$, to jedynym punktem w $C \setminus H$ jest $Q = [0, 0, \ldots, 0, 1, 0]$, odpowiadający punktowi $Q' = [0, 0]$ na krzywej C_1. Zauważmy, że $x = \frac{1}{v}$, więc $dx = \frac{-dv}{v^2}$ oraz $dx/y = -v^{g-1}/w dv$, więc (ponieważ $dv = \frac{2w\,dw}{f^*(v)}$) $dx/y = \frac{-2v^{g-1}dw}{f^*(v)}$. Ponadto styczna y punkcie Q' do krzywej C_1 ma równanie: $v = 0$, więc w jest uniformizatorem w Q'. Z równości $v = \frac{w^2}{a_0 v^d + a_1 v^{d-1} + \ldots + a_d}$ dostajemy więc $ord_Q(v) = 2$. W rezultacie $ord_Q(\frac{dx}{y}) = ord_Q(\frac{-2v^{g-1}dw}{f^*(v)}) = 2 \cdot (g-1)$.
- jeżeli $2|d$, to w $C \setminus H$ znajdują się dwa różne punkty: $Q_i = [0, 0, \ldots, 0, 1, (-1)^i\sqrt{a_0}]$ $(i = 1, 2)$, odpowiadające punktom $Q_i' = [0, (-1)^i\sqrt{a_0}]$ na krzywej C_1. Prosta $v = 0$ nie jest styczną w żadnym z tych punktów, jest więc uniformizatorem oraz $ord_{Q_i}(\frac{dx}{y}) = ord_{Q_i}(-v^{g-1}/w\,dv) = (g-1)$.

W obydwu przypadkach dostajemy: $2 \cdot genus(C) - 2 = deg\, div(\frac{dx}{y}) = 2g - 2$, więc szukany genus to g.

Genus (sposób II – twierdzenie Riemanna-Hurwitza):
Rozważmy morfizm $\phi = [x, 1] : C \to \mathbb{P}^1$. Zauważmy, że $|\phi^{-1}[x, 1]| = |\{[x, \pm\sqrt{f(x)}]\}| = 2$, o ile tylko $f(x) \neq 0$, więc w tych punktach ramifikacja nie występuje oraz $deg\,\phi = 2$. Jeżeli zaś α jest pierwiastkiem f, to $|\phi^{-1}[\alpha, 1]| = 1$, więc ze wzoru $\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = deg\,\phi = 2$ stwierdzamy, że $e_\phi([\alpha, 0]) = 2$. Pozostaje nam sprawdzić ramifikację na punktach leżących na $C \setminus H$. Zauważmy, że $x = \frac{1}{v}$, więc $\phi = [1, v]$.

- jeżeli $2 \nmid d$, to jedynym punktem w $C \setminus H$ jest $Q = [0, 0, \ldots, 0, 1, 0]$, odpowiadający punktowi $Q' = [0, 0]$ na krzywej C_1. Podobnie stwierdzamy, że $|\phi^{-1}([0, 1])| = |\{Q\}| = 1$, więc $e_\phi(Q) = 2$. Stąd stopień dywizora ramifikacji to $\sum(e_\phi(P) - 1) = d \cdot 1 + 1 = d + 1 = 2g + 2$.
- jeżeli $2|d$, to w $C \setminus H$ znajdują się dwa różne punkty: $Q_i = [0, 0, \ldots, 0, 1, (-1)^i\sqrt{a_0}]$ $(i = 1, 2)$, odpowiadające punktom $Q_i' = [0, (-1)^i\sqrt{a_0}]$ na krzywej C_1. Wtedy $\phi^{-1}([0, 1]) = |\{Q_1, Q_2\}| = 2$, więc w tych punktach ramifikacja nie występuje. Ostatecznie stopień dywizora ramifikacji to $\sum(e_\phi(P) - 1) = d \cdot 1 = 2g + 2$

Stąd z twierdzenia Riemanna-Hurwitza (jako że $char\, K \neq 2$ nie dzieli żadnego ze stopni ramifikacji): $2 \cdot genus(C) - 2 = -2 \cdot 2 + (2g + 2)$, więc $genus(C) = g$.

Baza holomoficznych form różniczkowych:
Pokażemy, że bazą holomorficznych form różniczkowych jest $\{x^i\,dx/y : i = 0, 1, \ldots, g-1\}$. Zauważmy najpierw, że formy te są liniowo niezależne nad $\overline{K}$ (w przeciwnym wypadku $1, x, \ldots, x^{g-1}$ byłyby liniowo zależne, ?) i jest ich tyle, ile wynosi wymiar przestrzenii form holomorficznych, tzn. g. Wystarczy więc pokazać, że są holomorficzne.

- załóżmy, że $2 \nmid d$. Zgodnie z tym, co już obliczyliśmy: $div(dx/y) = (2g-2)(Q)$. Oznaczmy: $\mathcal{O} = [1, 0, 0, \ldots, 0, f(0)]$. Widać, że wszystkie bieguny i zera x to (Q) oraz $\mathcal{O}$. Mamy: $x = \frac{1}{v}$, zaś zgodnie z tym, co już liczyliśmy, $ord_Q(v) = 2$, więc $ord_Q(x) = -2$, $ord_\mathcal{O}(x) = 2$ (bo $deg\, div\, x = 0$). Stąd $div(x) = 2(\mathcal{O}) - 2(Q)$, więc $div(x^i\,dx/y) = 2(\mathcal{O}) + (2g - 2 - 2i)(Q) \geqslant 0$ dla $i = 0, 1, \ldots, g-1$,

- załóżmy, że $2|d$. Wtedy $div(dx/y) = (g-1)(Q_1) + (g-1)(Q_2)$ oraz jak łatwo obliczyć, wyznaczając uniformizatory w odpowiednich punktach $div(x) = 2(\mathcal{O}) - (Q_1) - (Q_2)$, więc $div(x^i\, dx/y) = 2(\mathcal{O}) + (g-1-i)(Q_1) + (g-1-i)(Q_2) \geqslant 0$ dla $i = 0, 1, \ldots, g-1$.

2.15 (i) $\Rightarrow$ (ii)
niech $K(C)/K(t)$ – skończone i rozdzielcze rozszerzenie. Oznacza to, że $\phi = [t, 1] : C \to \mathbb{P}^1$ jest rodzielcze, więc w szczególności ramifikuje się w skończenie wielu punktach - poza tymi punktami $1 = e_\phi(P) = ord_P(\phi^* t_{\phi(P)}) = ord_P(t - t(P))$

(ii) $\Rightarrow$ (iii)
$t \in K(C)^p \Rightarrow \quad t = f^p$ dla $f \in K(C) \Rightarrow \quad |ord_P(t - t(P))| = p|ord_P(f - f(P))| \geqslant p > 1$

(iii) $\Rightarrow$ (i)
jeżeli $K(C)/K(t)$ nie jest skończone, to $t = const.$ i z doskonałości K: $t = c^p$ dla pewnego $c \in K$.
Jeżeli $K(C)/K(t)$ nie jest rozdzielcze, to $\phi = [t, 1] : C \to \mathbb{P}^1$ nie jest rozdzielcze, i faktoryzuje się po przez $Frob_q$: $\phi = \lambda \circ Frob_q =$ (z doskonałości K) $= \widehat{\lambda}^q$ dla pewnych $\lambda, \widehat{\lambda} : C \to \mathbb{P}^1$, gdzie $\widehat{\lambda} = [\widehat{f}, 1]$ dla pewnego $\widehat{f} \in K(C)$. Stąd $f = \widehat{f}^q$.

2.16 Niech $P \in C(K)$. Rozważmy ideał M_P pierścienia $\overline{K}[C]_P$ – jest to przestrzeń $\overline{K}$-liniowa, a ponadto działa na niej $G_{\overline{K}/K}$. Istotnie, jeżeli $f \in M_P$, tzn. $f(P) = 0$, to $f^\sigma(P) = f^\sigma(P^\sigma) = (f(P))^\sigma = 0$, więc $f^\sigma \in M_P$. Stąd z Lemma II.5.8.1, M_P ma bazę wektorów $G_{\overline{K}/K}$-niezmienniczych: $\{f_i\}_{i\in J}$. Ale jeżeli $f \in \overline{K}(C)$ jest $G_{\overline{K}/K}$-niezmiennicze, to $f \in K(C)$, zatem $f_i \in K(C)$. Ponadto $ord_P(f_i) \geqslant 1$ dla każdego i, zaś gdyby nierówność $ord_P(f_i) \geqslant 2$ zachodziło dla każdego i, to wszystkie kombinacje liniowe $\{f_i\}_{i\in J}$ byłyby zawarte w M_P^2. Stąd byłoby $M_P \subset M_P^2$ – sprzeczność! Stąd $ord_P(f_i) = 1$ dla pewnego i. To kończy dowód.

Zadania dodatkowe:

2.A Niech $C/\mathbb{C}$ będzie gładką krzywą genusu $\geqslant 1$, zaś $\omega \in \Omega^1(C)$ – niezerową 1–formą holomorficzną na C. Wykaż, że nie istnieją $g_1, \ldots, g_k, h \in \mathbb{C}(C)$ oraz $c_1, \ldots, c_k \in \mathbb{C}$ takie, że $\omega = \sum_{j=1}^k c_j \frac{d\, g_j}{g_j} + dh$.

Rozwiązanie: Zauważmy najpierw, że pochodna logarytmiczna rozkłada iloczyny na sumy i ilorazy na różnice: $\frac{d(UV)}{UV} = \frac{dU}{U} + \frac{dV}{V}$, $\frac{d(U/V)}{U/V} = \frac{dU}{U} - \frac{dV}{V}$.
Załóżmy nie wprost, że równość taka zachodzi oraz że k jest minimalne z możliwych. Zauważmy, że jeżeli $P \in C(\mathbb{C})$, $g = t_P^e \cdot G$, gdzie $G(P) \in \mathbb{C} \setminus \{0\}$, $ord_P(t_P) = 1$ mamy:

$$\frac{dg}{g} = e \underbrace{\frac{dt_P}{t_P}}_{\text{biegun rzędu 1 w } P} + \underbrace{\frac{dG}{G}}_{\text{regularne w } P} \qquad (*)$$

więc w szczególności jeżeli $ord_P(g) = e \neq 0$, to $ord_P(dg/g) = -1$. Jeżeli zaś $ord_P(g) = 0$, to $\frac{dg}{g}$ jest regularne w P.
Ponadto, jeżeli h nie byłoby stałe oraz P byłoby dowolnym biegunem h, to $ord_P(dh) = ord_P(h) - 1 \leqslant -2$ oraz ω miałoby biegun rzędu $\geqslant 2$ w P (bo $\frac{dg_j}{g_j}$ są regularne w P lub mają tam biegun rzędu 1). Stąd $h = const.$, $dh = 0$.
Na podstawie $(*)$ stwierdzamy, że jeżeli $g_j = t_P^{ord_P(g_j)} \cdot G_j$, to:

$$\omega = \sum_j c_j \frac{d\, g_j}{g_j} = \sum_j c_j \left(ord_P(g_j) \frac{dt_P}{t_P} + \frac{dG_j}{G_j} \right) = \left(\sum_{j=1}^k c_j ord_P(g_j) \right) \underbrace{\frac{dt_P}{t_P}}_{\text{biegun rzędu 1 w } P} + \text{coś regularnego w } P$$

więc dla dowolnego P musi być: $\sum_{j=1}^k c_j\, ord_P(g_j) = 0$.
Rozważmy jednorodny układ równań:

$$\forall_P \quad \sum_{j=1}^k x_j ord_P(g_j) = 0 \qquad (**)$$

o niewiadomych $(x_1, \ldots, x_k)$ (układ ten ma tak naprawdę tylko skończenie wiele niezerowych równań, bo $ord_P(g_j) = 0$ dla p.w. P) – ma on niezerowe rozwiązanie $(c_1, \ldots, c_k) \in \mathbb{C}^k$.

Lemat
Jednorodny układ równań liniowych o współczynnikach w $\mathbb{Q}$ ma niezerowe rozwiązanie $(c_1, \ldots, c_k) \in \mathbb{C}^k$ $\Leftrightarrow$ ma niezerowe rozwiązanie $(a_1, \ldots, a_k) \in \mathbb{Z}$.
Dowód: jeżeli $A \in M_{s,t}(\mathbb{Q})$ jest macierzą tego układu, to: $Ax = 0$ ma niezerowe rozwiązanie w $\mathbb{C} \Leftrightarrow$ A ma rząd $< t \Leftrightarrow$ $Ax = 0$ ma niezerowe rozwiązanie w $\mathbb{Q} \Leftrightarrow$ (po pomnożeniu rozwiązania przez mianowniki) $Ax = 0$ ma niezerowe rozwiązanie w $\mathbb{Z}$.

Niech $(a_1, \ldots, a_k) \in \mathbb{Z}^k$ będzie niezerowym rozwiązaniem układu $(**)$ (bez straty ogólności $a_k \neq 0$) i rozważmy funkcję: $T = \prod_j g_j^{a_k} \in \mathbb{C}(C)$ – spełnia ona dla każdego P: $div(T) = \sum_j a_j ord_P(g_j) = 0$, więc jest stała. Stąd:

$$0 = \frac{dT}{T} = \sum_j a_j \frac{dg_j}{g_j} \quad \Rightarrow \quad \frac{dg_k}{g_k} = \sum_{j=1}^{k-1} -\frac{a_j}{a_k} \frac{dg_j}{g_j}$$

oraz:

$$\omega = \sum_{j=1}^{k} c_j \frac{d\, g_j}{g_j} = \sum_{j=1}^{k-1} (c_j - \frac{a_j}{a_k}) \frac{dg_j}{g_j}$$

przecząc minimalności k.

Rozdział III

3.7 **[Washington, Elliptic curves – number theory and cryptography, 3.3, 9.5]**

3.8 (a) wystarczy zauważyć, że podgrupa $(\mathbb{C}/L)[m]$ elementów grupy $\mathbb{C}/L = \mathbb{C}/(\tau_1\mathbb{Z} + \tau_2\mathbb{Z})$ (gdzie $\tau_1/\tau_2 \notin \mathbb{R}$, $\tau_1, \tau_2 \neq 0$) to $\{a\frac{\tau_1}{m} + b\frac{\tau_2}{m} : a, b \in \mathbb{Z}/m\} \cong \mathbb{Z}/m \times \mathbb{Z}/m$. Stąd $deg[m] = |ker[m]| = m^2$.

(b) Ciało K jest charakterystyki 0, więc w naturalny sposób zawiera kopię $\mathbb{Q}$. Niech $E : y^2 = x^3 + px + q$ $(p, q \in K)$. Rozważmy ciało $L = \mathbb{Q}(p, q) \subset K$. Zauważmy, że L jest skończenie generowane nad $\mathbb{Q}$ (jest generowane przez p, q), więc można skorzystać z następującego lematu:

> **Lemat** Jeżeli ciało L jest skończenie generowane nad $\mathbb{Q}$ (tzn. ma skończony stopień transcendentny nad $\mathbb{Q}$), to istnieje zanurzenie $\overline{L} \to \mathbb{C}$.
> (Źródło: **[Washington, Elliptic Curves, Apprendix C, Corollary C.6]**)
>
> **Dowód:** Niech $\alpha_1, \ldots, \alpha_n \in L$ będzie bazą transcendentną $L/\mathbb{Q}$ (tzn. maksymalnym zbiorem algebraicznie niezależnym), i niech $F = \mathbb{Q}(\alpha_1, \ldots, \alpha_n) \subset L$. Zauważmy, że stopień transcendentny $\mathbb{C}/\mathbb{Q}$ jest równy $\mathfrak{C}$, więc możemy wybrać algebraicznie niezależne elementy $\tau_1, \ldots, \tau_n$, i zdefiniować zanurzenie $\tau : F \to \mathbb{C}$ przez $\tau(\alpha_i) = \tau_i$ $(i = 1, \ldots, n)$. Takie zanurzenie możemy jednak przedłużyć do zanurzenia $\widetilde{\tau} : \overline{F} \to \mathbb{C}$. Rozszerzenie L/F jest algebraiczne (bo $\alpha_1, \ldots, \alpha_n$ był **maksymalnym** zbiorem algebraicznie niezależnym), więc $L \subseteq \overline{F}$ i $\overline{L} = \overline{F}$. Stąd $\widetilde{\tau} : \overline{L} \to \mathbb{C}$ jest szukanym zanurzeniem.

Prawo dodawania na krzywych jest zdefiniowane przez funkcje wymierne o współczynnikach z L, więc $E_{tors} \subset E(\overline{L})$. Zanurzenie $\tau : \overline{L} \to \mathbb{C}$ indukuje izomorfizm grupy $E(\overline{L})$ z grupą $E'(\tau(\overline{L}))$ (gdzie $E' : y^2 = x^3 + \tau(p)x + \tau(q)$), więc w szczególności $E[m] \cong E'[m] \cong \mathbb{Z}/m \times \mathbb{Z}/m$.

3.9 (a) definicja dodawania.

(b) pokażemy, że dla gładkiej krzywej C oraz $P \in C$ zachodzi: $I(H_C \cap C, P) = r \Leftrightarrow$ prosta L styczna do C w P spełnia: $I(C \cap L, P) = r + 2$.

(c) zgodnie z tw. Bezout: $\sum I(H_C \cap C, P) = 9$. Ale $I(H_C \cap C, P) = I(C \cap L, P) - 2 \leqslant 1$, więc punktów w $H_C \cap C$ jest dokładnie 9.

3.5 załóżmy, że (x_0, y_0) jest osobliwością na E/K; wykażemy, że $x_0, y_0 \in K$. Istotnie, jeżeli $\sigma \in Gal(\overline{K}/K)$, to $\sigma((x_0, y_0))$ jest osobliwością na $\sigma(E) = E$. Ale E może mieć tylko jedną osobliwość, więc $\sigma(x_0, y_0) = (x_0, y_0)$. Stąd $(x_0, y_0) \in E(K)$. Możemy więc bez straty założyć, że $(x_0, y_0) = (0, 0)$.

(a) załóżmy, że $(0, 0)$ jest nodem.
– wtedy $f_x(P) = f_y(P) = 0$ i rozwijając f w szereg Taylora:

$$f(x, y) - f(0, 0) = (y - \alpha_1 x)(y - \alpha_2 x) - x^3$$

$$(y - \alpha_1 x)(y - \alpha_2 x) = f(x, y) + x^3 \in K(x, y)$$

(bo C jest zdefiniowana nad K, czyli $f \in K[x, y]$) więc $[K(\alpha_1, \alpha_2) : K] \in \{1, 2\}$. Jeżeli $\alpha_1, \alpha_2 \in K$, to analogicznie jak w **[III Proposition 2.5]** pokazujemy, że

$$E_{ns}(K) \to K^* \qquad (x, y) \mapsto \frac{y - \alpha_1 x}{y - \alpha_2 x}$$

jest izomorfizmem.
Załóżmy, że $\alpha_1, \alpha_2 \notin K$ oraz $[L : K] = [K(\alpha_1, \alpha_2) : K] = 2$. Pokażemy, że

$$E_{ns}(K) \to \{t \in L : N_{L/K}(t) = 1\} \qquad (x, y) \mapsto \frac{y - \alpha_1 x}{y - \alpha_2 x}$$

jest izomorfizmem. Niech $Gal(L/K) = \{1, \tau\}$. Wtedy $\tau(\alpha_1) = \alpha_2$ i na odwrót.
Zauważmy, że z 90tego twierdzenia Hilberta:

$$\{t \in L : N_{L/K}(t) = 1\} = \{\frac{s}{\sigma(s)} : \sigma \in Gal(L/K)\} =$$

$$\left\{\frac{s}{\sigma(s)} : \sigma \in Gal(L/K)\right\} = \left\{\frac{a+\alpha_1 b}{a+\alpha_2 b} : a, b \in K\right\}$$

3.12 Załóżmy, że $\phi \in ker(Aut(E) \mapsto Aut(E[m]))$, tzn. ϕ jest takim automorfizmem E, że

$$\forall_{P \in E[m]} \qquad \phi(P) = P \Rightarrow E[m] \subset ker(\phi - id)$$

Wtedy z twierdzenia Lagrange'a $m^2 = |E[m]|$ dzieli $|ker(\phi - I)| = \deg(\phi - id)$. Stąd albo $\deg(\phi - id) = 0$, tzn. $\phi = id$, albo też $m^2 \leqslant \deg(\phi - id)$.
Ale deg jest formą kwadratową, więc stosując nierówność trójkąta:

$$m \leqslant \sqrt{\deg(\phi - id)} \leqslant \sqrt{\deg(\phi)} + \sqrt{\deg(-id)} = 1 + 1$$

Jeżeli $m = 2$, to równość w nierówności trójkąta jest możliwa tylko, gdy $\phi = k \cdot id$, a ponieważ ϕ ma być izomorfizmem to $k = \pm 1$.

3.13 (a) teza wynika z **[Silverman, AEC, II Theorem 2.4 c)]** zastosowanego do podciała elementów stałych przy działaniu Φ (tzn. $\overline{K}(C)^\Phi$) ciała $\overline{K}(C)$.

(b) Niech $Q \in C$. Podobnie jak zadaniu 2.10 rozważamy rozszerzenie ciał $\overline{K}(C)/\phi^*\overline{K}(C') = \overline{K}(C)/\overline{K}(C)^\Phi$. Jest to rozszerzenie Galois (jako że $\overline{K}(C)^\Phi$ jest ciałem stałym ze względu na podgrupę automorfizmów), w szczególności jest rozdzielcze. Rozważmy też pierścienie Dedekinda: $A = \phi^*\mathcal{O}_Q \subset \overline{K}(C)^\Phi$ oraz B, zdefiniowe jako domknięcie całkowite A w $\overline{K}(C)$. Rozważmy ponadto ideał maksymalny $\mathfrak{m} = \phi^*\mathfrak{m}_Q$ – wtedy $\mathfrak{m}B = \prod_{P \in \varphi^{-1}(Q)} \mathfrak{m}_P^e$ gdzie $e = e_\phi(P)$ (wykładniki są równe, bo rozszerzenie jest Galois). Wybierzmy dowolny $P \in \varphi^{-1}(Q)$ i rozważmy grupę dekompozycji

$$D_{\mathfrak{m}_P} = \{\sigma \in Gal(\overline{K}(C)/\overline{K}(C)^\Phi) : \sigma(\mathfrak{m}_P) = \mathfrak{m}_P\}$$

– ma ona moc $ef = e$ (stopień każdego ideału jest równy 1).
Z drugiej strony, $Gal(\overline{K}(C)/\overline{K}(C))^\Phi = \Phi^* = \{\alpha^* : \alpha \in \Phi\}$ oraz $\alpha^*(\mathfrak{m}_P) = \{f \circ \alpha \in \overline{K}(C) : f(P) = 0\} = \{g \in \overline{K}(C) : g(\alpha^{-1}(P)) = 0\} = \mathfrak{m}_{\alpha^{-1}(P)}$. Stąd:

$$D_{\mathfrak{m}_P} = \{\sigma \in Gal(\overline{K}(C)/\overline{K}(C)^\Phi) : \mathfrak{m}_{\alpha^{-1}(P)} = \mathfrak{m}_P\} = \{\alpha^* \in \Phi^* : \alpha^{-1}(P) = P\}$$

gdzie ostatnia równość wynika z następującego lematu:

> **Lemat** Niech $Q, Q' \in C(\overline{K})$. Wtedy jeżeli $\mathfrak{m}_Q \subset \mathfrak{m}_{Q'}$, to $Q = Q'$ (gdzie $\mathfrak{m}_Q := \{f \in \overline{K}(C) : f(Q) = 0\}$). (źródło: **[Galbraith - Mathematics of Public Key Cryptography, słabsza wersja Lemma 7.1.19]**)
>
> **Dowód lematu:** bez straty ogólności (po ewentualnej liniowej zamianie zmiennych) możemy założyć, że $P, Q \in U_n = \{[x_0, \ldots, x_n] \in \mathbb{P}^n : x_n \neq 0\} \cong \mathbb{A}^n$. Niech $C' = C \cap U_n$ będzie odpowiednią rozmaitością afiniczną. Niech $R = \overline{K}(C')$ będzie pierścieniem współrzędnych C', zaś $\mathfrak{m} = \mathfrak{m}_Q \cap R = \{f \in R : f(Q) = 0\}$, $\mathfrak{n} = \mathfrak{m}_{Q'} \cap R$. Wtedy $\mathfrak{m}$, $\mathfrak{n}$ są ideałami maksymalnymi ($f \mapsto f(P)$ wyznacza izomorfizm $R/\mathfrak{m} \cong \overline{K}$, więc pierścień ilorazowy jest ciałem i $\mathfrak{m}$ jest ideałem maksymalnym), więc z twierdzenia Hilberta o zerach $|V(\mathfrak{m})| = |V(\mathfrak{n})| = 1$, co daje $V(\mathfrak{m}) = \{Q\}$, $V(\mathfrak{n}) = \{Q'\}$.
> Ponadto $\mathfrak{m}_Q \subset \mathfrak{m}_{Q'}$, więc $\mathfrak{m} \subset \mathfrak{n}$ i z maksymalności ideałów: $\mathfrak{m} = \mathfrak{n}$, czyli $\{Q\} = V(\mathfrak{m}) = V(\mathfrak{n}) = \{Q'\}$.

Stąd: $e = |D_{\mathfrak{m}_P}| = |\{\alpha^* \in \Phi^* : \alpha(P) = P\}|$.

(d) stopień ϕ to stopień rozszerzenia $\overline{K}(C)/\overline{K}(C)^\Phi$, czyli $|\Phi|$, więc z twierdzenia Riemanna–Hurwitza:

$$2genus(C) - 2 = (2genus(C') - 2) \cdot |\Phi| + \sum (e_\phi(P) - 1) =$$

$$= (2genus(C') - 2) \cdot |\Phi| + \sum_{\alpha \in \Phi \setminus \{id\}} |\{P \in C : \alpha P = P\}|$$

3.15 (a) niech $(S,T) \in \ker\phi \times \ker\widehat{\phi}$ i niech $T_0 \in E_2$ będzie takie, że $\phi(T_0) = T$. Rozważmy dywizor

$$D_{\phi,T} = \phi^*(T) - \phi^*(O) = \sum_{P\in\ker\phi} ((T_0+P)-(P))$$

Wtedy $deg(D_{\phi,T}) = 0$, a ponadto

$$sum(D_{\phi,T}) = \sum_{P\in\ker\phi}(T_0+P-P) = [|\ker\phi|]T_0 = [m]T_0 = \widehat{\phi}(\phi(T_0)) = \widehat{\phi}(T) = O$$

(bo $T \in \ker\widehat{\phi}$). Stąd $D_{\phi,T} = div(g_{\phi,T})$ dla pewnego $g_{\phi,T} \in \overline{K}(C)$. Ponadto $S \in \ker\phi$, więc $\ker\phi + S = \ker\phi$ co daje:

$$div(g_{\phi,T}(X+S)) = \sum_{P\in\ker\phi}((T_0+P-S)-(P-S)) = \sum_{P\in\ker\phi+S}((T_0+P)-(P)) =$$

$$= \sum_{P\in\ker\phi}((T_0+P)-(P)) = div(g_{\phi,T})$$

więc $g_{\phi,T}(X+S)/g_{\phi,T}(X)$ jest stałą i możemy zdefiniować: $e_\phi(S,T) = g_{\phi,T}(X+S)/g_{\phi,T}(X)$

(c) zauważmy, że $div(\psi^* g_{\phi,T}) = \psi^*(\phi^*(T) - \phi^*(O)) = (\phi\circ\psi)^*(T) - (\phi\circ\psi)^*(O) = div(g_{\phi\circ\psi,T})$, więc bez straty ogólności można przyjąć, że $\psi^* g_{\phi,T} = g_{\phi\circ\psi,T}$. Stąd:

$$e_{\phi\circ\psi}(S,T) = g_{\phi\circ\psi,T}(X+S)/g_{\phi\circ\psi,T}(X) = \psi^* g_{\phi,T}(X+S)/\psi^* g_{\phi,T}(X) = g_{\phi,T}(\psi(X)+\psi(S))/g_{\phi,T}(\psi(X))$$

(b)
- **jest "alternująca", tzn.** $e_\phi(S,T) = e_{\widehat{\phi}}(T,S)^{-1}$**:**
  niech S', T' będą takie, że $\widehat{\phi}(S') = S$, $\phi(T') = T$. Wtedy, korzystając z podpunktu c) i własności Weil pairing:

  $$e_\phi(S,T) = e_\phi(\widehat{\phi}(S'),T) = e_{\phi\circ\widehat{\phi}}(S',T) = e_m(S',T) = e_m(S',\phi(T')) = e_m(\widehat{\phi}(S'),T') = e_m(S,T') =$$
  $$= e_m(T',S)^{-1} = e_{\widehat{\phi}\circ\phi}(T',S)^{-1} = e_{\widehat{\phi}}(\phi(T'),S)^{-1} = e_{\widehat{\phi}}(T,S)^{-1}$$

  (jak widać c) pozwala nam w wielu przypadkach na sprowadzenie badania własności e_ϕ do badania e_m)
- **liniowość ze względu na pierwszą zmienną:**
- **liniowość ze względu na drugą zmienną:**
- e_ϕ **jest niezdegenerowane:**
- **niezmienniczość Galois:** zauważmy, że ϕ jest zdefiniowane nad K, więc $\widehat{\phi}$ również i $\ker\phi^\sigma = \ker\phi$ oraz $\widehat{\phi}^\sigma(T_0^\sigma) = T^\sigma$ dla dowolnego $\sigma \in G_{\overline{K}/K}$. Stąd

  $$div(g_{\phi,T}^\sigma) = \sum_{P\in\ker\phi}((T_0^\sigma+P^\sigma)-(P^\sigma)) = \sum_{P\in\ker\phi^\sigma}((T_0^\sigma+P)-(P)) = \sum_{P\in\ker\phi}((T_0^\sigma+P)-(P)) = div(g_{\phi,T^\sigma})$$

  więc $e_\phi(S,T)^\sigma = (g_{\phi,T}(X+S)/g_{\phi,T}(X))^\sigma = g_{\phi,T}^\sigma(X^\sigma+S^\sigma)/g_{\phi,T}^\sigma(X^\sigma) = g_{\phi,T^\sigma}(X^\sigma+S^\sigma)/g_{\phi,T^\sigma}(X^\sigma) = e_\phi(S^\sigma,T^\sigma)$.

3.16 (a) niech $D, D', E, E' \in Div^0(E)$, $sum(D) = sum(D') = P$, $sum(E) = sum(E') = Q$, $f, f', g, g' \in K(C)$, $div(f) = mD$, $div(f') = mD'$, $div(g) = mE$, $div(g') = mE'$; chcemy pokazać, że $\frac{f(D)}{g(E)} = \frac{f'(D')}{g'(E')}$.

Załóżmy najpierw, że $supp\, D \cap supp\, E' = supp\, D' \cap supp\, E = \varnothing$. Zauważmy, że $sum(D-D') = \mathcal{O}$ oraz $deg\,(D-D') = 0$, więc $D - D' \sim 0$ oraz $D - D' = div(s)$ dla pewnego $s \in K(C)^*$. Ponadto $div(s^m) = div(f/f')$, więc f/f' oraz s^m różnią się o stałą: $f/f' = c\cdot s^m$. Stąd z prawa wzajemności Weila (*):

$$\frac{f(E)}{f'(E)} = \prod \frac{f}{f'}(P)^{n_P} = \prod (c\cdot s^m)(P)^{n_P} = c^{deg\,E} s^m(E) = s(mE) =$$

$$= s(div(g)) \overset{(*)}{=} g(div(s)) = g(D-D') = \frac{g(D)}{g(D')}$$

czyli $f(E)/g(D) = f'(E)/g(D')$ i analogicznie $f'(E)/g(D') = f'(E')/g'(D')$.

Jeżeli $supp\, D \cap supp\, E', supp\, D' \cap supp\, E \neq \varnothing$, to możemy znaleźć $D'', E'' \in Div^0(E)$ o wymaganych własnościach takie, że $supp\, D'' \cap (supp\, D \cup supp\, D') = \varnothing$, $supp\, E'' \cap (supp\, E \cup supp\, E') = \varnothing$ i wtedy z już udowodnionego przypadku: $f(E)/g(D) = f''(E'')/g''(D'') = f'(E')/g'(D')$.

(b) korzystając z prawa wzajemności Weila (*):

$$\widetilde{e}_m(P,Q)^m = \left(\frac{f_P(D_Q)}{f_Q(D_P)}\right)^m = \frac{f_P(mD_Q)}{f_Q(mD_P)} = \frac{f_P(div(f_Q))}{f_Q(div(f_P))} \overset{(*)}{=} 1$$

3.21 (a) niech E, E' będą zadane wzorami Weierstrassa, i takie, że $E \cong C$, $E' \cong C'$ – wtedy z definicji $j(C,O) = j(E)$, $j(C',O') = j(E')$. Ponadto $E \cong E \cong C \cong C' \cong E'$, więc $j(E) = j(E')$.

(b) ten automorfizm to translacja $\tau_{O'}(P) = P + O'$.

3.22 (a) zauważmy, że C ma strukturę krzywej eliptycznej nad $\overline{K}$ (bo $C(\overline{K}) \neq \varnothing$ i C ma genus 1). Stąd istnieje krzywa E o równaniu Weierstrassa $E : y^2 = x^3 + px + q$ ($p, q \in \overline{K}$) izomorficzna z C; niech $\phi : C \to E$ będzie izomorfizmem. Wtedy dla $\sigma \in G_{\overline{K}/K}$: $\phi^\sigma : C^\sigma \to E^\sigma$ jest izomorfizmem (gdzie $E^\sigma : y^2 = x^3 + \sigma(p)x + \sigma(q)$, itd.). Zauważmy, że C jest zdefiniowane nad K, więc $C^\sigma = C$ oraz $E \cong C = C^\sigma \cong E^\sigma$. Krzywe E, E^σ zadane krótkimi równaniami Weierstrassa są izomorficzne, więc $j(E) = j(E^\sigma)$. Stąd dla dowolnego $\sigma \in G_{\overline{K}/K}$:

$$\sigma(j(E)) = \sigma\left(1728\frac{4p^3}{4p^3+27q^2}\right) = 1728\frac{4\sigma(p)^3}{4\sigma(p)^3+27\sigma(q)^2} = j(E^\sigma) = j(E)$$

więc $j(E) \in K$.

(b) jeżeli $(E,O)/K$, to $O \in E(K)$. Na odwrót, jeżeli $O \in E(K)$ jest dowolnym punktem, to z definicji para (E,O) jest krzywą eliptyczną.

(c) niech $E : y^2 = x^3 + px + q$ ($p, q \in \overline{K}$) będzie dowolnym równaniem Weierstrassa odpowiadającym C. Wiemy już, że $j(E) = \frac{1728\cdot 4p^3}{4p^3+27q^2} \in K$. Załóżmy najpierw, że $p, q \neq 0$. Niech $c = \sqrt{\frac{p}{q}}$, $E' : y^2 = x^3 + c^4px + c^6q = x^3 + \frac{p^3}{q^2}x + \frac{p^3}{q^2}$. Wtedy $E \to E'$, $(x,y) \mapsto (c^2x, c^3y)$ jest izomorfizmem krzywych. Ponadto $\frac{p^3}{q^2} = \frac{1728\cdot 4\cdot j(E)-4}{27} \in K$, więc E'/K.

3.23 (dla *char* $K \neq 2,3$) Niech $C_\alpha : y^2 + \alpha xy + y = x^3$. Podstawiając $s = y + \frac{\alpha x+1}{2}$, $t = x + \frac{\alpha^2}{12}$ dostajemy krzywą eliptyczną $E_\alpha : s^2 = t^3 + (\alpha/2 - \alpha^4/48)t + (1/4 + \alpha^6/864 - \alpha^3/24)$ o j-niezmienniku: $j(E_\alpha) = \frac{\alpha^3(\alpha^3-24)^2}{(\alpha^3-27)}$ oraz wyróżniku: $\Delta(E_\alpha) = \alpha^3 - 27$.

(a) niech E będzie krzywą eliptyczną o j-niezmienniku równym j. Wtedy w $\overline{K}$ równanie $\frac{\alpha^3(\alpha^3-24)^2}{(\alpha^3-27)} = j$ ma rozwiązanie α_0. Stąd $j(E_{\alpha_0}) = j(E)$ oraz $E \cong E_\alpha \cong C_\alpha$.

(b)

(c) dla $\alpha = \xi_3^j \sqrt[3]{27}$ ($j = 0, 1, 2$)

3.24 Niech $\mathcal{P} = (P_1, P_2, \dots,) \in T_\ell(E)$, $\mathcal{Q} = (Q_1, Q_2, \dots,) \in T_\ell(E)$ (tzn. $P_n, Q_n \in E[\ell^n]$) będzie bazą $T_\ell(E) \cong \mathbb{Z}_\ell^2$ (jako $\mathbb{Z}_\ell$ modułu). Niech też $\phi \in End_K(E) \setminus \mathbb{Z}$, zaś $\rho(\phi) \in Gl_2(\mathbb{Z}_\ell) \subset Gl_2(\mathbb{Q}_\ell)$ będzie macierzą ϕ_ℓ w bazie $(\mathcal{P}, \mathcal{Q})$. Zauważmy, że ϕ jest zdefiniowane nad K, więc dla dowolnego $\sigma \in G_{\overline{K}/K}$: $\phi \circ \sigma = \sigma \circ \phi$. Wykażemy najpierw, że macierz $\rho(\phi)$ nie jest postaci nI_2 ($n \in \mathbb{Z}_l$).

Istotnie, załóżmy nie wprost, że $\rho(\phi) = nI_2$ dla pewnego $n \in \mathbb{Z}_\ell$. Oznacza to, że obrazy $\phi \otimes 1$ oraz $id \otimes n \in End(E) \otimes \mathbb{Z}_\ell$ przy naturalnym odwzorowaniu $End(E) \otimes \mathbb{Z}_l \to End(T_\ell(E))$ są równe, więc zgodnie z **[Silverman, AEC, III, Theorem 7.4]** mamy: $\phi \otimes 1 = id \otimes n \in End(E) \otimes \mathbb{Z}_l$. Zauważmy, że $End(E)$ jest wolnym $\mathbb{Z}$ – modułem rangi $\leqslant 4$, tzn. (jako $\mathbb{Z}$ - moduły) $End(E) \cong \mathbb{Z}^k$ dla $k \in \{0, 1 \dots, 4\}$. Niech $e_1, e_2, \dots, e_k$ będzie dowolną bazą $End(E)$ jako $\mathbb{Z}$ -modułu – wtedy $End(E) \otimes \mathbb{Z}_\ell$ ma naturalną strukturę $\mathbb{Z}_\ell$-modułu, a ponadto: $End(E) \otimes \mathbb{Z}_\ell \cong \mathbb{Z}^k \otimes \mathbb{Z}_\ell \cong \mathbb{Z}_\ell^k$, przy czym bazą $End(E) \otimes \mathbb{Z}_\ell$ jako wolnego $\mathbb{Z}_\ell$ modułu jest $e_1 \otimes 1, \dots, e_k \otimes 1$. Niech $\phi = \sum a_i e_i$, $id = \sum b_i e_i$ ($a_i, b_i \in \mathbb{Z}$) – wtedy

$$\sum a_i(e_i \otimes 1) = \phi \otimes 1 = id \otimes n = \sum b_i n(e_i \otimes 1)$$

więc porównując współczynniki bazy: $a_i = nb_i$, czyli $n \in \mathbb{Z}$ oraz $\phi = \sum a_i e_i = n \sum b_i e_i = n \cdot id$, wbrew założeniu, że $\phi \notin \mathbb{Z}$.

Możemy więc skorzystać z następującego lematu:

Lemat Niech L będzie dowolnym ciałem, zaś $A \in Gl_2(L)$, będzie nieskalarną macierzą (tzn. $A \neq lI_2$ dla dowolnego $l \in L$). Wtedy centralizatorem A, zdefiniowanym jako $Z(A) := \{B \in Gl_2(L) : AB = BA\}$ jest zbiór $\{l_1 I_2 + l_2 A : l_1, l_2 \in L\}$. W szczególności, jeżeli $B, B' \in Z(A)$, to $BB' = B'B$.

Dowód: zauważmy najpierw, że skoro A nie jest macierzą skalarną, to istnieje wektor $v \in L^2$, $v \neq 0$ nie będący wektorem własnym A. Wtedy (v, Av) jest bazą L^2 i w tej bazie A ma postać $\begin{pmatrix} 0 & * \\ 1 & * \end{pmatrix}$, tzn. $TAT^{-1} = \begin{pmatrix} 0 & x \\ 1 & y \end{pmatrix} =: A'$ dla $T \in Gl_2(L)$. Ale jeżeli macierz $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ komutuje z macierzą A' to (z bezpośrednich obliczeń): $xc = b$, $a + yc = d$, więc $B = \begin{pmatrix} a & xc \\ c & a+yc \end{pmatrix} = aI_2 + c\begin{pmatrix} 0 & x \\ 1 & y \end{pmatrix}$, więc $Z(A') = \{aI_2 + cA' : a, c \in L\}$ oraz $Z(A) = T^{-1}Z(A')T = \{aI_2 + cA : a, c \in L\}$, co kończy dowód.

Wystarczy więc teraz rozważyć zanurzenie $\rho : G_{\overline{K}/K} \to Gl_2(\mathbb{Z}_\ell) \subset Gl_2(\mathbb{Q}_\ell)$ (reprezentację Galois) i zauważyć, że (ponieważ $\phi \circ \sigma = \sigma \circ \phi$, więc $\rho(\phi)\rho(\sigma) = \rho(\sigma)\rho(\phi)$) $\rho(G_{\overline{K}/K}) \subset Z(\rho(\phi))$.

3.29 (a) Rozważmy morfizm $P \mapsto x(P)$ (pierwszą współrzędną równania Weierstrassa). Wtedy $f = x \circ \tau_T = \tau_T^* \circ x$, więc

$$div(f) = div(\tau_T^* \circ x) = \tau_T^* div(x) = \tau_T^*((P_1) + (P_2) + (P_3) - 3(\mathcal{O})) = (P_1 + T) + (P_2 + T) + (P_3 + T) - 3(T)$$

(gdzie $\{P_1, P_2, P_3\} = E[2] \setminus \{\mathcal{O}\}$).

($\Rightarrow$) Załóżmy, że $T \in E[3]$ - wtedy $T + T + T = \mathcal{O}$ oraz $P_1 + T \quad + P_2 + T \quad + P_3 + T = \mathcal{O}$ więc (z definicji dodawania) istnieją proste $L = \alpha X + \beta Y + \gamma Z$, $L' = \alpha' X + \beta' Y + \gamma' Z$ które przecinają E odpowiednio w $P_1 + T$, $P_2 + T$, $P_3 + T$ oraz (z krotnością 3) w P. Wtedy $div(L/L') = (P_1 + T) + (P_2 + T) + (P_3 + T) - 3(T) = div(f)$, więc $f = c \cdot L/L'$ ($c = const. \in \overline{K}$) i f jest transformacją liniową.
($\Leftarrow$) Załóżmy, że $f = \frac{\alpha X + \beta Y + \gamma Z}{\alpha' X + \beta' Y + \gamma' Z}$. Rozpatrzmy dywizor biegunów f: z jednej strony $(f)_\infty = 3(T)$, zaś z drugiej $(f)_\infty = div(\alpha' X + \beta' Y + \gamma' Z)$. Ale dywizor prostej to (z definicji dodawania) suma trzech punktów, sumujących się do zera. Stąd $T + T + T = \mathcal{O}$.

Zadania dodatkowe:

3.A Niech E_1/K, E_2/K – krzywe w postaci Weierstrassa, $\phi : E_1 \to E_2$ - niestała, rozdzielcza izogenia. Wtedy $\phi = [f(x), cyf'(x)]$ dla pewnego $f \in K(x)$, $c \in K^*$ ($f'(x)$ oznacza formalną pochodną f).

Rozwiązanie: Zauważmy, że $\phi = [x \circ \phi, y \circ \phi]$. Ponadto $\phi(-P) = -\phi(P)$, więc $(x \circ \phi)(-P) = x(-\phi(P)) = x(\phi(P))$. Stąd, ponieważ ciało funkcji parzystych to $K(x)$: $x \circ \phi = f(x)$ dla pewnego $f \in K(x)$. Analogicznie stwierdzamy, że $y \circ \phi$ jest funkcją nieparzystą, więc jest postaci $yg(x)$ dla pewnego $g \in K(x)$. Stąd $\phi = [f(x), yg(x)]$ Ponadto, że $\omega = dx/y$ jest niezmienniczą formą różniczkową, więc wg **[AEC, Corollary 5.6]** dla pewnego $a_\phi \in K^*$:

$$\frac{df(x)}{yg(x)} = \phi^*\left(\frac{dx}{y}\right) = a_\phi \frac{dx}{y} \qquad \Rightarrow \qquad g(x) = \frac{1}{a_\phi}\frac{df(x)}{dx} = \frac{1}{a_\phi} f'(x)$$

czyli $\phi = [f(x), \frac{1}{a_\phi} yf'(x)]$

Rozdział IV

4.0 (zadanie z tekstu) Niech R będzie dowolnym pierścieniem przemiennym. Pokaż, że R jest beztorsyjny (tzn. grupa $(R,+)$ jest beztorsyjna lub równoważnie jeżeli $nr = \underbrace{r+r+\ldots+r}_{n} = 0$, to $n=0$ lub $r=0$) wtedy i tylko wtedy, jeżeli homomorfizm $R \to R\otimes\mathbb{Q}$, $r \mapsto r\otimes 1$ jest iniekcją.

Rozwiązanie:

($\Rightarrow$) załóżmy, że $nr=0$, $n\in\mathbb{Z}$, $r\in R$, $n\neq 0$. Wtedy: $r\otimes 1 = n(r\otimes\frac{1}{n}) = nr\otimes\frac{1}{n} = 0\otimes\frac{1}{n} = 0 = 0\otimes 1$, więc z różnowartościowości tego odwzorowania $r=0$.

($\Leftarrow$) **Sposób I:**

pokażemy, że jeżeli pierścień R jest charakterystyki 0 oraz $r\otimes 1 = 0$, to r jest elementem torysjnym. Niech $S = \{n\cdot 1_R : n\in\mathbb{Z}\setminus\{0\}\}$ będzie zbiorem niezerowych "liczb całkowitych" w R – jest to wtedy zbiór multyplikatywny, więc możemy rozpartywać lokalizację względem niego: $S^{-1}R = R\times S/\sim$, gdzie $(r,n)\sim(r',n')$ wtedy i tylko wtedy, gdy istnieje $m\in S$ takie, że $rn'm = r'nm$. Wykażemy, że $R\otimes\mathbb{Q}\cong S^{-1}R$ (jako grupy abelowe). Istotnie, izomorfizmy dane są jako:

$$R\otimes\mathbb{Q}\to S^{-1}R, \qquad r\otimes\frac{a}{b}\mapsto[(ar,b)]_\sim$$

$$S^{-1}R\to R\otimes\mathbb{Q}, \qquad [(r,b)]_\sim\mapsto r\otimes\frac{1}{b}$$

Stąd, jeżeli $r\otimes 1=0$, to $[(r,1)]_\sim = [(0,1)]_\sim$, więc z definicji $\sim$ istnieje $m\in S$ takie, że $mr=0$.

($\Leftarrow$) **Sposób II:**

Skorzystamy z następującego lematu:

> **Lemat (na podstawie [Atiyah-Macdonald, Wpr. do algebry komutatywnej, Wniosek 2.13])** Jeżeli M,N są A-modułami oraz $\sum x_i\otimes y_i = 0$ w $M\otimes_A N$, to istnieją skończenie generowane podmoduły $M_0\subset M$, $N_0\subset N$ takie, że $\sum x_i\otimes y_i = 0$ w $M_0\otimes_A N_0$.
> **Dowód:** Z definicji $M\otimes N = A^{M\times N}/D$, gdzie D jest podmodułem generowanym przez elementy $(m_1+m_2,n)-(m_1,n)-(m_2,n)$ itd., więc $\sum x_i\otimes y_i = 0 \Rightarrow \sum x_i\otimes y_i$ jest sumą skończenie wielu elementów z D. Niech M_0 będzie generowane przez pierwsze współrzędne elementów występujących w tej sumie oraz $x_1,\ldots,x_n$; analogicznie definiujemy N_0. Jasne jest, że $\sum x_i\otimes y_i = 0$ w $M_0\otimes_A N_0$.

Załóżmy, że R jest beztorsyjny oraz $r\otimes 1 = 0$ w $R\otimes\mathbb{Q}$. Wtedy istnieje skończenie generowany podmoduł M $\mathbb{Z}$-modułu $\mathbb{Q}$ taki, że $r\otimes 1 = 0$ w $M\otimes\mathbb{Q}$. M jest skończenie generowany, więc $M\subset\frac{1}{n}\mathbb{Z}$ dla pewnego n. Rozważmy $f: R\times\frac{1}{n}\mathbb{Z}\to R$, $f(x,\frac{a}{n}) = ax$ – jest to odwzorowanie dwuliniowe, więc z uniwersalności iloczynu tensorowego: $f(x,\frac{a}{n}) = \widetilde{f}(x\otimes\frac{a}{n})$. Stąd: $0 = \widetilde{f}(r\otimes 1) = f(r\otimes\frac{n}{n}) = nr$ oraz $r=0$ z beztorsyjności R.

4.1 (b) Niech $\mathcal{F}(X) = F(X,0)\in R[\![X]\!]$ – wtedy $F(X,Y) = X+Y+\ldots$, więc $\mathcal{F}(X) = X+\ldots$. Zgodnie z **„lematem o odwrotnym szeregu potęgowym"** ([**AEC, Lemma IV.2.4, str. 122**]) istnieje więc $\mathcal{G}\in R[\![X]\!]$ spełniające $(\mathcal{G}\circ\mathcal{F})(X) = (\mathcal{F}\circ\mathcal{G})(X) = X$.
Ponadto, z łączności:

$$\mathcal{F}(X) = F(X,0) = F(X,F(0,0)) = F(F(X,0),0) = (\mathcal{F}\circ\mathcal{F})(X)$$

więc

$$\mathcal{F}(X) = ((\mathcal{G}\circ\mathcal{F})\circ\mathcal{F})(X) = (\mathcal{G}\circ\mathcal{F})(X) = X$$

Analogicznie $F(0,Y) = Y$.

(a) $*$ **istnienie** $i(X)$**:**

niech $f(Y) = F(X,Y) - X \in R[\![X]\!][\![Y]\!]$. Wtedy $f(Y) = Y+\ldots$, więc z **„lematu o odwrotnym szeregu potęgowym"** ([**AEC, Lemma IV.2.4, str. 122**]) istnieje $g\in[\![X]\!][\![Y]\!]$ takie, że

$(f \circ g)(Y) = (g \circ f)(Y) = Y$, czyli $F(X, g(Y)) = Y + X$. Podstawiając $Y := -X$ dostajemy $F(X, g(-X)) = 0$ i możemy przyjąć $i(X) = g(-X) \in R[\![X]\!]$.

∗ **jednoznaczność:**

załóżmy, że $F(X, i_2(X)) = 0$. Zauważmy, że $(g \circ f)(Y) = Y$, tzn. $g(F(X, Y) - X) = Y$. Podstawiając $Y := i_2(X)$, dostajemy:

$$i_2(X) = g(F(X, i_2(X)) - X) = g(-X) = i(X)$$

∗ $F(i(X), X) = 0$:

Zauważmy, że $g(0) = g(F(X, 0) - X) = 0$. Podstawiając $Y := F(i(X), X)$ w $g(F(X, Y) - X) = Y$ i korzystając z łączności oraz z $F(0, Y) = Y$:

$$F(i(X), X) = g(F(X, F(i(X), X)) - X) = g(F(F(X, i(X)), X) - X) = g(F(0, X) - X) = g(0) = 0$$

Rozdział V

5.4 (a) Niech $\phi : E_1 \to E_2$ będzie niezerową izogenią stopnia d zdefiniowaną nad $\mathbb{F}_q$. Niech $Frob_i = Frob_q^{E_i} : E_i \to E_i$ $(i = 1, 2)$ będą automorfizmami Frobeniusza na odpowiednich krzywych. Wtedy $E_i(\mathbb{F}_q) = q + 1 - tr(Frob_i)$, więc wystarczy wykazać, że $tr(Frob_1) = tr(Frob_2)$. Wybierzmy dowolną liczbę pierwszą $\ell \neq p$ i ustalmy bazy w $T_\ell(E_1)$, $T_\ell(E_2)$. Zauważmy, że $\rho_\ell(\phi) \in M_2(\mathbb{Q}_\ell)$ jest macierzą odwracalną (bo $\det \phi = \deg \phi \neq 0$). Ponadto ϕ jest zdefiniowane nad $\mathbb{F}_q$, więc $Frob_2 \circ \phi = \phi \circ Frob_1$, tzn. $\rho_\ell(Frob_2)\rho_\ell(\phi) = \rho_\ell(\phi)\rho_\ell(Frob_1)$, czyli $\rho_\ell(Frob_2) = \rho_\ell(\phi)\rho_\ell(Frob_1)\rho_\ell(\phi)^{-1}$. Wystarczy teraz zauważyć, że dla dowolnych macierzy $tr(ABA^{-1}) = tr(B)$, więc $tr(Frob_1) = tr(Frob_2)$.

(b) Załóżmy, że $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$, wtedy $tr(Frob_1) = tr(Frob_2)$ oraz $det(Frob_1) = det(Frob_2) = q$. Stąd macierze $\rho_\ell(Frob_1)$, $\rho_\ell(Frob_2) \in M_2(\mathbb{Q}_\ell)$ mają ten sam ślad i wyznacznik, więc mają te same wartości własne $\{\lambda_1, \lambda_2\} \subset \overline{\mathbb{Q}_\ell}$. Wykażemy, że $\rho_\ell(Frob_1) = B\rho_\ell(Frob_2)B^{-1}$ dla pewnej macierzy $B \in M_2(\mathbb{Z}_\ell) \cap Gl_2(\mathbb{Q}_\ell)$. Rozważmy dwa przypadki:

1^o $\lambda_1 \neq \lambda_2$. Wtedy macierze $\rho_\ell(Frob_1), \rho_\ell(Frob_2)$ są diagonalizowalne nad $\overline{\mathbb{Q}_\ell}$, tak więc są podobne nad $\overline{\mathbb{Q}_\ell}$ do macierzy $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ i muszą być podobne do siebie nad $\overline{\mathbb{Q}_\ell}$.

> **Lemat** Jeżeli K - ciało charakterystyki 0 $A, B \in M_n(K)$ są podobne nad $\overline{K}$, to są podobne nad K.
> **Dowód:** Rozważmy przestrzeń liniową $\{T \in\}$

Z **lematu** stwierdzamy, że $\rho_\ell(Frob_1), \rho_\ell(Frob_2) \in M_n(\mathbb{Q}_\ell)$ są podobne nad $\mathbb{Q}_\ell$, tzn. $\rho_\ell(Frob_1) = B\rho_\ell(Frob_2)B^{-1}$ dla $B \in Gl_2(\mathbb{Q}_\ell)$. Mnożąc przez mianowniki możemy założyć, że $B \in M_2(\mathbb{Z}_\ell) \cap Gl_2(\mathbb{Q}_\ell)$.

2^o $\lambda_1 = \lambda_2$. Oznacza to, że wielomian charakterystyczny $x^2 - tr(Frob_i)x + q$ ma dwa równe pierwiastki i $\Delta = tr(Frob_i)^2 - 4q = 0$, a więc zachodzi równość w nierówności Hassego. Z dowodu nierówności wynika, że istnieją całkowite $(n_i, m_i) \neq (0, 0)$ takie, że $[n_i] = [m_i] \circ Frob_i$ dla $i = 1, 2$. Porównując stopnie: $n_i^2 = m_i^2 \cdot q$, więc $m_i | n_i$. Stąd $[m_i] \circ [n_i/m_i] = [m_i] \circ Frob_i$, więc (jako że $Hom(E_i)$ to dziedzina całkowitości) $[n_i/m_i] = Frob_i$. Porównując stopnie i ślady obu stron stwierdzamy, że q jest kwadratem i $Frob_1 = Frob_2 = [n_i/m_i] = [\pm\sqrt{q}]$. Stąd $\rho_\ell(Frob_1) = \rho_\ell(Frob_2)$.

5.5 Zauważmy, że dowolny ordynek ciała kwadratowego urojonego $K = \mathbb{Q}(\sqrt{D})$ jest postaci $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$, gdzie $f \in \mathbb{Z}_+$ - tzw. przewodnik ordynka, $\mathcal{O}_K$ - pierścień liczb całkowitych w K (patrz **zadanie 3.20**).

Wykażemy najpierw, że jeżeli $\ell \in \mathbb{Z}$, $\ell\mathcal{O}_K$ jest pierwszym ideałem w $\mathcal{O}_K$, oraz $\ell \nmid f$, to $\ell\mathcal{O}$ jest pierwszym ideałem $\mathcal{O}$. Istotnie, wtedy możemy wybrać $\alpha, \beta \in \mathbb{Z}$ spełniające $f\alpha + \ell\beta = 1$.

Jeżeli więc $xy \in \ell\mathcal{O}$, $x, y \in \mathcal{O}$, to ponieważ $\ell\mathcal{O} \subset \ell\mathcal{O}_K$, zaś $\ell\mathcal{O}_K$ jest ideałem pierwszym, mamy $x \in \ell\mathcal{O}_K$ lub $y \in \ell\mathcal{O}_K$; bez straty ogólności $x = \ell z$ dla $z \in \mathcal{O}_K$. Stąd jednak:

$$x = f\alpha x + \beta\ell x = \underbrace{\ell\,(\alpha \underbrace{fz}_{\in f\mathcal{O}_K} + \beta x)}_{\in \mathcal{O}} \in \ell\mathcal{O}$$

co dowodzi pierwszości ideału.

Niech $f_1, \ldots, f_n$ będą przewodnikami ordynków $\mathcal{R}_1, \ldots, \mathcal{R}_n$. Wybierzmy dowolną liczbę pierwszą $\ell \in \mathbb{Z}$ taką, że $\ell \nmid f_1 \ldots f_n$ oraz $(\frac{K/\mathbb{Q}}{\ell}) = \tau \in Gal(K/\mathbb{Q})$ (symbol Artina równy sprzężeniu zespolonemu) – na mocy tw. Czebotariewa takich liczb jest nieskończenie wiele (gęstość Dirichleta = 1/2). Wtedy stopień ideałów $\mathcal{O}_K$ leżących nad $\ell\mathcal{O}_K$ jest równy rzędowi $(\frac{K/\mathbb{Q}}{\ell})$ i wynosi 2. Z twierdzenia efg stwierdzamy więc, że ideał $\ell\mathcal{O}_K$ jest pierwszy. Z tego, co udowodniliśmy, wynika więc, że $\ell\mathcal{R}_i$ są ideałami pierwszymi $\mathcal{R}_i$ dla $i = 1, \ldots, n$.

5.6 (a) $E(\mathbb{F}_q)$ jest skończoną grupą abelową, więc ma rozkład na czynniki niezmiennicze: $E(\mathbb{F}_q) \cong \mathbb{Z}/k_1\mathbb{Z} \times \mathbb{Z}/k_1k_2\mathbb{Z} \times \ldots \times \mathbb{Z}/k_1k_2 \ldots k_l\mathbb{Z}$ dla $k_1, \ldots k_l \in \mathbb{Z}_+ \setminus \{1\}$. Ale $\mathbb{Z}/k_1\mathbb{Z} \times \mathbb{Z}/k_1k_2\mathbb{Z} \times \ldots \times \mathbb{Z}/k_1k_2 \ldots k_l\mathbb{Z}$ ma k_1^l elementów rzędu k_1, zaś $E(\mathbb{F}_q) \subset E$ maksymalnie k_1^2, więc $l \in \{1, 2\}$. W obydwu przypadkach grupa jest wymaganej postaci (dla $l = 2$ jest $(m, n) = (k_1, k_2)$, zaś dla $l = 1$ jest $(m, n) = (1, k_1)$).

Ponadto, jeżeli byłoby $char\,\mathbb{F}_q = p|m$, to $E(\mathbb{F}_q)$ zawierałoby min. p^2 elementów rzędu dzielącego p – jest to niemożliwe, bo $E[p] \cong 0$ lub $\mathbb{Z}/p\mathbb{Z}$.

(b) mamy: $E[m] \subset E(\mathbb{F}_q)$, więc $\mu_m \subset \mathbb{F}_q$. Ponadto $NWD(m,p) = 1$, więc μ_m zawiera pierwiastek pierwotny ζ_m rzędu m. Mamy: $\zeta_m \in \mathbb{F}_q$, więc $\zeta_m^{q-1} = 1$, co daje $m|q-1$.

(c) jeżeli E – supersingularna, to $p+1 = m^2 n$, więc $m|p+1$. Ale $m|p-1$, więc $m|(p+1)-(p-1) = 2$ oraz $m \in \{1,2\}$. Jeżeli ponadto $p \equiv 1 \pmod 4$, to $4 \nmid p+1$, więc $m = 1$.

5.8 Oznaczmy: $Hom^0(E_1,E_2) = Hom(E_1,E_2) \otimes \mathbb{Q}$, $End^0(E) = Hom^0(E,E)$ i niech $E_\gamma : y^2 = x\cdot(x-1)\cdot(x-\gamma)$ oznacza dla $\gamma \in \overline{K} \setminus \{0,1\}$ krzywą w postaci Legendre'a. Skorzystamy z następujących faktów:

(1) istnieje naturalnie określone mnożenie między elementami $Hom^0(E_2,E_3)$ oraz $Hom^0(E_1,E_2)$. Każdy element $\phi \in Hom(E_1,E_2)$ ma odwrotność multyplikatywną $\phi^{-1} \in Hom^0(E_2,E_1)$,

uzasadnienie: mnożenie tensorów prostych określamy jako: $(\phi_1 \otimes q_1)\cdot(\phi_2 \otimes q_2) := (\phi_1 \circ \phi_2) \otimes (q_1 q_2)$ i przedłużamy mnożenie liniowo na wszystkie tensory.
Ponadto elementem odwrotnym do $\phi \in Hom(E_1,E_2)$ jest $\phi^{-1} := \frac{1}{deg\,\phi}\widehat{\phi} \in Hom^0(E_2,E_1)$ (tzn. $\widehat{\phi} \otimes \frac{1}{deg\,\phi}$)

(2) jeżeli krzywe E_1, E_2 są izogeniczne, to $End^0(E_1) \cong End^0(E_2)$ (jako $\mathbb{Q}$-algebry). Izomorfizm dany jest wzorem $End^0(E_1) \ni x \mapsto p^{-1}\cdot x \cdot p \in End^0(E_2)$, gdzie $p \in Hom(E_2,E_1)$ – dowolna izogenia, zaś $p^{-1} \in Hom^0(E_1,E_2)$ jest odwrotnością multyplikatywną, określoną jak wyżej,

(3) jeżeli E_1/K, E_2/K są izogenicznymi krzywymi eliptycznymi, ciało K zawiera domknięte algebraicznie podciało L oraz $j(E_1) \in L$, to $j(E_2) \in L$ (równoważnie: jeżeli jedną z nich można określić nad L, to druga jest izomorficzna nad $\overline{K}$ z pewną krzywą zdefiniowaną nad L),

uzasadnienie: niech $\phi : E_1 \to E_2$ będzie izogenią. Wtedy z I tw. o izomorfizmie dla krzywych eliptycznych (wynikającego z **[AEC, III, Proposition 4.12, str. 74]** oraz **[AEC, Corollary 4.11, str. 73]**) wynika, że $\phi = u \circ \pi$, gdzie $\pi : E_1 \to E_1/\ker\alpha$, $u : E_1/\ker\alpha \to E_2$ - izomorfizm. Ale z konstrukcji wynika, że $E_1/\ker\alpha$ jest określone nad najmniejszym domkniętym algebraicznie ciałem zawierającym współczynniki E_1, więc E_2 jest izomorficzne z $E_1/\ker\alpha$ określonym nad L,

(4) jeżeli dane są ciała $L = \overline{L} \subset K$ oraz $\alpha, \beta \in K \setminus \overline{L}$, to istnieje $\sigma \in Gal(K/L)$ takie, że $\sigma(\alpha) = \beta$.

Niech E/K, $j(E) \notin \overline{\mathbb{F}_p}$. Bez straty ogólności przyjmijmy, że $E = E_\lambda$. Wtedy $j(E_\lambda) \notin \overline{\mathbb{F}_p}$, więc $\lambda \notin \overline{\mathbb{F}_p}$. Załóżmy nie wprost, że $End(E)$ jest ordynkiem w urojonym ciele kwadratowym. Niech $N < 0$ będzie takie, że $End^0(E) \cong \mathbb{Q}(N)$ oraz $\sqrt{N} \in End(E)$.

Zauważmy, że wtedy dla dowolnej krzywej E'/K spełniającej $j(E) \notin \overline{\mathbb{F}_p}$ zachodzi $End(E') \cong End(E)$. Istotnie, jeżeli $E' \cong E_\mu$ (nad $\overline{K}$), to $\mu \notin \overline{\mathbb{F}_p}$, więc istnieje $\sigma \in Gal(K/\mathbb{F}_p)$???? takie, że $\sigma(\mu) = \lambda$ oraz $(E')^\sigma = E$, co oznacza, że $End(E') \cong End(E)$ (izomorfizm to $f(P) \mapsto f^\sigma(P)$). Stąd dla każdego takiego E' równanie $x^2 = N$ ma dokładnie 2 rozwiązania w $End^0(E')$, które oznaczymy jako $\alpha_{E'}, -\alpha_{E'} \in End(E')$.

Wybierzmy dowolną liczbę pierwszą $\ell \nmid pN$ i dowolne $\xi = (\xi_1, \xi_2, \ldots) \in T_\ell(E)$. Niech $\Phi_k = \langle \xi_k \rangle \cong \mathbb{Z}/\ell^k\mathbb{Z}$ będzie podgrupą generowaną przez ξ_k. Niech $E_k = E/\Phi_k$ i niech $\pi_k : E \to E_k$ będzie izogenią ilorazową. Wtedy E_k oraz E są izogeniczne, więc z **(3)** dostajemy $j(E_k) \notin \overline{\mathbb{F}_p}$ i $End(E_k) \cong End(E)$. Niech $\alpha := \alpha_E$, $\alpha_k := \alpha_{E_k}$.

Pokażemy, że ξ jest wektorem własnym α. Zgodnie z **(2)** funkcja $f_k(x) = p_k \cdot x \cdot p_k^{-1} : End^0(E) \to End^0(E_k)$ jest izomorfizmem (ciał). Wiemy jednak, że $f_k(\alpha)^2 = f_k(\alpha^2) = N$, więc $f_k(\alpha) = \pm\alpha_k$, tzn. $\pi_k \circ \alpha = \pm\alpha_k \circ \pi_k$. W szczególności (jako że α_k jest endomorfizmem) $\alpha(\ker(\pi_k)) \subset \ker(\pi_k)$, czyli $\alpha(\Phi_k) \subset \Phi_k$. Ponieważ zachodzi to dla każdego k, to ξ jest wartością własną α.

Każdy wektor $\xi \in T_\ell(E)$ jest wektorem własnym α, więc $\rho_\ell(\alpha) \in M_2(\mathbb{Z}_\ell)$ jest macierzą skalarną aI_2 ($a \in \mathbb{Z}_\ell$). Ale $End(E) \otimes \mathbb{Z}_\ell \to End(T_\ell(E))$ jest zanurzeniem, więc $a \in \mathbb{Z}$ oraz $\alpha = [a] \in \mathbb{Z}$, wbrew założeniu – sprzeczność kończy dowód.

5.9 Zauważmy, że dla $p \neq 2,3$:

$$\#Aut(E) = \begin{cases} 4 & j(E) = 1728 \\ 6 & j(E) = 0 \\ 2 & j(E) \neq 0, 1728 \end{cases}$$

([**AEC, III.10**]). Przyjmijmy $\epsilon_p(\alpha) = 1$, jeżeli krzywa o j-niezmienniku α jest supersingularna oraz $= 0$ w przeciwnym wypadku. Korzystając ze wzoru:

$$\text{ilość krzywych supersingularnych} \quad = \quad \frac{p-1}{12} + \frac{2}{3}\epsilon_p(0) + \frac{1}{2}\epsilon_p(1728)$$

dostajemy:

$$\begin{aligned} \sum_{E/\mathbb{F}_p - ss} \frac{1}{\#Aut(E)} &= \sum_{E/\mathbb{F}_p - ss, j(E) \neq 0, 1728} \frac{1}{4} + \frac{\epsilon_p(0)}{6} + \frac{\epsilon_p(1728)}{4} = \\ &= \left(\frac{p-1}{12} - \frac{1}{3}\epsilon_p(0) - \frac{1}{2}\epsilon_p(1728)\right) \cdot \frac{1}{2} + \frac{\epsilon_p(0)}{6} + \frac{\epsilon_p(1728)}{4} = \frac{p-1}{24} \end{aligned}$$

5.10 Oznaczmy $t = tr(Frob_q)$.

(a) ($\Rightarrow$) Załóżmy, że $E/\mathbb{F}_q$ jest supersingularna, wtedy $E^{(q)} = E$ oraz $\widehat{Frob_q} : E \to E$ jest czysto nierozdzielcze i ma stopień q, więc $\widehat{Frob_q} = \Psi \circ Frob_q$ gdzie Ψ jest rozdzielczym automorfizmem oraz $[q] = \widehat{Frob_q} \circ Frob_q = \Psi \circ Frob_q^2$.

Rozważmy dowolną liczbę pierwszą $\ell \neq p$ i niech $\rho_\ell(Frob_q) \in M_2(\mathbb{Q}_\ell)$ będzie macierzą $Frob_q$, zaś $\rho_\ell(\Psi) \in M_2(\mathbb{Q}_\ell)$, $\det(\rho_\ell(\Psi)) = deg(\Psi) = 1$. Wtedy z jednej strony $[q] = \Psi \circ Frob_q^2$, więc $\rho_\ell(Frob_q)^2 = q\rho_\ell(\Psi)^{-1}$. Z drugiej strony z twierdzenia Cayleya-Hamiltona:

$$\begin{aligned} \rho_\ell(Frob_q)^2 &= tr(\rho_\ell(Frob_q))\rho_\ell(Frob_q) - \det(\rho_\ell(Frob_q))I_2 = \\ &= tr(Frob_q)\rho_\ell(Frob_q) - deg(Frob_q)I_2 = t\rho_\ell(Frob_q) - qI_2 \end{aligned}$$

Stąd $t\rho_\ell(Frob_q) - qI_2 = q\rho_\ell(\Psi)^{-1}$, czyli $t\rho_\ell(Frob_q) = (qI_2 + q\rho_\ell(\Psi)^{-1})$ i obliczając wyznaczniki obydwu stron:

$$t^2 q = q^2 \cdot \det(qI_2 + q\rho_\ell(\Psi)^{-1})$$

co daje $q^2 | t^2 q$, czyli $q | t^2$ i $p | t$.

($\Leftarrow$) Załóżmy, że $p|t$. Wtedy, biorąc dowolne $\ell \neq p$ i korzystając z twierdzenia Cayleya-Hamiltona: $\rho_\ell(Frob_q)^2 = t\rho_\ell(Frob_q) - qI_2$, tzn. $(\rho_\ell(Frob_q)^2)_\ell = (t\rho_\ell(Frob_q) - qI_2)_\ell$. Ale odwzorowanie $Hom(E) \otimes \mathbb{Z}_\ell \to Hom(T_\ell(E))$ jest iniekcją, więc $(Frob_q)^2 = [t] \circ Frob_q - [q]$. Stąd, jeżeli $P \in E[p]$, to:

$$(Frob_q)^2(P) = Frob_q \circ [t/p]([p]P) - [q/p]([p]P) = 0$$

Ale $Frob_q$ jest różnowartościowy, więc $P = O$ i $E[p] = \{O\}$, czyli E jest supersingularna.

(b) Mamy: $tr(Frob_p) = p + 1 - \#E(\mathbb{F}_p)$, więc jeżeli $\#E(\mathbb{F}_p) = p + 1$, to $p | tr(Frob_p) = 0$. Na odwrót, jeżeli $p | tr(Frob_p) = p + 1 - \#E(\mathbb{F}_p)$, to ponieważ dla $p \geqslant 5$ korzystając z nierówności Hassego:

$$0 \leqslant |p + 1 - \#E(\mathbb{F}_p)| < 2\sqrt{p} < p$$

więc $|p + 1 - \#E(\mathbb{F}_p)| = 0$

5.11 Wybierzmy dowolną liczbę pierwszą $\ell \neq 2, 3$. Niech $p \neq 2, 3$ będzie dowolną liczbą pierwszą taką, że:

- p nie dzieli wyróżnika krzywej E,
- p rozkłada się całkowicie w $\mathbb{Q}(E[\ell])$ na ideały pierwsze $\beta_1, \ldots, \beta_g$ ($g = [\mathbb{Q}(E[\ell]) : \mathbb{Q}]$), bądź też równoważnie symbol Artina p jest trywialny: $(\frac{\mathbb{Q}(E[\ell])/\mathbb{Q}}{p}) = id$,

– żaden z ideałów $\beta_1, \ldots, \beta_g$ nie dzieli mianowników współrzędnych afinicznych punktów w $E[\ell]$.

Z twierdzenia Czebotariewa istnieje nieskończenie wiele takich liczb pierwszych (ich gęstość Dirichleta to $\frac{1}{[\mathbb{Q}(E[\ell]):\mathbb{Q}]}$).

Niech $\mathcal{O}$ będzie pierścieniem liczb całkowitych w $\mathbb{Q}(E[\ell])$ – wtedy $\mathcal{O}/\beta_j \cong \mathbb{F}_p$. Niech $\widetilde{E}$ oznacza redukcję krzywej E do $\mathcal{O}/\beta_i \cong \mathbb{F}_p$. Z założenia redukcja $\pmod{\beta_j} : E[\ell] \to \widetilde{E}(\mathcal{O}/\beta_j)$ jest iniekcją, więc $\widetilde{E}[\ell] = E[\ell]\, mod\, \beta_j \subset \widetilde{E}(\mathbb{F}_p)$ i dla $Q \in \widetilde{E}[\ell]$ jest $Frob_p(Q) = Q$.

Stąd macierz działania $Frob_p$ na $\widetilde{E}[\ell]$ przystaje $\pmod{\ell}$ do I_2 oraz $tr\, Frob_p \equiv tr\, I_2 \equiv 2 \pmod{\ell}$, więc $\#E(\mathbb{F}_p) = p + 1 - tr\, Frob_p \equiv p + 1 - 2 \equiv p - 1 \pmod{\ell}$.

Załóżmy nie wprost, że $\widetilde{E}$ jest supersingularna – wtedy $|\widetilde{E}(\mathbb{F}_p)| = p + 1$, więc byłoby: $p - 1 \equiv p + 1 \pmod{\ell}$, czyli $\ell | 2$ co daje sprzeczność.

5.14 Ustalmy $\mathbb{Z}/m\mathbb{Z}$-bazę w $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Niech $v \in (\mathbb{Z}/m\mathbb{Z})^2$ będzie wektorem współrzędnych punktu P w tej bazie, zaś $F = \rho_{2,m}(Frob_q), \widehat{F} = \rho_{2,m}(\widehat{Frob_q}) \in M_2(\mathbb{Z}/m\mathbb{Z})$ będą macierzami odpowiednich przekształceń w tej bazie. Wtedy (ponieważ P ma rząd m) $k \cdot v = 0 \Leftrightarrow m|k$

Niech też $p(x) = \det(xI - F) \in \mathbb{Z}/m\mathbb{Z}[x]$ będzie wielomianem charakterystycznym macierzy F.

Fakt 1 Jeżeli $NWD(m, q-1) = 1$, $f \in \mathbb{Z}/m\mathbb{Z}[x]$ oraz $f(1) = f(q) = 0$, to $(x-1)(x-m)|f(x)$.
Dowód: Zgodnie z algorytmem Euklidesa (ponieważ współczynnik przy najwyższej potędze w $(x-1)(x-m)$ jest odwracalny) możemy zapisać $f(x) = q(x) \cdot (x-1)(x-m) + ax + b$, gdzie $q \in \mathbb{Z}/m\mathbb{Z}[x]$, $a, b \in \mathbb{Z}/m\mathbb{Z}$. Ponadto $0 = f(1) = a + b$, $0 = f(q) = aq + b$, więc $0 = a(1-q)$, czyli (ponieważ $1 - q \in U(\mathbb{Z}/m\mathbb{Z})$) $a = 0$, $b = 0$ oraz $f(x) = q(x) \cdot (x-1)(x-m)$.

Fakt 2 Jeżeli $A \in M_n(\mathbb{Z}/m\mathbb{Z})$, $v \in (\mathbb{Z}/m\mathbb{Z})^n$ jest wektorem rzędu addytywnego m (tzn. $kv = 0 \Leftrightarrow k \equiv 0 \pmod{m}$) oraz $Av = 0$, to $\det A = 0$.
Dowód: Niech $A^\wedge$ będzie macierzą dołączoną macierzy A, wtedy $A^\wedge A = AA^\wedge = \det A \cdot I$. Stąd: $0 = A^\wedge Av = \det A \cdot v$, więc $m | \det A$.

Zauważmy, że $P \in E(\mathbb{F}_q)$, więc $Frob_q(P) = P$ oraz $Fv = v$, co daje $(I-F)v = 0$ i z faktu 2: $p(1) = \det(I-F) = 0$. Ponadto $\widehat{Frob_q}(P) = \widehat{Frob_q}(Frob_q(P)) = [q]P$, więc $(qI - \widehat{F})v = 0$ oraz $p(q) = \det(qI - F) = \det(\widehat{qI - F}) = \det(qI - F) = 0$.

Na mocy **Faktu 1** oznacza to, że $(x-1)(x-q)|p(x)$, więc $p(x) = (x-1)(x-q)$. Rozpatrzmy wielomian $g(x) = x^d - 1$ – wtedy $g(1) = g(q) = 0$, więc $p(x) = (x-1)(x-q)|g(x)$. Ale na mocy twierdzenia Cayleya-Hamiltona $p(F) = 0$, więc $F^d - I = g(F) = 0$ oraz $F^d = I$. Oznacza to, że $Frob_{q^d}|_{E[m]} = id$, więc $E[m] \subset E(\mathbb{F}_{q^d})$.

Zadania dodatkowe:

5.A Wykazać, że krzywa eliptyczna E/K ($char\, K = p$) jest supersingularna wtw. gdy istnieje nieskończenie wiele izogenicznych z nią krzywych (z dokładnością do $\overline{K}$-izomorfizmu).

Rozwiązanie:
($\Rightarrow$) Załóżmy, że krzywa E jest supersingularna. Wtedy z dowodu **[AEC, V.3, Theorem 3.1,** $(iii) \Rightarrow (iv)$**]** wynika, że dowolna krzywa E' izogeniczna z E jest również supersingularna oraz $j(E') \in \mathbb{F}_{p^2}$, w szczególności takich krzywych jest mniej niż p^2.

($\Leftarrow$) Niech $End(E)$ będzie izomorficzne z ordynkiem $\mathcal{O}$ w $\mathbb{Q}(\sqrt{n})$, $n \leqslant 0$ (przy czym dla $End(E) \cong \mathbb{Z}$ przyjmujemy $n = 0$). Niech $\mathcal{L} = \{\ell \in \mathbb{P} : \ell \nmid 2np, \ell\mathcal{O}$ jest ideałem pierwszym w $\mathcal{O}\}$ – z twierdzenia Czebotariewa i zadania 5.5 jest to zbiór nieskończony (dla $End(E) = \mathbb{Z}$ zbiór $\mathcal{L}$ składa się z liczb pierwszych nie dzielących $2np$). Niech H_ℓ będzie dowolną podgrupą cykliczną rzędu ℓ w E. Pokażemy, że krzywe „ilorazowe" $\{E/H_\ell : \ell \in \mathcal{L}\}$ są

parami różne.

Niech $\ell_1, \ell_2 \in \mathcal{L}$, $\ell_1 \neq \ell_2$. Zauważmy najpierw, że dla dowolnego $\varphi \in End(E)$ jest: $\deg \varphi \neq \ell_1\ell_2$ - istotnie, jeżeli $\varphi = a + b\sqrt{n}$ $(a, b \in \mathbb{Z})$ w $\mathcal{O}$, to $\widehat{\varphi} = \overline{a + b\sqrt{n}}$, więc $\deg \varphi = (a + b\sqrt{n})\overline{(a + b\sqrt{n})} = a^2 - nb^2$ i jeżeli $\ell_1\ell_2 = a^2 - nb^2 = (a + b\sqrt{n})(a - b\sqrt{n})$, to (ponieważ $\ell_1\mathcal{O}$ jest ideałem pierwszym w $\mathcal{O}$) $\ell_1|(a + b\sqrt{n})$ lub $\ell_1|(a - b\sqrt{n})$. Załóżmy, że $\ell_1|(a + b\sqrt{n})$ – wtedy również $\ell_1|\overline{(a + b\sqrt{n})}$ oraz $\ell_1|2a = (a + b\sqrt{n}) + \overline{(a + b\sqrt{n})}$, czyli $\ell_1|a$ oraz $\ell_1|b$, więc $\ell_1^2|a^2 - nb^2 = \ell_1\ell_2$ i $\ell_1|\ell_2$, wbrew założeniu $\ell_1 \neq \ell_2$.

Załóżmy nie wprost, że krzywe E/H_{ℓ_1} oraz E/H_{ℓ_2} są izomorficzne oraz $\Psi : E/H_{\ell_1} \to E/H_{\ell_2}$ jest izomorfizmem. Niech $\pi_j : E \to E/H_{\ell_j}$ będzie odwzorowaniem ilorazowym dla $j = 1, 2$ (oczywiście $\deg \pi_j = \# \ker \pi_j = \#H_{\ell_j} = \ell_j$). Wtedy $\widehat{\pi_2} \circ \Psi \circ \pi_1 : E \to E$ byłoby odwzorowaniem stopnia $\ell_1\ell_2$ wbrew temu, co udowodniliśmy. To oznacza, że E jest izogeniczna z nieskończenie wieloma krzywymi – wszystkimi ze zbioru $\{E/H_\ell : \ell \in \mathcal{L}\}$.

Rozdział VI

6.1 Po zróżniczkowaniu równości: $\theta'(z+\omega_i) = a_i\theta'(z)$ $(i=1,2)$, więc funkcja $g(z) = \frac{\theta'(z)}{\theta(z)}$ spełnia $g(z+\omega_i) = g(z)$ i jest funkcją eliptyczną. Stąd $0 = \sum_{w\in\mathbb{C}/\Lambda} res_w(g)$ ([**AEC, VI, Theorem 2.2**]), a ponadto z twierdzenia Rouche'go: $res_w(\theta'/\theta) = ord_w(\theta) \geqslant 0$ (bo θ jest holomorficzna). Łącząc to: $0 \leqslant \sum_{w\in\mathbb{C}/\Lambda} ord_w(\theta) = 0$, więc $\forall_{w\in\mathbb{C}/\Lambda} \quad ord_w(\theta) = 0$, czyli $\theta(z)$ nie ma zer i funkcja $g(z) = \theta'(z)/\theta(z)$ jest całkowitą funkcją eliptyczną – musi być zatem stała: $g(z) = c$. Rozwiązując równanie różniczkowe:

$$\int_0^z \theta'(w)/\theta(w)\,dw = \int_0^z c\,dw \qquad \Rightarrow \qquad \int_{\theta 0}^{\theta(z)} du/u = cz$$
$$\Rightarrow \qquad \log\theta(z) = \log\theta(0) + cz \quad \Rightarrow \quad \theta(z) = \theta(0)\exp(cz)$$

6.A Wykazać, że jeżeli $z_0,\ldots,z_n \in \mathbb{C}\setminus\Lambda$, to:

$$\begin{vmatrix} 1 & \wp(z_0) & \wp'(z_0) & \wp''(z_0) & \ldots & \wp^{(n-1)}(z_0) \\ 1 & \wp(z_1) & \wp'(z_1) & \wp''(z_1) & \ldots & \wp^{(n-1)}(z_1) \\ \ldots & & & & & \\ 1 & \wp(z_n) & \wp'(z_n) & \wp''(z_n) & \ldots & \wp^{(n-1)}(z_n) \end{vmatrix} = (-1)^{n(n-1)/2} 1!2!\ldots n! \frac{\sigma(z_0+\ldots+z_n)\prod_{0\leqslant i<j\leqslant n}\sigma(z_i-z_j)}{\prod_{0\leqslant i\leqslant n}\sigma(z_i)^{n+1}}$$

Rozwiązanie: Wykażemy to indukcyjnie wg n. Załóżmy, że teza zachodzi dla $n-1$ i ustalmy liczby $z_0,\ldots,z_{n-1} \in \mathbb{C}\setminus\Lambda$. Bez straty ogólności załóżmy, że są one różne (w przeciwnym wypadku obie strony się zerują). Rozważmy funkcje:

$$f(z) = \begin{vmatrix} 1 & \wp(z_0) & \wp'(z_0) & \wp''(z_0) & \ldots & \wp^{(n-1)}(z_0) \\ 1 & \wp(z_1) & \wp'(z_1) & \wp''(z_1) & \ldots & \wp^{(n-1)}(z_1) \\ \ldots & & & & & \\ 1 & \wp(z) & \wp'(z) & \wp''(z) & \ldots & \wp^{(n-1)}(z) \end{vmatrix}$$

$$g(z) = \frac{\sigma(z_0+\ldots+z)\prod_{0\leqslant i\leqslant n-1}\sigma(z_i-z)}{\sigma(z)^{n+1}}$$

Zauważmy najpierw, że funkcja g jest eliptyczna – istotnie, jeżeli $\omega\in\Lambda$, $\sigma(z+\omega) = e^{az+b}\sigma(z)$, to:

$$g(z+\omega) = ...$$

Zauważmy, że $\wp^{(k)}(z) = \frac{(-1)^k(k+1)!}{z^{k+2}} +$ (funkcja holomorficzna), więc z założenia indukcyjnego:

$$\lim_{z\to 0} z^{n+1}f(z) = \lim_{z\to 0}\begin{vmatrix} 1 & \wp(z_0) & \wp'(z_0) & \wp''(z_0) & \ldots & \wp^{(n-1)}(z_0) \\ 1 & \wp(z_1) & \wp'(z_1) & \wp''(z_1) & \ldots & \wp^{(n-1)}(z_1) \\ \ldots & & & & & \\ z^{n+1} & z^{n+1}\wp(z) & z^{n+1}\wp'(z) & z^{n+1}\wp''(z) & \ldots & z^{n+1}\wp^{(n-1)}(z) \end{vmatrix} =$$

$$= \begin{vmatrix} 1 & \wp(z_0) & \wp'(z_0) & \wp''(z_0) & \ldots & \wp^{(n-1)}(z_0) \\ 1 & \wp(z_1) & \wp'(z_1) & \wp''(z_1) & \ldots & \wp^{(n-1)}(z_1) \\ \ldots & & & & & \\ 0 & 0 & 0 & 0 & \ldots & (-1)^{n-1}n! \end{vmatrix} =$$

$$= (-1)^{n-1}n!\begin{vmatrix} 1 & \wp(z_0) & \wp'(z_0) & \wp''(z_0) & \ldots & \wp^{(n-2)}(z_0) \\ 1 & \wp(z_1) & \wp'(z_1) & \wp''(z_1) & \ldots & \wp^{(n-2)}(z_1) \\ \ldots & & & & & \\ 1 & \wp(z_{n-1}) & \wp'(z_{n-1}) & \wp''(z_{n-1}) & \ldots & \wp^{(n-2)}(z_{n-1}) \end{vmatrix} =$$

$$= (-1)^{n-1}n!\cdot\left((-1)^{n(n-1)/2}1!2!\ldots(n-1)!\frac{\sigma(z_0+\ldots+z_{n-1})\prod_{0\leqslant i<j\leqslant n-1}\sigma(z_i-z_j)}{\prod_{0\leqslant i\leqslant n-1}\sigma(z_i)^n}\right) \qquad (*)$$

co oznacza, że f ma $n+1$-krotny biegun w 0 i współczynnik przy z^{-n-1} w $f(z)$ dany jest wzorem $(*)$. Jest to jej jedyny biegun w $\mathbb{C}/\Lambda$, więc f jest funkcją elityczną rzędu $n+1$. Z własności wyznacznika $f(z_0) = \ldots =$

$f(z_{n-1}) = 0$, więc (ponieważ f musi mieć tyle zer co biegunów) f ma jeszcze jedno zero p. Ale $0 = sum(div(f)) = p + \sum_{i=0}^{n-1} z_i - n \cdot 0$, więc $p = -z_0 - \ldots - z_{n-1}$ oraz $div(f) = (p) + \sum_{i=0}^{n-1}(z_i) - n \cdot (0) = div(g)$.

Stąd $f(z) = cg(z)$ dla pewnego $c \in \mathbb{C}$. Mamy:

$$\lim_{z\to 0} z^{n+1} cg(z) = c\sigma(z_0 + \ldots + z_{n-1} + 0) \lim_{z\to 0} \left(\frac{z}{\sigma(z)}\right)^{n+1} = c\sigma(z_0 + \ldots + z_{n-1})$$

więc $c = \ldots$.

6.3 (a) Zauważmy najpierw, że prawa strona jest funkcją eliptyczną zmiennej z – jeżeli $\omega \in \Lambda$, to dla pewnych $c, d \in \mathbb{C}$ ([**AEC, VI, Lemma 3.3 (c)**]) $\sigma(z+\omega) = e^{cz+d}\sigma(z)$, więc:

$$-\frac{\sigma(z+a+\omega)\sigma(z-a+\omega)}{\sigma(z+\omega)^2\sigma(a)^2} = -\frac{\left(e^{c(z-a)+d}\sigma(z+a)\right)\left(e^{c(z+a)+d}\sigma(z-a)\right)}{(e^{cz+d}\sigma(z))^2\sigma(a)^2} = -\frac{\sigma(z+a)\sigma(z-a)}{\sigma(z)^2\sigma(a)^2}$$

Dla ustalonego $a \not\equiv 0 \pmod{\Lambda}$ funkcja $z \mapsto \wp(z) - \wp(a)$ ma podwójny biegun w 0, więc jest stopnia dwa. Stąd nie ma ona innych zer oprócz $\pm a$ ($\wp(z)$ jest funkcją parzystą) oraz $div(\wp(z)-\wp(a)) = (a)+(-a)-2(0)$.

Funkcja $\sigma(z)$ ma pojedyncze zera tylko w punktach kraty Λ, więc $div\left(-\frac{\sigma(z+a)\sigma(z-a)}{\sigma(z)^2\sigma(a)^2}\right) = (a)+(-a)-2(0) = div(\wp(z)-\wp(a))$ czyli $\wp(z)-\wp(a) = C\left(-\frac{\sigma(z+a)\sigma(z-a)}{\sigma(z)^2\sigma(a)^2}\right)$ dla pewnej stałej C (zależnej tylko od a). Stałą tą wyliczymy, porównując współczynniki przy z^{-2} w rozwinięciu w szereg Laurenta – po lewej stronie jest to 1 ([**AEC, VI, Theorem 3.5**]), zaś po prawej jest to:

$$\begin{aligned}\lim_{z\to 0}\left(z^2\left(-C\frac{\sigma(z+a)\cdot\sigma(z-a)}{\sigma(z)^2\sigma(a)^2}\right)\right) &= C\frac{\sigma(a+0)\sigma(a-0)}{\sigma(a)^2}\lim_{z\to 0}\frac{z^2}{\sigma(z)^2} = \\ &= C\lim_{z\to 0}\prod_{\omega\neq 0}\left(1-\frac{z}{\omega}\right)^{-1} e^{z/\omega+\frac{1}{2}(z/\omega)^2} = C\end{aligned}$$

więc $C = 1$.

(d) Wykażemy równość, korzystając z **6.A** oraz następującego lematu:

Lemat Niech f będzie funkcją holomorficzną w pewnym zbiorze otwartym $U \subset \mathbb{C}$. Zdefiniujmy:

$$W_f^{(0)}(z,w) = f(z), \qquad W_f^{(k+1)}(z,w) = \frac{W_f^{(k)}(z,w) - \frac{1}{k!}f^{(k)}(w)}{z-w}$$

Wtedy:

$$\forall_{z\in U} \quad \lim_{w\to z} W_f^{(k)}(z,w) = \frac{1}{k!}f^{(k)}(z)$$

Dowód: jak łatwo wykazać indukcyjnie:

$$W_f^{(k)}(z,w) = \frac{f(z) - \sum_{j=0}^{k-1}\frac{1}{j!}f^{(j)}(w)(z-w)^j}{(z-w)^k} = \sum_{j=k}^{\infty}\frac{1}{j!}f^{(j)}(w)(z-w)^{j-k}$$

Z oszacowania Cauchy'ego: $|f^{(n)}(w)| \leqslant \frac{1}{n!r^{n+1}}\sup_{|u-w|\leqslant r}|f(u)|$, więc dla ustalonego z szereg ten jest zbieżny niemal jednostajnie na U wg w. Możemy więc dokonać przejścia granicznego: $\lim_{w\to z} W_f^{(k)}(z,w) = \frac{1}{k!}f^{(k)}(z)$.

Podzielmy obie strony **6.A** przez $\prod_{1\leqslant i<j\leqslant n}(z_i - z_j)$ i obliczmy granicę iterowaną

$$\lim_{z_n\to z}\lim_{z_{n-1}\to z_n}\ldots\lim_{z_2\to z_3}\lim_{z_1\to z_2}$$

lewej oraz prawej strony dla pewnego $z \in \mathbb{C}$:

$*$ prawa strona:

$$\lim_{z_n\to z}\lim_{z_{n-1}\to z_n}\ldots\lim_{z_1\to z_2}(-1)^{n(n-1)/2}1!2!\ldots n!\frac{\sigma(z_0+\ldots+z_n)}{\prod_{0\leqslant i\leqslant n}\sigma(z_i)^{n+1}}\prod_{0\leqslant i<j\leqslant n}\frac{\sigma(z_i-z_j)}{z_i-z_j} =$$

$$= (-1)^{n(n-1)/2}1!2!\ldots n!\frac{\sigma((n+1)z)}{\sigma(z)^{(n+1)^2}}\cdot 1$$

$*$ lewa strona:

$$\lim_{z_n\to z}\lim_{z_{n-1}\to z_n}\dots\lim_{z_1\to z_2}\frac{1}{\prod_{0\leqslant i<j\leqslant n}(z_i-z_j)}\begin{vmatrix} 1 & \wp(z_0) & \wp'(z_0) & \wp''(z_0) & \dots & \wp^{(n-1)}(z_0)\\ 1 & \wp(z_1) & \wp'(z_1) & \wp''(z_1) & \dots & \wp^{(n-1)}(z_1)\\ \dots & & & & & \\ 1 & \wp(z_n) & \wp'(z_n) & \wp''(z_n) & \dots & \wp^{(n-1)}(z_n)\end{vmatrix}$$

Wykonajmy teraz następujące n kroków – w k-tym kroku:

· odejmijmy k-ty wiersz przemnożony przez $\frac{1}{k}$ od wierszy $k+1, k+2, \dots, n$,

· podzielmy wiersze $k+1, k+2, \dots, n$ przez odpowiednio $z_k - z_{k+1}$, $z_k - z_{k+2}$, $\dots$, $z_k - z_n$,

· przejdźmy granicznie $z_k \to z_{k+1}$.

jak łatwo zauważyć, po wykonaniu k-tego kroku granica przyjmie postać:

$$(-1)^{?}\lim_{z_n\to z}\lim_{z_{n-1}\to z_n}\dots\lim_{z_{k+1}\to z_{k+2}}\prod_{k+1\leqslant i<j\leqslant n}(z_i-z_j)^{-1}$$

$$\begin{vmatrix} 1 & \frac{1}{0!}\wp(z_{k+1}) & \frac{1}{0!}\wp(z_{k+1}) & \dots & \frac{1}{0!}\wp^{(n)}(z_{k+1})\\ 0 & \frac{1}{1!}\wp'(z_{k+1}) & \frac{1}{1!}\wp''(z_{k+1}) & \dots & \frac{1}{1!}\wp^{(n+1)}(z_{k+1})\\ 0 & \frac{1}{2!}\wp''(z_{k+1}) & \frac{1}{2!}\wp'''(z_{k+1}) & \dots & \frac{1}{2!}\wp^{(n+2)}(z_{k+1})\\ & & \dots & & \\ 0 & \frac{1}{k!}\wp^{(k)}(z_{k+1}) & \frac{1}{k!}\wp^{(k+1)}(z_{k+1}) & \dots & \frac{1}{k!}\wp^{(n+k)}(z_{k+1})\\ 0 & W_{\wp}^{(k+1)}(z_{k+2},z_{k+1}) & W_{\wp'}^{(k+1)}(z_{k+2},z_{k+1}) & \dots & W_{\wp^{(n)}}^{(k+1)}(z_{k+2},z_{k+1})\\ & & \dots & & \\ 0 & W_{\wp}^{(k+1)}(z_{n-1},z_{k+1}) & W_{\wp'}^{(k+1)}(z_{n-1},z_{k+1}) & \dots & W_{\wp^{(n)}}^{(k+1)}(z_{n-1},z_{k+1})\\ 0 & W_{\wp}^{(k+1)}(z_n,z_{k+1}) & W_{\wp'}^{(k+1)}(z_n,z_{k+1}) & \dots & W_{\wp^{(n)}}^{(k+1)}(z_n,z_{k+1})\end{vmatrix}$$

i po n-tym kroku:

$$(-1)^{n-1}\begin{vmatrix} 1 & \wp(z) & \wp'(z) & \dots & \wp^{(n-1)}(z)\\ 0 & \wp'(z) & \wp''(z) & \dots & \wp^{(n)}(z)\\ 0 & \wp''(z) & \wp'''(z) & \dots & \wp^{(n+1)}(z)\\ & & \dots & & \\ 0 & \wp^{(n)}(z) & \wp'''(z) & \dots & \wp^{(2n-1)}(z)\end{vmatrix} = (-1)^{n-1}\begin{vmatrix} \wp'(z) & \wp''(z) & \dots & \wp^{(n)}(z)\\ \wp''(z) & \wp'''(z) & \dots & \wp^{(n+1)}(z)\\ & \dots & & \\ \wp^{(n)}(z) & \wp'''(z) & \dots & \wp^{(2n-1)}(z)\end{vmatrix}$$

co kończy dowód.

6.4 (a)

(b) pierwsza równość jest oczywista, druga wynika ze scałkowania równości $\wp(z+\omega)=\wp(z)$, trzecia z podstawienia $z=-\omega/2$ w równości $\zeta(z+\omega)=\zeta(z)+\eta(\omega)$ i skorzystaniu z nieparzystości ζ.

(c) łatwe

(d) niech D będzie fundamentalnym równoległobokiem o wierzchołkach a, $a+\omega_1$, $a+\omega_1+\omega_2$, $a+\omega_2$ i takim, że $0\in int\, D$ (w zerze mamy biegun, więc musimy go ominąć) – wtedy

$$1=res_0(\zeta)=\frac{1}{2\pi i}\int_{\partial D}\zeta(z)dz=\frac{1}{2\pi i}\left(\int_a^{a+\omega_2}+\int_{a+\omega_2}^{a+\omega_1+\omega_2}+\int_{a+\omega_1+\omega_2}^{a+\omega_1}+\int_{a+\omega_1}^{a}\right)\zeta(z)\,dz$$

– podstawiając w drugiej całce $z\mapsto z-\omega_2$, w trzeciej $z\mapsto z-\omega_1$, korzystając z relacji $f(z+\omega_i)=f(z)+\eta(\omega_i)$ oraz z $\int_a^{\omega_i+a}+\int_{\omega_i+a}^{a}=0$:

$$1=\frac{1}{2\pi i}\int a^{\omega_2+a}\eta(\omega_1)dz+\int a^{\omega_1+a}\eta(\omega_2)dz=\frac{1}{2\pi i}\left(\omega_2\eta(\omega_1)-\omega_1\eta(\omega_2)\right)$$

(e) całkując równość $\zeta(z+\omega)=\zeta(z)+\eta(\omega)$ wg z: $\log\sigma(z+\omega)=\log(z)+\omega(\eta)z+d$ ($d\in\mathbb{C}$ – stała zależna od ω, określona z dokładnością do wielokrotności $2\pi i$), czyli $\sigma(z+\omega)=e^{\eta(\omega)z+d}\sigma(z)$.

Jeżeli $\omega/2 \notin \Lambda$, to podstawiając $z = -\omega/2$ w równości $\sigma(z+\omega) = e^{\eta(\omega)z+d}\sigma(z)$, korzystając z nieparzystości σ oraz z tego, że $\zeta(\omega/2) \neq 0$:

$$\sigma(\omega/2) = -e^{-\eta(\omega)\omega/2+d}\sigma(\omega/2) \quad \Rightarrow \quad -1 = e^{-\eta(\omega)\omega/2+d}$$

i $d = \eta(\omega)\omega/2 + 2\pi in$ $(n \in \mathbb{Z})$, więc

$$\sigma(z+\omega) = e^{\eta(\omega)z+d}\sigma(z) = -e^{\eta(\omega)(z+\omega/2)}\sigma(z) \qquad (*)$$

Jeżeli $\omega/2 \in \Lambda$, to $\omega = 2a_1\omega_1 + 2a_2\omega_2$ $(a_i \in \mathbb{Z})$, więc stosując $(*)$ $|2a| + |2b|$ razy i z liniowości η:

$$\sigma(z+\omega) = \sigma(z + 2a_1\omega_1 + 2a_2\omega_2) = (-1)^{2a+2b} \exp\left(\sum_{j=1}^{2} 2a_j\eta(\omega_j)(z+\omega_j/2)\right)\sigma(z) = e^{\eta(\omega)(z+\omega/2)}\sigma(z)$$

6.12

(a) Rozważmy pętle $\alpha = \alpha_4^{-1} * \alpha_3 * \alpha_2^{-1} * \alpha_1$, $\beta = \beta_1 * \beta_2^{-1}$, gdzie:

$$\alpha_1(t) = \left(t, \sqrt{(1-t^2)\cdot(1-k^2t^2)}\right), \quad 0 \leqslant t \leqslant 1 \text{ – ścieżka od } (0,1) \text{ do } (1,0)$$

$$\alpha_2(t) = \left(-t, \sqrt{(1-t^2)\cdot(1-k^2t^2)}\right), \quad 0 \leqslant t \leqslant 1 \text{ – ścieżka od } (0,1) \text{ do } (-1,0)$$

$$\alpha_3(t) = \left(-t, -\sqrt{(1-t^2)\cdot(1-k^2t^2)}\right), \quad 0 \leqslant t \leqslant 1 \text{ – ścieżka od } (0,-1) \text{ do } (-1,0)$$

$$\alpha_4(t) = \left(t, -\sqrt{(1-t^2)\cdot(1-k^2t^2)}\right), \quad 0 \leqslant t \leqslant 1 \text{ – ścieżka od } (0,-1) \text{ do } (1,0)$$

$$\beta_1(t) = \left(t, i\cdot\sqrt{(t^2-1)\cdot(1-k^2t^2)}\right), \quad 1 \leqslant t \leqslant 1/k \text{ – ścieżka od } (1,0) \text{ do } (1/k,0)$$

$$\beta_2(t) = \left(t, -i\cdot\sqrt{(t^2-1)\cdot(1-k^2t^2)}\right), \quad 1 \leqslant t \leqslant 1/k \text{ – ścieżka od } (1,0) \text{ do } (1/k,0)$$

(gdzie $*$ oznacza mnożenie dróg o tych samych końcach). Pętle te tworzą bazę $\pi_1(E(\mathbb{C}),(1,0)) \cong \mathbb{Z}^2$; uzasadnimy to na koniec rozwiązania.

Zauważmy, że periody dane są wzorami (patrz np. dowód Proposition 5.2. (a)):

$$\omega_1 = \int_\alpha \frac{dx}{y}, \qquad \omega_2 = \int_\beta \frac{dx}{y},$$

czyli:

$$\omega_1 = \int_t \frac{x'(t)dt}{y(t)} = -\int_{t=0}^{1} \frac{dt}{-\sqrt{(1-t^2)\cdot(1-k^2t^2)}} + \int_{t=0}^{1} \frac{-dt}{-\sqrt{(1-t^2)\cdot(1-k^2t^2)}} -$$
$$-\int_{t=0}^{1} \frac{-dt}{\sqrt{(1-t^2)\cdot(1-k^2t^2)}} + \int_{t=0}^{1} \frac{dt}{\sqrt{(1-t^2)\cdot(1-k^2t^2)}} = 4\int_{t=0}^{1} \frac{dt}{\sqrt{(1-t^2)\cdot(1-k^2t^2)}}$$

i analogicznie uzyskujemy drugi period.

α, β są bazą $\pi_1(E(\mathbb{C}),(1,0))$: niech Λ będzie kratą odpowiadającą E. Zauważmy, że bazą $\pi_1(\mathbb{C}/\Lambda)$

Rozdział VII

7.4 Przy izomorfizmie z grupą "formalną" $E_1(K) \cong E(\mathcal{M})$ zbiór $E_k(K) \subset E_1(K)$ odpowiada podgrupie $E(\mathcal{M}^k) \subset E(\mathcal{M})$, jest więc podgrupą, a z twierdzenia ?? mamy:

$$E_k(K)/E_{k+1}(K) \cong E(\mathcal{M}^k)/E(\mathcal{M}^{k+1}) \cong \mathcal{M}^k/\mathcal{M}^{k+1} \cong k^+$$

7.5 (a)

(b)

(c)

7.6 Oznaczmy: $\Phi(P) = y(P)^2 - x(P)^3 - Ax(P) - B$.

(a) fff

(b) $E(K)$ jest domknięte – jest to przeciwobraz 0 przy ciągłej funkcji Φ, jest więc zwarte jako domknięty podzbiór zwartego $\mathbb{P}^n(K)$. K jest pierścieniem topologicznym, wszystki działania są w nim ciągłe w szczególności również funkcje wymierne są ciągłe w swojej dziedzinie. Translacja jest zaś dana przez funkcje wymierne na każdej współrzędnej.

(c) pokażemy, że $E(K) \setminus E_0(K)$ jest domknięte. Niech $(P_n)_n \subset E(K) \setminus E_0(K)$ będzie ciągiem o granicy P. Wtedy ciągi $(\frac{\partial\Phi}{\partial x}(P_n))_n$ oraz $(\frac{\partial\Phi}{\partial y}(P_n))_n$ są zbieżne (w K) do odpowiednio $\frac{\partial\Phi}{\partial x}(P)$ oraz $\frac{\partial\Phi}{\partial y}(P)$. Ponadto $P_n \notin E_0(K)$, więc $v(\frac{\partial\Phi}{\partial y}(P_n)), v(\frac{\partial\Phi}{\partial y}(P_n)) > 0$. Z dyskretności metryki ciągi te muszą mieć więc od pewnego momentu tą samą waluację:

$$\forall_{n>N} \qquad v(\frac{\partial\Phi}{\partial x}(P_n)) = v(\frac{\partial\Phi}{\partial x}(P)), \qquad v(\frac{\partial\Phi}{\partial y}(P_n)) = v(\frac{\partial\Phi}{\partial y}(P))$$

więc $v(\frac{\partial\Phi}{\partial x}(P)), v(\frac{\partial\Phi}{\partial y}(P)) > 0$ oraz $P \notin E_0(K)$.

(d) zauważmy, że warstwy $E_0(K)$ w grupie $E(K)$ są rozłącznymi zbiorami otwartymi (translacja jest homeomorfizmem, więc z otwartości $E_0(K)$ wynika otwartość jego warstw) pokrywającymi zbiór zwarty – musi być ich więc skończenie wiele.

7.7 Niech π będzie uniformizatorem pierścienia liczb całkoiwtych R ciała K.
We wszystkich trzech podpunktach zredukowana krzywa to $\widetilde{E} : y^2 = x^3$. Ma ona punkt osobliwy $(0,0)$, więc $E(K) \setminus E_0(K) = \{(x,y) \in E(K) : v(x), v(y) > 0\}$.

(a) Dane równanie krzywej jest minimalne (jako że $v(B) = 1$). Załóżmy nie wprost, że $(x,y) \in E(K) \setminus E_0(K)$ – wtedy byłoby $x, y \equiv 0 \pmod{\pi}$, więc $B \equiv y^2 - x^3 - Ax \equiv 0 \pmod{\pi^2}$ – sprzeczność, bo $v(B) = 1$.
(uwaga: równość $E(K) = E_0(K)$ nie oznacza, że E/K ma dobrą redukcję, a że punkt osobliwy $\widetilde{E}$ nie należy do obrazu redukcji)

(b) Niech $A = \pi A'$, $B = \pi^2 B'$. Zauważmy najpierw, że $E(K) \setminus E_0(K) \neq \varnothing$. Istotnie, z lematu Hensla istnieje punkt (a,b) na krzywej $F(x,y) = y^2 - \pi x^3 - A'x - B' = 0$, redukujący się do punktu $(-B'/A', 0)$ na krzywej zredukowanej $y^2 = A'x + B'$ (jako że $F'(-B'/A', 0) \equiv -A' \not\equiv 0 \pmod{\pi}$). Wtedy punkt $P_0 = (\pi a, \pi b)$ należy do $E(K)$ i redukuje się do $(0,0)$.

Niech $P_i = (x_i, y_i) \in E(K) \setminus E_0(K)$ dla $i = 1, 2$ będą różnymi punktami (wtedy $v(x_i), v(y_i) > 0$). Pokażemy, że $P_1 + P_2 \in E_0$. Istotnie, $P_1 + P_2 = P_3$, $P_3 = (x_3, y_3)$ gdzie $x_3 = \lambda^2 - x_1 - x_2$, $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$. Ale:

$$y_1^2 - y_2^2 = (x_1^3 + Ax_1 + B) - (x_2^3 + Ax_2 + B) = \pi(x_1 - x_2) \cdot \big(\pi((x_1/\pi)^2 + x_1x_2/\pi^2 + (x_2/\pi)^2) + A'\big)$$

więc (drugi nawias po prawej stronie ma zerową waluację) $v((y_1 - y_2)(y_1 + y_2)) = 1 + v(x_1 - x_2)$ oraz $v(\lambda) = v(\frac{y_2 - y_1}{x_2 - x_1}) = 1 - v(y_1 + y_2) \leqslant 0$. Stąd również $v(x_3) = v(\lambda^2 - x_1 - x_2) \leqslant 0$, więc $P_1 + P_2 \in E_0(K)$.
Analogicznie, jeżeli $P_1 \notin E_0(K)$, to $[2]P_1 \in E_0(K)$ – $v(x([2]P_0)) = v(\frac{x_1^4 - 2Ax_1^2 - 8Bx_1 + A^2}{4(x_1^3 + Ax_1 + B)}) \leqslant 2 - 2 = 0$.
Reasumując, dla każego $P \in E(K)$ mamy $P \equiv 0 \pmod{E_0(K)}$ lub $P \equiv P_0 \pmod{E_0(K)}$, więc $E(K)/E_0(K) = \{[\mathcal{O}], [P_0]\} \cong \mathbb{Z}/2$.

(c) Załóżmy, że $E(K) \neq E_0(K)$, $P_0 = (x_0, y_0) \in E(K) \setminus E_0(K)$. Zauważmy najpierw, że $[2]P_0 \notin E_0(K)$ – istotnie, $v(x([2]P_0)) = v(\frac{x_0^4 - 2Ax_0^2 - 8Bx_0 + A^2}{4(x_0^3 + Ax_0 + B)}) \geqslant 3 - 2 = 1$ oraz $v(y([2P_0])) = \frac{1}{2}v(x([2]P_0)^3 + Ax([2]P_0) + B) > 0$.

Niech $P_i = (x_i, y_i) \in E(K) \setminus E_0(K)$ dla $i = 1, 2$ będą różnymi punktami (wtedy $v(x_i), v(y_i) > 0$). Pokażemy, że $P_1 + P_2 \in E_0(K)$ lub $P_1 - P_2 \in E_0(K)$. Zauważmy napierw, że $v(y_i^2) = v(x_i^3 + Ax_i + B) = 2$, więc $v(y_i) = 1$. Niech $\varepsilon \in \{-1, 1\}$ będzie takie, że $v(y_1 - \varepsilon y_2) = 1$ (gdyby $v(y_1 - y_2) \geqslant 2$ oraz $v(y_1 - y_2) \geqslant 2$, to $v(y_1) = v(2y_1) = v((y_1 - y_2) + (y_1 + y_2)) \geqslant 2$ – sprzeczność). Wtedy $v(\frac{y_1 - \varepsilon y_2}{x_1 - x_2}) = 1 - v(x_1 - x_2) \leqslant 0$, więc $v(x(P_1 + \varepsilon P_2)) = v(\left(\frac{y_1 - \varepsilon y_2}{x_1 - x_2}\right)^2 - x_1 - x_2) \leqslant 0$ oraz $P_1 + \varepsilon P_2 \in E_0(K)$.

W szegółności, biorąc P_0 mamy: $P_0 \notin E_0(K)$, $[2]P_0 \notin E_0(K)$, więc musi być $[2]P_0 - P_0 \in E_0(K)$ lub $[2]P_0 + P_0 \in E_0(K)$, czyli $[3]P_0 \in E_0(K)$.

Ostatecznie, dla dowolnego $P \in E(K)$ mamy: $P \in E_0(K)$ lub $P - P_0 \in E_0(K)$ lub $P + P_0 \in E_0(K)$, więc $E(K)/E_0(K) = \{[\mathcal{O}], [P_0], [-P_0]\} \cong \mathbb{Z}/3$.

7.8 Niech $\mathcal{M}$ będzie ideałem maksymalnym w pierścieniu liczb całkowitych $\mathcal{R}$ ciała K^{nr} – wtedy ciało reszt (mod $\mathcal{M}$) to $R/\mathcal{M} = \overline{k}$. Ponadto $\widetilde{E}_{ns}(\overline{k})$ jest krzywą eliptyczną lub grupą izomorficzną z $\overline{k}^*$ lub z $\overline{k}^+$. We wszystkich trzech grupach mnożenie przez m jest epimorfizmem. Stąd, wybierając dowolny punkt $P \in E(K^{nr})$, znajdziemy taki punkt $T \in E_{ns}(\overline{k})$, że $\widetilde{P} = [m]T$. Ale redukcja $E_0(K^{nr}) \to E_{ns}(\overline{k})$ jest surjekcją, więc $T = \widetilde{S}$ dla pewnego $S \in E_0(K^{nr})$, więc dla pewnego $R \in E_1(K^{nr})$ jest $P = [m]S + R$. Wystarczy teraz zauważyć, że na podstawie **[AEC, Lemma IV.2.3 (b)]** mnożenie przez $[m]$ na "grupie formalnej" $E_1(K^{nr})$ jest izomorfimem, więc $R = [m]Q$ dla pewnego $Q \in E_1(K^{nr})$ oraz $P = [m](S + Q)$.

7.9 (a) niech $\mathcal{D} = \{L : L/K$ – skończone rozszerzenie, E ma dobrą redukcję nad L$\}$, zaś $J = \bigcup_{L \in \mathcal{D}} I_L$ będzie sumą wszystkich grup inercji. Oznaczmy też dla dowolnej liczby pierwszej $\ell \neq char(k)$:

$$J_\ell = \ker\left(\rho_\ell : I_K \to Aut(T_\ell(E)) \cong Gl_2(\mathbb{Z}_\ell)\right) = \{\sigma \in I_K : \sigma \text{ działa trywialnie na } T_\ell(E)\} =$$

$$= \{\sigma \in I_K : \rho_\ell(\sigma) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\}$$

a także

$$H_{\ell,n} = \left\{\sigma \in I_K : \forall_i \quad \rho_{\ell_i}(\sigma) \cong \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{\ell^a}\right\} = \ker\left((mod\,\ell^a) : \rho_\ell \to Gl_2(\mathbb{Z}/\ell\mathbb{Z})\right)$$

(odwzorowanie $(mod\,\ell^a)$ to zwykła redukcja współczynników macierzy $\pmod{\ell^a}$).
Zauważmy, że ponieważ E ma potencjalnie dobrą redukcję, I_K działa na $T_\ell(E)$ przez skończony iloraz I_K/J_ℓ. Wykażemy, że $J = J_\ell = H_{\ell,n}$.
Zauważmy najpierw, że $J_\ell = J$ – istotnie, z kryterium Ogga-Nerona-Shafarevicza wynika, że $J \subset J_\ell$ (grupy inercji ciał dobrej redukcji działają trywialnie na $T_\ell(E)$), zaś z dowodu **[AEC, Corollary VII.7.3]** wynika, że (ponieważ I_K działa na $T_\ell(E)$ przez iloraz I_K/J_ℓ, jest to najmniejszy iloraz po przez który działa oraz E ma potencjalnie dobrą redukcję) istnieje ciało K' takie, że $K' \in \mathcal{D}$ oraz $I_{K'} = J_\ell$ (tak więc $J_\ell \subset J$).

Zauważmy teraz, że $J_\ell \subset H_{\ell,n} \subset H_{\ell,1}$ – wystarczy więc wykazać, że $H_{\ell,1} \subset J_\ell$. Załóżmy niewprost, że $1 < |H_{\ell,1}/J_\ell|$ i niech q będzie dowolnym dzielnikiem pierwszym $|H_{\ell,1}/J_\ell|$ (grupa ta jest skończona, bo $|I_K/J_\ell| < \infty$). Wtedy istnieje element $[\sigma] \in J_\ell/H_{\ell,1}$ rzędu q. Oznacza to, że $\rho_\ell(\sigma) \equiv I_2 \pmod{\ell}$, czyli $\rho_\ell(\sigma) = I_2 + \ell^k M$ dla pewnego $M \in M_2(\mathbb{Z}/\ell\mathbb{Z})$, $M \not\equiv O_2 \pmod{\ell}$, $k \geqslant 1$ oraz $(I_2 + \ell^k M)^q = I_2$. Z rozwinięcia dwumianowego: $q\ell^k M + \ell^{2k}(\sum_{j=2}^{q} \binom{q}{j} \ell^{kj-2k} M^j) = O_2$, czyli $qM + \ell^k(\ldots) = O_2$. Jeżeli $q \neq \ell$, to z poprzedniej równości $qM \equiv O_2 \pmod{\ell}$ oraz $M \equiv O_2 \pmod{\ell}$. Podobnie, gdy $q = \ell$, $M + \ell^{k-1}(\sum_{j=2}^{q} \binom{q}{j} \ell^{kj-2k} M^j) = O_2$ i (ponieważ $q|\binom{q}{j}$ dla $j \neq q, 0$) $M \equiv O_2 \pmod{\ell}$, wbrew założeniu. Sprzeczność oznacza, że $J_\ell = H_{\ell,1}$.

Niech $m = \prod_{i=1}^{g} \ell_i^{a_i}$. Zauważmy teraz, że

$$I_{K(E[m])} = I_K \cap Gal(\overline{K}/K(E[m])) = \{\sigma \in I_K : \sigma|_{E[m]} = id\} = \{\sigma \in I_K : \forall_i \quad \sigma|_{E[\ell_i^{a_i}]} = id\} = \\ = \bigcap_i H_{\ell_i, a_i} = J$$

Stąd grupa inercji $K(E[m])/K$ to: $I(K(E[m])/K) \cong I_K/I_{K(E[m])} = I_K/J$.

(b) Zauważmy, że równoważnie:

dla pewnego m, $(m, char(k)) = 1$: $K(E[m])/K$ jest nierozgałęzione, tzn. $|I_{K(E[m])/K}| = 1$,

$\Leftrightarrow$ (na mocy (a)) dla każdego m, spełniającego $(m, char(k)) = 1$: $|I_{K(E[m])/K}| = 1$, tzn. $K(E[m])/K$ jest nierozgałęzione,

$\Leftrightarrow$ dla każdego m spełniającego $(m, char(k)) = 1$: $K(E[m]) \subset K^{nr}$, tzn. $Gal(K^{nr}/K) \cong I_K$ działa trywialnie na $K(E[m])$,

$\Leftrightarrow$ dla każdego m spełniającego $(m, char(k)) = 1$: I_K działa trywialnie na $E[m]$

$\Leftrightarrow$ (na mocy Nerona-Ogga-Shafarevicza) E ma dobrą redukcję nad K,

(c) Niech $p := char(k)$. Zauważmy, że $K(E[m])/K$ jest łagodnie rozgałęzione $\Leftrightarrow \quad p \nmid \#I_{K(E[m])/K}$. Ale na mocy (a) liczba $\#I_{K(E[m])/K}$ nie zależy od wyboru m. Wystarczy więc zauważyć, że $1 \leqslant \#I_{K(E[2])/K} \leqslant 4$, więc dla $p \geqslant 5$ mamy $p \nmid \#I_{K(E[2])/K}$.

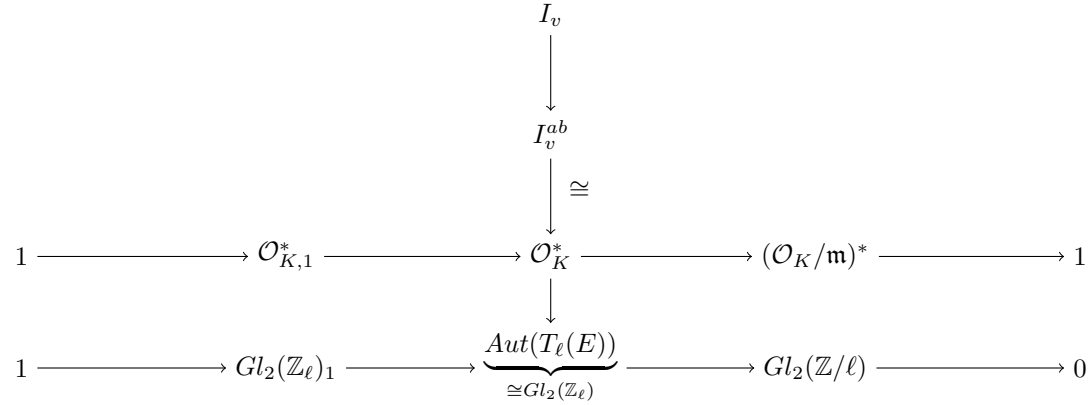
7.10 **(na podstawie [AEC II, Theorem 2.6.4, str. 149])**
Niech $\ell \in \mathbb{P} \setminus \{p\}$. Chcemy pokazać, że $image(I_v \to Aut(T_\ell(E)))$ jest skończony, bowiem $j(E) \in R$ wtw. gdy krzywa ma potencjalnie dobrą redukcję, czyli wtw. gdy I_v działa na $T_\ell(E)$ przez skończony iloraz.
Zauważmy, że zgodnie z zadaniem 3.24 $G_{\overline{K}/K}$ działa abelowo na $T_\ell(E)$ – oznacza to, że komutator $[G_{\overline{K}/K}, G_{\overline{K}/K}]$ działa trywialnie na $T_\ell(E)$ oraz, że działanie $G_{\overline{K}/K} \circlearrowright T_\ell(E)$ faktoryzuje się przez działanie $G_{\overline{K}/K}/[G_{\overline{K}/K}, G_{\overline{K}/K}] \cong G_{K^{ab}/K}$. Skorzystamy z lokalnej teorii ciał klas:

> **Twierdzenie (lokalna wzajemność Artina)**
> Istnieje homomorfizm $\rho_K : K^* \to G_{K^{ab}/K}$, który jest ciągłą iniekcją o gęstym obrazie. Indukuje on topologiczny izomorfizm grup $\rho_K : \mathcal{O}_K^* \to I_v^{ab}$.

oraz z opisu grupy $Gl_n(\mathbb{Z}_\ell)_1 := \{A \in Gl_n(\mathbb{Z}_\ell) : A \equiv I \pmod{\ell}\} = \ker(Gl_n(\mathbb{Z}_\ell) \to Gl_n(\mathbb{Z}/\ell))$ dostarczanego przez teorię szeregów formalnych:

> **Twierdzenie** Dla dowolnego ciała lokalnego K o ideale maksymalnym $\mathfrak{m}$ oraz uniformizatorze π mamy izomorfizm:
> $$Gl_n(\mathcal{O}_K)_1 \cong M_n(\mathfrak{m}), \quad 1 + \pi A \mapsto \log(1 + qA) := \sum_{n=1}^{\infty} \frac{(-1)^{n+1}\pi^n}{n} A^n$$
> W szczególności: $\mathcal{O}_{K,1}^* := \{x \in \mathcal{O}_K^* : x \equiv 1 \pmod{\mathfrak{m}}\} \cong \mathfrak{m}$ oraz $Gl_n(\mathbb{Z}_\ell)_1 \cong M_2(\ell\mathbb{Z}_\ell)$.

Zgodnie z powyższym twierdzeniem, $\mathcal{O}_{K,1}^*$ jest więc grupą pro-p (tzn. proskończoną grupą, taką że iloraz przez dowolną otwartą podgrupę normalną jest p-grupą; równoważnie – granicą odwrotną systemu dyskretnych skończonych p-grup), zaś $Gl_2(\mathbb{Z}_\ell)_1$ jest grupą pro-ℓ. Rozważmy diagram:



– z samej definicji wiersze są w nim dokładne. Zauważmy, że nie istnieją nietrywialne homomorfizmy z ℓ-grup do p-grup, więc przecięcie obrazu $\mathcal{O}^*_{K,1}$ oraz $Gl_2(\mathbb{Z}_\ell)_1$ w grupie $Aut(T_\ell(E))$ jest trywialne. Stąd (jako że $image(\mathcal{O}^*_{K,1} \to Aut(T_\ell(E))) \cap \ker(Gl_2(\mathbb{Z}_\ell) \to Gl_2(\mathbb{Z}/\ell)) = 1$) mamy zanurzenie w skończoną grupę

$$image\left(\mathcal{O}^*_{K,1} \to Aut(T_\ell(E))\right) \hookrightarrow Gl_2(\mathbb{Z}/\ell)$$

oraz $|image\left(\mathcal{O}^*_{K,1} \to Aut(T_\ell(E))\right)| < \infty$ Ale $\mathcal{O}^*_K/\mathcal{O}^*_{K,1} \cong (\mathcal{O}_K/\mathfrak{m})^*$ jest skończoną grupą, więc $image\left(\mathcal{O}^*_K \to Aut(T_\ell(E))\right)$ jest również skończony, co oznacza, że $image(I_v^{ab} \to Aut(T_\ell(E)))$ jest skończony i kończy tezę.

7.13 Niestety w zadaniu brakuje założeń – może się zdarzyć, że $v(r) < 0$ i $r \notin \mathbb{Z}_p$. Wystarczy jednak, żeby spełniony był jeden z równoważnych warunków:

(i) $E'(\mathbb{Q}_p)[p] = 0$,

(ii) jeżeli $R \in E'(\mathbb{Q}_p)$ oraz $[p]R \in E'_2(\mathbb{Q}_p)$, to $R \in E'_1(\mathbb{Q}_p)$,

(iii) istnieje $R \in E'(\mathbb{Q}_p)$ taki, że $[p]R \notin E'_2(\mathbb{Q}_p)$,

Istotnie, gdyby $S \in E'(\mathbb{Q}_p)[p]$, $S \neq \mathcal{O}$, to $r = \frac{0}{0}$ byłoby nieokreślone (łatwo wskazać inne przykłady, w których uzyska się błędny wynik).

Zauważmy najpierw, że zgodnie z **[AEC, Theorem IV.6.4]** $\log_{\mathcal{F}} : E'_1(\mathbb{Q}_p) \to p\mathbb{Z}_p$ jest izomorfizmem, a ponadto podgrupy $E'_2(\mathbb{Q}_p) \supseteq E'_3(\mathbb{Q}_p) \supseteq \ldots$ odpowiadają w tym izomorfizmie podgrupom $p^2\mathbb{Z}_p \supseteq p^3\mathbb{Z}_p \supseteq \ldots$; w szczególności $E'_{k+1}(\mathbb{Q}_p) = pE'_k(\mathbb{Q}_p)$ dla $k = 1, 2, \ldots$.

Równoważność warunków:

$(i) \Rightarrow (ii)$: Niech $R \in E'(\mathbb{Q}_p) \setminus E'_1(\mathbb{Q}_p)$ będzie dowolnym punktem nie będącym w jądrze redukcji (tzn. $\widetilde{R} \neq \mathcal{O}$). Załóżmy nie wprost, że $[p]R \in E'_2(\mathbb{Q}_p) = pE'_1(\mathbb{Q}_p)$ – oznacza to, że istnieje $T \in E'_1(\mathbb{Q}_p)$ taki, że $[p]R = [p]T$, czyli $R - T \in E'(\mathbb{Q}_p)[p] = 0$ oraz $R = T \in E'_1(\mathbb{Q}_p)$ – sprzeczność kończy dowód.

$(ii) \Rightarrow (iii)$: oczywiste.

$(iii) \Rightarrow (i)$: załóżmy, że $S \in E'(\mathbb{Q}_p)[p]$, $S \neq \mathcal{O}$. Wtedy zgodnie z **twierdzenia ???**: $S \notin E'_1(\mathbb{Q}_p)$, więc $E(\mathbb{F}_p) = \langle \widetilde{S} \rangle$. Stąd, dla dowolnego $R \in E'(\mathbb{Q}_p)$: $\widetilde{R} = [a]\widetilde{S}$ dla pewnego $a \in \{0, \ldots, p-1\}$, więc $R - [a]S \in E'_1(\mathbb{Q}_p)$ oraz $[p]R = [p]R - [a][p]S \in pE'_1(\mathbb{Q}_p) = E'_2(\mathbb{Q}_p)$

Dowód zadania:

(a) redukcja jest "na" (patrz twierdzenie????)

(b) $\#E(\mathbb{F}_p) = p$, więc dowolny niezerowy element $E(\mathbb{F}_p)$ ma rząd p, czyli $[p]P', [p]Q'$ należą do jądra redukcji $E'_1(\mathbb{Q}_p)$.

(c) zakładamy, że $P \neq \mathcal{O}$. Wtedy $P' \notin E'_1(\mathbb{Q}_p)$, więc (z warunku (ii)) $[p]P' \notin E'_2(\mathbb{Q}_p)$ – oznacza to, że $\log_{\mathcal{F}}([p]P') \in p\mathbb{Z}_p \setminus p^2\mathbb{Z}_p$ oraz $v(\log_{\mathcal{F}}([p]P')) = 1$. Analogicznie: $[p]Q' \in E_1(\mathbb{Q}_p)$, więc $v(\log_{\mathcal{F}}([p]P')) \geqslant 1$ i ostatecznie

$$v(r) = v(\log_{\mathcal{F}}([p]Q')) - v(\log_{\mathcal{F}}([p]P')) \geqslant 0$$

(równość zachodzi, o ile $Q \neq \mathcal{O}$).

(d) mamy:

$$\log_{\mathcal{F}}([p](Q' - [m]P')) = \log_{\mathcal{F}}([p]Q') - m\log_{\mathcal{F}}([p]P') = (r-m)\log_{\mathcal{F}}([p]P')$$

więc $v(\log_{\mathcal{F}}([p](Q' - [m]P')) = v(r-m) + v(\log_{\mathcal{F}}([p]P')) \geqslant 2$ oraz $[p](Q' - [m]P') \in E'_2(\mathbb{Q}_p)$, co daje (z warunku (ii)) $Q' - [m]P' \in E'_1(\mathbb{Q}_p)$, czyli $P = \widetilde{P'} = \widetilde{[m]Q'} = mQ$.

Rozdział VIII

8.1 ($rank_{\mathbb{Z}/m}(G)$ to największe r takie, że G ma podgrupę izomorficzną z $(\mathbb{Z}/m)^r$)

8.2 Wykażemy, że jeżeli $E[2] \subset E(\mathbb{Q})$, to $rank_{\mathbb{Z}}(E(\mathbb{Q})) + 2 \leqslant rank_{\mathbb{Z}/m}(E(\mathbb{Q})/mE(\mathbb{Q}))$. Istotnie, jeżeli $E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^r$, to $E(\mathbb{Q})/2E(\mathbb{Q}) \cong (E(\mathbb{Q})_{tors}/2E(\mathbb{Q})_{tors}) \otimes (\mathbb{Z}/2)^r$. Wystarczy więc wykazać, że $(E(\mathbb{Q})_{tors}/2E(\mathbb{Q})_{tors})$ zawiera podgrupę $\cong (\mathbb{Z}/2)^2$. Niech: $E[2] = \{\mathcal{O}, P_1, P_2, P_3\}$ (wtedy $P_3 = P_1 + P_2$) i wybierzmy dla każdego $i \in \{1,2,3\}$ największe takie a_i, że $P_i = [2^{a_i}]S_i$ dla pewnego $S_i \in E(\mathbb{Q})$. Załóżmy bez straty ogólności, że $a_1 \leqslant a_2 \leqslant a_3$. Wykażemy, że $\langle [S_2] \rangle \times \langle [S_3] \rangle \subset (E(\mathbb{Q})_{tors}/2E(\mathbb{Q})_{tors})$ jest izomorficzne z $(\mathbb{Z}/2)^2$. Istotnie, z maksymalności a_i: $S_1, S_2, S_3 \notin 2E(\mathbb{Q})$. Wystarczy wykazać, że $\langle [S_2] \rangle \cap \langle [S_3] \rangle = \{\mathcal{O}\}$, tzn. że $S_2 \not\equiv -S_3 \pmod{2E(\mathbb{Q})}$. Istotnie, załóżmy nie wprost, że $S_2 + S_3 = [2]T$ dla $T \in E(\mathbb{Q})$. Jeżeli $a_2 < a_3$, to $[2^{a_3}]S_2 = 0$, więc $P_3 = [2^{a_3}]S_3 = [2^{a_3}]S_2 + [2^{a_3}]S_3 = [2^{a_3}][2]T = [2^{a_3+1}]T$ wbrew maksymalności a_3. Jeżeli zaś $a_2 = a_3$, to $P_1 = P_2 + P_3 = [2^{a_2}]P_2 + [2^{a_3}]P_3 = [2^{a_3}][2]T = [2^{a_3+1}]T$, wbrew maksymalności a_1.
Stąd $E(\mathbb{Q})/2E(\mathbb{Q})$ zawiera podgrupę izomorficzną z $(\mathbb{Z}/2)^2 \times (\mathbb{Z}/2)^r$, więc $rank_{\mathbb{Z}}(E(\mathbb{Q}))+2 \leqslant rank_{\mathbb{Z}/m}(E(\mathbb{Q})/mE(\mathbb{Q}))$.

W naszym zadaniu mamy: $\Delta_{E_d} = 4d^6$ oraz $E[2] = \{(0,0), (d,0), (-d,0)\} \subset E(\mathbb{Q})$, więc w notacji z 8.1: $S = \{v \in M^0_{\mathbb{Q}} : v(2d) > 0\} \cup \{$ nieskończona waluacja $\mathbb{Q}\}$, czyli $\#S = \nu(2d) + 1$. Stąd, ponieważ grupa klas jest trywialna:

$$rank_{\mathbb{Z}}(E(\mathbb{Q})) + 2 \leqslant rank_{\mathbb{Z}/m}(E(\mathbb{Q})/mE(\mathbb{Q})) \overset{(8.1)}{\leqslant} 2\#S + 0 = 2\nu(2d) + 2$$

8.3 Niech $\Phi : E(L) \to E(L) \otimes \mathbb{Q}$ będzie kanonicznym homomorfizmem o jądrze $E(L)_{tors}$.

(a) Wybierzmy skończone rozszerzenie Galois M/K takie, że $rank\, E(M) = r$. Niech $E(M) = E(L)_{tors} \oplus \langle P_1 \rangle \oplus \ldots \oplus \langle P_r \rangle$. wykażemy, że bazą $E(L) \otimes \mathbb{Q}$ jest $\Phi(P_1), \ldots, \Phi(P_r)$.
Wystarczy wykazać, że dla dowolnego $P \in E(L)$ punkt $\Phi(P)$ można zapisać jako kombinację liniową $P_1, \ldots, P_r$. Niech $C = M(P)$ – wtedy rozszerzenie C/K jest skończone oraz $M \subset C \subset L$, więc $rank\, E(C) = r$; $E(C) = E(C)_{tors} \oplus \langle S_1 \rangle \oplus \ldots \oplus \langle S_r \rangle$. Wtedy $[P_1, \ldots, P_r] = A[S_1, \ldots, S_r] + [T_1, \ldots, T_r]$ dla pewnych $A \in M_n(\mathbb{Q})$, $T_i \in E(C)_{tors}$ oraz domnażając przez iloczyn $rz(T_1) \ldots rz(T_r)$
?? ??????????
??

(b) Niech $t = \#E(L)_{tors}$, $\sup_{K \subset M \subset L} rankE(M) = r$. Wybierzmy skończone rozszerzenie Galois M/K takie, że $E(L)_{tors} \subset E(M)$ oraz $rank\, E(M) = r$. Niech $E(M) = E(L)_{tors} \oplus \langle P_1 \rangle \oplus \ldots \oplus \langle P_r \rangle$.

Zauważmy najpierw, że rząd dowolnego elementu w grupie $E(L)/E(M)$ dzieli t. Istotnie, niech $[P] \in E(L)/E(M)$, zaś $C = M(P)$. Wtedy rozszerzenie C/K jest skończone oraz $M \subset C \subset L$, więc $rank\, E(C) = r$. Stąd $E(C)$ oraz $E(M)$ są grupami tej samej rangi, więc ich iloraz jest skończony i $[s]P \in E(M)$ dla pewnego $s \in \mathbb{Z}_+$. Stąd dla dowolnego $\sigma \in G_{\overline{K}/M}$ mamy: $[s]P = ([s]P)^\sigma$, więc $[s](P - P^\sigma) = \mathcal{O}$, co daje $P - P^\sigma \in E(L)_{tors}$, więc $[t](P - P^\sigma) = \mathcal{O}$, $[t]P = ([t]P)^\sigma$ oraz $[t]P \in E(M)$.

Niech $\| \sum_i q_i \Phi(P_i) \|_\infty = \max |q_i|$ oraz $U := \{x \in E(L) \otimes \mathbb{Q} : \|x\|_\infty < \frac{1}{t}\}$. Wykażemy, że $\Phi(E(L)) \cap U = \{\mathcal{O}\}$. Istotnie, jeżeli $x = \sum_i \frac{a_i}{b} \Phi(P_i) \neq \mathcal{O}$, gdzie $a_i, b \in \mathbb{Z}$ $NWD(a_1, \ldots, a_r, b) = 1$, to rząd punktu $\sum_i a_i \Phi(P_i)$ w $E(L)/E(M)$ wynosi $|b|$. Stąd $|b|$ dzieli t, więc $b \leqslant t$ oraz $\|x\|_\infty = \frac{1}{|b|} \max_i |q_i| \geqslant \frac{1}{t}$.

Stąd $\mathcal{O}$ ma otoczenie otwarte nie zawierające pozostałych punktów z podgrupy $\Phi(E(L))$, więc $E(L)/E(L)_{tors} \cong \Phi(E(L))$ (izomorfizm jest indukowany przez Φ) jest podgrupą skończenie generowaną i (ze skończoności $E(L)_{tors}$) $E(L)$ jest również grupą skończenie generowaną.

8.7 (a)

(b) Rozważmy miarę probalilistyczną na $\mathbb{Z}_+^{N+1}$ daną wzorem: $P(A) = \lim_{n \to \infty} \frac{|A \cap \{1, \ldots, n\}^{N+1}|}{n^{N+1}}$. Niech $A_n = (n\mathbb{Z}_+)^{N+1}$ – wtedy $P(A_n) = \frac{1}{n^{N+1}}$.

$$B = \{(x_0, \ldots, x_N) \in \mathbb{Z}_+^{N+1} : NWD(x_0, \ldots, x_N) = 1\}$$

Oczywiście

$$\lim_{C \to \infty} \frac{\mu_{\mathbb{Q}}(N, C)}{C^{N+1}} = \lim_{C \to \infty} \frac{\#\{(x_0, \ldots, x_N) \in \mathbb{Z}^{N+1} : NWD(x_0, \ldots, x_N) = 1\}}{C^{N+1}} = 2^{N+1} P(B)$$

(punkty mające przynajmniej jedną współrzędną zerową możemy pominąć – jest ich co najwyżej C^N; 2^{N+1} pojawia się ze względu na znak).

Niech $(p_n)_n$ będzie ciągiem kolejnych liczb pierwszych. Zauważmy, że zbiory $A_{p_{i_1}}$, $A_{p_{i_2}}, \ldots, A_{p_{i_k}}$ są niezależne dla dowolnych różnych liczb pierwszych – istotnie, $P(\bigcap_{j=1}^{k} A_{p_{i_j}}) = P(A_{p_{i_1}\ldots p_{i_k}}) = \frac{1}{(p_{i_1}\ldots p_{i_k})^{N+1}} = P(A_{p_{i_1}})\ldots P(A_{p_{i_k}})$. Stąd również ich dopełnienia muszą być niezależne, więc ponieważ $B = \bigcap_n A'_n$:

$$\begin{aligned} P(B) &= P(\bigcap_{k=1}^{\infty} A'_{p_k}) = \lim_{n\to\infty} P(\bigcap_{k=1}^{n} A'_{p_k}) = \lim_{n\to\infty} \prod_{k=1}^{n} P(A'_{p_k}) \\ &= \lim_{n\to\infty} \prod_{k=1}^{n} (1 - \frac{1}{p_k^{N+1}}) = \prod_{k=1}^{\infty} (1 - \frac{1}{p_k^{N+1}}) = \frac{1}{\zeta(N+1)} \end{aligned}$$

z produktu Eulera dla funkcji ζ.

8.9 Bez straty ogólności możemy założyć, że wszystkie

8.10 Dla $P_n = [n, 1, n]$ mamy $F(P_n) = P_n$, więc $H(F(P_n)) = H(P_n)$.

8.15 Załóżmy nie wprost, że taka krzywa istnieje, i że jej globalny model minimalny to $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Będziemy korzystali ze wzorów **[AEC, III.1, str. 42]**.

Załóżmy najpierw nie wprost, że $2|a_1$. Wtedy $b_2 = a_1^2 + 4a_4 \equiv 0 \pmod 4$, $b_4 = 2a_4 + a_1a_3 \equiv 0 \pmod 2$, $b_6 = a_3^2 + 4a_6 \equiv a_3^2 \pmod 4$, więc:

$$\pm 1 = \Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \equiv -27b_6^2 \equiv 5b_6^2 \pmod 8$$

co daje sprzeczność, jak że kwadraty przystają do $0, 1$ lub $4 \pmod 8$. Stąd $2 \nmid a_1$ oraz $c_4 = b_2^2 - 24b_4 \equiv 1 \pmod 8$.

Niech $\Delta = \varepsilon \in \{-1, 1\}$; podstawmy $c_4 = u + \varepsilon 12$ (wtedy $u \equiv 1 \mp 4 \pmod 8 \equiv 5 \pmod 8$). Wtedy:

$$\Delta = \frac{c_4^3 - c_6^2}{1728} \Rightarrow (u + \varepsilon 12)^3 - c_6^2 = \varepsilon 12^3 \Rightarrow u(u^2 + \varepsilon 3 \cdot 12u + 3 \cdot 12^2) = c_6^2 \qquad (*)$$

Zauważmy, że $NWD(u, u^2 + \varepsilon 3 \cdot 12u + 3 \cdot 12^2) | 3^3$. Stąd, po podzieleniu (*) przez kwadrat $NWD(u, u^2 + \varepsilon 3 \cdot 12u + 3 \cdot 12^2) = 3^\alpha$ stwierdzamy, że iloczyn względnie pierwszych liczb $\frac{u}{3^\alpha}$, $\frac{u^2 + \varepsilon 3 \cdot 12u + 3 \cdot 12^2}{3^\alpha}$ jest kwadratem, więc u jest kwadratem, bądź trzykrotnością kwadratu. To jednak oznacza sprzeczność, bo kwadrat lub jego trzykrotność przystaje do $0, 1, 3, 4 \pmod 8$, zaś $u \equiv 5 \pmod 8$.

8.22 (a) wybierzmy dowolne $1 < \varepsilon < \frac{1}{l^{-1} + m^{-1} + n^{-1}}$. Bez straty ogólności wystarczy pokazać, że jest skończenie wiele $x, y, z > 0$ spełniających (∗). Mamy: $z^l = x^m + y^n \geqslant x^m$, czyli $x \leqslant z^{l/n}$ i analogicznie $y \leqslant z^{l/m}$. Z hipotezy *abc*:

$$|z^l| \leqslant \kappa_\varepsilon |rad(x^m y^n z^l)|^\varepsilon \leqslant \kappa_\varepsilon (|xyz|)^\varepsilon \leqslant \kappa_\varepsilon (z^{l/n + l/m + 1})^\varepsilon$$

czyli $|z|^\alpha < \kappa_\varepsilon$ (gdzie $\alpha = l - (l/n + l/m + 1) \cdot \varepsilon = l \cdot (1 - \varepsilon(l^{-1} + m^{-1} + n^{-1})) > 0$), czyli ilość możliwości na z jest skończona. Dla każdego z istnieje maks. z^2 liczb x, y spełniających tą równość, co kończy dowód.

(b) zauważmy, że jest tylko skończenie wiele $(l, m, n) \in \mathbb{Z}_+^3$ spełniających $l^{-1} + m^{-1} + n^{-1} > 1/4$. Jeżeli zaś $l^{-1} + m^{-1} + n^{-1} \leqslant 1/4$, to biorąc w (a): $\varepsilon = 2 < \frac{1}{l^{-1} + m^{-1} + n^{-1}}$ dostajemy: $|z|^\alpha < \kappa_2$, gdzie $\alpha = l \cdot (1 - 2(l^{-1} + m^{-1} + n^{-1})) \geqslant \frac{1}{2}l$. Stąd:

$$\kappa_2 \geqslant |z|^\alpha \geqslant |z|^{l/2} \geqslant 2^{l/2}$$

więc $l \leqslant 2\log_2(\kappa_2)$. Ponadto $\kappa_2 \geqslant |z|^{l/2} \geqslant |z|^{1/2}$, więc $|z| \leqslant \kappa_2^2$. Stąd: $2^m + 2^n \leqslant x^m + y^m = z^l \leqslant \kappa_2^{2l} \leqslant 2^{4\log_2(\kappa_2)}$, więc m oraz n również są ograniczone.

Rozdział IX

9.1 (a) patrz (b),

(b) Niech A będzie zbiorem liczb ϕ-aproksymowalnych z odcinka $[0, 1]$ – wtedy α jest ϕ-aproksymowalne $\Leftrightarrow \{\alpha\} \in A$, więc zbiór wszystkich liczb ϕ-aproksymowalnych to $\bigcup_{n\in\mathbb{Z}}(A + n)$. Wystarczy więc wykazać, że

$\mu(A) = 0$.
Zauważmy, że:

$$A = \left\{ x \in [0,1] : \forall_N \exists_{q>N} \exists_{(p,q)=1} \quad x \in B\left(\frac{p}{q}, \frac{1}{q\phi(q)}\right) \right\} \subset \bigcap_{N=1}^{\infty} \bigcup_{q=N}^{\infty} B_q$$

gdzie $B_q = B\left(1/q, \frac{1}{q\phi(q)}\right) \cup B\left(2/q, \frac{1}{q\phi(q)}\right) \cup \ldots B\left(q/q\frac{1}{q\phi(q)}\right)$. Ale $\mu(B_q) \leqslant q \cdot \frac{1}{q\phi(q)}$, więc dla każdego N:

$$\mu(A) \leqslant \mu\left(\bigcap_{N=1}^{\infty} \bigcup_{q=N}^{\infty} B_q\right) \leqslant \mu\left(\bigcup_{q=N}^{\infty} B_q\right) \leqslant \sum_{q=N}^{\infty} \frac{1}{\phi(q)}$$

i (jako że $\lim_{N\to\infty} \sum_{q=N}^{\infty} \frac{1}{\phi(q)} = 0$) mamy: $\mu(A) = 0$.

9.2

9.4 – **oznaczenia:** Oznaczmy: $[n]P = (\frac{a(nP)}{d(nP)^2}, \frac{b(nP)}{d(nP)^3})$.
Niech: $E_{k,p}(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) : v_p(x(P)) \leqslant -2k\}$ – wtedy $E_{1,p}(\mathbb{Q}_p) \supseteq E_{2,p}(\mathbb{Q}_p) \supseteq \ldots$ są wstępującymi podgrupami oraz $E_{k,p}(\mathbb{Q}_p) \cong p^k\mathbb{Z}_p$ dla $p \neq 2$, $k = 1, 2 \ldots$, (logarytm formalny jest izomorfizmem), zaś dla $p = 2$: $E_{k,p}(\mathbb{Q}_2) \cong 2^k\mathbb{Z}_2$ dla $k = 2, 3 \ldots$.

– **Krok 1: wzrost mianownika:** Zgodnie z mocnym tw. Siegela: $\lim_{n\to\infty} \frac{\log a(nP)}{\log d(nP)^2} = 1$, a ponadto $\max(\log a(nP), \log d(nP)^2) = h([n]P) = h(P)n^2 + O(1)$,
więc $\log d([n]P) \leqslant h([n]P) \leqslant cn^2 + O(1)$ oraz $\log d([n]P) > cn^2 + o(n^2)$

– **Krok 2: wzrost potęg w mianownikach:** zauważmy, że jeżeli $Q \in E_{1,p}(\mathbb{Q}_p)$ dla $p \neq 2$, to:

$$v_p(d([s]Q)) = v_p(s) + v_p(d(Q)) \qquad (*)$$

– istotnie, mnożenie przez s w grupie $E_{1,p}(\mathbb{Q}_p) \cong p\mathbb{Z}_p$ zwiększa waluację o $v_p([s])$.
Ze wzoru na podwojenie punktu łatwo zauważyć ponadto, że dla $P \in E_{1,2}(\mathbb{Q}_2)$ mamy: $v_2([2]P) = v_2(P) + O(1)$.

– **Krok 3: przeformułowanie tezy:** Ustalmy n. Niech P_n będzie zbiorem "nieprymitywnych" dzielników pierwszych $d([n]P)$, tzn. $p \in P_n$ wtw. gdy $n_p | n$ (czyli $p | d([n]P)$) oraz gdy $n_p < n$. Niech $A_n = \prod_{p\in P_n} p^{v_p(d([n]P))}$ będzie "nieprymitywną" częścią $d([n]P)$. Wtedy chcemy pokazać, że (jeżeli tylko n jest dostatecznie duże) $d([n]P) > A_n$ – wtedy dowolny dzielnik pierwszy q liczby $\frac{d([n]P)}{A_n}$ będzie spełniał $n_q = n$.

– **Krok 4: jaka potęga $p \in P_n$ dzieli $d([n]P)$?**
Zauważmy, że dla każdego $p \in P_n \setminus 2$ mamy zgodnie z $(*)$:

$$v_p([n]P) = v_p(\frac{n}{n_p}) + v_p(d([n_p]P)) \leqslant v(n) + v_p(d([n_p]P)) \qquad (**)$$

Jeżeli $2 \in P_n$, to mamy: $n = 2^t \cdot g \cdot n_2$ dla $2 \nmid g$, więc (mnożenie przez nieparzystą liczbę nie zmienia waluacji, bo: $E_{k,2}(\mathbb{Q}_2)/E_{k+1,2}(\mathbb{Q}_2) \cong \mathbb{Z}/2$):

$$v_2([n]P) = v_2([2^t][n_2]P) \leqslant v_2([n_2]P) + O(t) \leqslant v_2([n_2]P) + O(\log_2(n))$$

– **Krok 5: szacujemy A_n:**
z kroku 4 (korzystając z $(**)$) mamy:

$$A_n = \prod_{p\in P_n} p^{v_p(d([n]P))} \leqslant \prod_p p^{v_p(n)} \cdot \prod_{p\in P_n} p^{v_p(d([n_p]P))} \cdot 2^{O(\log_2(n))} \leqslant n^2 \cdot C \cdot \prod_{k|n, k\neq n} d([k]P)$$

więc:

$$\log A_n \leqslant C + 2\log n + \sum_{k|n,k\neq n} \log d([k]P) \leqslant C + \log n + \sum_{k|n,k\neq n} \left(ck^2 + O(1)\right)$$

Wtedy:

$$\sum_{k|n,k\neq n} \left(ck^2 + O(1)\right) < \sum_{k=2}^{\infty} c\frac{n^2}{k^2} + n <$$

$$< c\underbrace{(\frac{\pi^2}{6}-1)}_{<0,7} n^2 + n < (0,7+\delta)cn^2$$

(skorzystaliśmy m.in. z równości $\sum \frac{1}{n^2} = \frac{\pi^2}{6}$) Ostatecznie więc $\log A_n < (0,7+\delta)cn^2 < cn^2 + o(n^2) = \log d([n]P)$, co dowodzi tezy.

9.5 (a) **(na podstawie artykułu Lewisa i Mahlera „On representation of integers by binary forms") Uwaga: nierówność jest oczywiście prawdziwa dla dowolnego $t \in \mathbb{C}$.**
Dla $h(x) = \sum c_i x^i \in \mathbb{C}[x]$ będziemy oznaczali: $H(h) = \max_i |a_i|$ (wysokość wielomianu) oraz $\Delta(h) = \prod_{i<j}(\alpha_i - \alpha_j)^2$ (wyróżnik wielomianu). Niech $f(x) = \sum a_i x^i = a_n \prod_i (x - \xi_i) \in \mathbb{Z}[x]$.

Lemat 1 $H(g) \leqslant nH(f)$, gdzie $g(x) = \frac{f(x)}{x-\xi_j}$.
Dowód: Załóżmy najpierw, że $|\xi_j| < 1$. Wtedy: $g(x) = \sum_{k=0}^{\infty} \frac{\xi_j^k}{x^{k+1}}$??

Lemat 2 $|\Delta(f)| \leqslant n^{2n-1} H(f)^{2n-2}$.
Dowód: $\Delta(f) = \frac{1}{a_0} \left| \begin{matrix} na_n & (n-1)a_{n-1} & \dots & 0 & 0 \end{matrix} \right| \leqslant$ (nierówność Hadamadra)
$\leqslant \sqrt{(na_n)^2 + ((n-1)a_{n-1})^2 + \dots} \leqslant H(f)^{2n-1}$

Lemat 3 Jeżeli $\Delta(f) \neq 0$, to $|f'(\xi_j)| \geqslant \frac{1}{n^{2n} H(f)^n}$.
Dowód: Niech $g(x) = \frac{f(x)}{x-\xi_j}$. Wtedy $\Delta(f) = \prod_{i<j}(\xi_i - \xi_j)^2 = \prod_i f'(\xi_i) = \Delta(g) \cdot f'(\xi)$, więc $|f'(\xi)| = \frac{|\Delta(f)|}{|\Delta(g)|} \geqslant \frac{1}{|\Delta(g)|} \overset{\text{lem. 2}}{\geqslant} \frac{1}{n^{2n-1} H(g)^{2n-2}} \overset{\text{lem. 1}}{\geqslant} \frac{1}{n^{2n} H(f)^{2n-2}}$.

Niech $|t - \xi_j| = \min_i |t - \xi_i|$. Wtedy dla $i \neq j$: $|t - \xi_i| \geqslant \frac{|\xi_i - \xi_j|}{2}$ (rysunek :)). Stąd:

$$|f(t)| = |a_n| \prod_i |t - \xi_i| \geqslant \left(\prod_{i \neq j} \frac{|\xi_i - \xi_j|}{2} \right) \cdot |t - \xi_j| = \frac{1}{2^{n-1}} f'(\xi_j) \cdot |t - \xi_j| \overset{\text{Lem. 3}}{\geqslant} \frac{1}{(2n^2 H(f))^n} |t - \xi_j|$$

9.7 Załóżmy nie wprost, że $T_\ell(E) \otimes \mathbb{Q}_\ell (\cong \mathbb{Q}_\ell^2)$ ma nietrywialną $G_{\overline{K}/K}$-niezmienniczą podprzestrzeń V – wtedy musi być ona jednowymiarową przestrzenią $\mathbb{Q}_\ell$–liniową. Załóżmy, że jest ona generowana przez element $P = (P_1, P_2, \dots) \in T_\ell(E)$ (gdzie $P_i \in E[\ell^i]$). Zauważmy, że $P \neq \mathcal{O}$, więc dla $i > i_0$ mamy: $P_i \neq \mathcal{O}$ (jeżeli $P_i = \mathcal{O}$, to $P_{i-1} = \mathcal{O}$ oraz $P_1 = P_2 = \dots = P_i = \mathcal{O}$).

Z niezmienniczości V, dla każdego $\sigma \in G_{\overline{K}/K}$ istnieje $a = a(\sigma) \in \mathbb{Q}_\ell$ spełniające: $P^\sigma = aP$. Jak łatwo zauważyć, $a \in \mathbb{Z}_\ell$ (jeżeli byłoby $a = \frac{b}{\ell^k}$ to $\forall_i \quad \ell^k P_i = bP_i$ oraz $\ell^k P^\sigma = bP$, czyli $\forall_i \quad (\ell^k - b)P_i = \mathcal{O}$. Mamy jednak $NWD(\ell, \ell^k - b) = 1$, więc byłoby $P_i = \mathcal{O}$ dla każdego i).
Stąd dla każdego i mamy: $P_i^\sigma = aP_i \in \langle P_i \rangle \subset E[\ell^i]$, czyli $\langle P_i \rangle$ jest nietrywialną niezmienniczą $G_{\overline{K}/K}$–podprzestrzenią $E[\ell^i]$. Sprzeczność z twierdzeniem Serre'a dla dostatecznie dużych i kończy dowód.

9.9 (a) zauważmy, że $\max(|z|_v, \frac{1}{|z|_v^{n_v - 1}}) \geqslant 1$, czyli równoważnie: $\max(|z|_v^{n_v}, 1) \geqslant |z|_v^{n_v - 1}$. Stąd:

$$H_K(z) = \prod_w \max(1, |z|_w^{n_w}) = \prod_{w \neq v} \max(1, |z|_w^{n_w}) \cdot \max(1, |z|_v^{n_v}) \geqslant \prod_{w \neq v} |z|_w^{n_w} \cdot |z|_v^{n_v - 1} =$$

(na mocy formuły iloczynowej) $= \frac{1}{|z|_v^{n_v}}$.

(b) ustalmy $z \in K^*$. Niech $S_- = \{v \in S : |z|_v < 1\}$. Wtedy:

$$H_K(z) \cdot \prod_{v \in S} \min(1, |z|_v^{n_v}) = \prod_v \max(1, |z|_v^{n_v}) \cdot \prod_{v \in S_-} |z|_v^{n_v} \geqslant \left(\prod_{v \in S_-} 1 \cdot \prod_{v \in M_K \setminus S_-} |z|_v^{n_v} \right) \cdot \prod_{v \in S_-} |z|_v^{n_v} =$$

$$= \prod_v |z|_v^{n_v} = 1$$

9.10 Rozważmy (zgodnie ze wskazówką) tożsamość $(t^2-5)^2((t+9)^2+4)-(t^2+6t-11)^3=-1728(t-2)$. Chcemy podstawić za t taką liczbę, że $(t+9)^2+4$ jest "prawie" kwadratem. W tym celu wybierzmy dowolne rozwiązanie równania $u^2-2v^2=-1$ (jest ich nieskończenie wiele – dane są one przez $u_n+\sqrt{2}v_n=(1+\sqrt{2})^n$ dla $2\nmid n$) i podstawmy $t=2u-9$ – wtedy $(t+9)^2+4=4(u^2+1)=8v^2$ oraz postawiając: $x=\frac{t^2+6t-11}{2}$, $y=(\frac{t^2-5}{2})\cdot v$ dostajemy:

$$0<|y^2-x^3|=216|t-2|<(216\sqrt{2}+\varepsilon)\sqrt{\frac{t^2+6t-11}{2}}$$

Rozdział X

10.1 (a) Ustalmy P,T. Wtedy odwzorowanie $\sigma\mapsto e_\phi(\delta_\phi(P)(\sigma),T)$ jest kocyklem (jako że $\delta_\phi(P)(\sigma)$ jest kocyklem "multyplikatywnym" oraz e_ϕ jest "liniowe"), czyli $(\sigma\mapsto e_\phi(\delta_\phi(P)(\sigma),T))\in H^1(G_{\overline{K}/K},\mu_m)$. Ale $\delta_K:K^*\to H^1(G_{\overline{K}/K},\mu_m)$ jest izomorfizmem, więc istnieje $b(P,T)\in K^*$ takie, że

$$e_\phi(\delta_\phi(P)(\sigma),T)=\delta_K(b(P,T))$$

Dwuliniowość $(P,T)\mapsto b(P,T)$ wynika z dwuliniowości lewej strony.

(b) Niech $\forall_T\quad b(P,T)=1$. Wtedy $\forall_T\quad e_\phi(\delta_\phi(P),T)=1$, więc ($e_\phi$ jest niezdegenerowane) $\delta_\phi(P)=\mathcal{O}$. Niech $\phi(R)=P$ – wtedy: $\delta_\phi(P)=\mathcal{O}\Rightarrow\forall_\sigma\quad R^\sigma-R=\mathcal{O}$, czyli $R\in E(K)$ oraz $P\in\phi(E(K))$, tzn. $[P]=[\mathcal{O}]$ w grupie $E'(K)/\phi(E(K))$.

(c) wykażemy najpierw, że takie funkcje $f_t\in K(E')$, $g_T\in K(E)$ można wybrać.

> **Lemat** Niech $f\in\overline{K}(C)$. Wtedy $cf\in K(C)$ dla pewnego $c\in\overline{K}\Leftrightarrow\quad div(f)\in Div_K(C)$.
> **Dowód:** Załóżmy, że $div(f)\in Div_K(C)$. Wtedy $\forall_\sigma\quad div(f^\sigma)=div(f)$, więc istnieje $c_\sigma\in\overline{K}$ takie, że $f^\sigma/f=c_\sigma$. Ale wtedy $(\sigma\mapsto c_\sigma)\in H^1(G_{\overline{K}/K},\overline{K}^*)=0$ (90-te tw. Hilberta), więc c_σ jest kocyklem: $c_\sigma=a^\sigma/a$. To jednak oznacza, że $(\frac{1}{a}f)^\sigma=\frac{1}{a}f$, więc $\frac{1}{a}f\in K(C)$ – druga implikacja jest oczywista.

Zauważmy, że $div(g_T)=\phi^*(T)-\phi^*(\mathcal{O})\in Div_K(E)$, więc bez straty ogólności $g_T\in K(E)$. Wtedy $div(g_T^m)=\phi^*(m(T)-m(\mathcal{O}))$, więc $g_T^m=f_T\circ\phi$ dla $div(f_T)=m(T)-m(\mathcal{O})$.
Zgodnie z zadaniem 3.15: $e_\phi(S,T)=g_T(X+S)/g_T(X)$. Niech $P=\phi(R)$ – wtedy:

$$e_\phi(\delta_\phi(P)(\sigma),T)=e_\phi(R^\sigma-R,T)=g_T(X+R^\sigma-R)/g_T(X)=$$

(podstawiając $X:=R$)

$$=g_T(R^\sigma)/g_T(R)=(g_T(R))^\sigma/g_T(R)=(\sqrt[m]{f_T(\phi(R))})^\sigma/(\sqrt[m]{f_T(\phi(R))})=(\sqrt[m]{f_T(P)})^\sigma/\sqrt[m]{f_T(P)}=\delta_K(f_T(P))$$

(d) wystarczy zauważyć, że $div_\infty(x)=2(\mathcal{O})$, więc $div_\infty(x-x(T))=2(\mathcal{O})$. Ponadto $x(P)-x(T)=\mathcal{O}$ wtw gdy $P=T(=-T)$, więc T musi być dwukrotnym zerem $x-x(T)$ oraz $div(x-x(T))=2(T)-2(\mathcal{O})$.
Ponadto $(x-x(T))\circ\phi=$ ...???????

10.2 (a) Wybierzmy dowolne $q_i\in C_i(\overline{K})$ $(i=1,2)$. Wtedy $\theta_i:C_i\to E$, $\theta(p)=p-q_i:C_i\to E$ jest izomorfizmem rozmaitości algebraicznych nad K. Ponadto C_i ma strukturę krzywej eliptycznej nad $\overline{K}$; suma $p_1,p_2\in C_i$ jest dana przez $\theta_i^{-1}(\theta_i(p_1)+\theta_i(p_2))=(p_1-q_i)+p_2$. Stąd również $C_1\times C_2$ ma strukturę rozmaitości abelowej, przy czym $\Psi((p_1,p_2))=(p_1-q_1,p_2-q_2):C_1\times C_2\to E\times E$ jest izomorfizmem.

Niech $\phi:C_1\times C_2\to C_3$ będzie kanoniczną projekcją na grupę ilorazową

$$C_3:=(C_1\times C_2)\Big/\{(p_1,p_2):(p_1-q_1)+(p_2-q_2)=\mathcal{O}\}$$

– jest ona zdefiniowana nad K, bo $C_1\times C_2$ jest zdefiniowana nad K, zaś podgrupa "w mianowniku" jest niezmiennicza wg działania $G_{\overline{K}/K}$.
Mamy ponadto izomorfizmy rozmaitości abelowych:

$$C_3\cong\left(E\times E\Big/\{(P_1,P_2):P_1+P_2=\mathcal{O}\}\right)\cong E$$

– pierwszy z nich jest indukowany przez Ψ, drugi przez odwzorowanie $(P_1, P_2) \mapsto P_1 + P_2$. Stąd C_3 jest krzywą. Ma ona naturalną strukturę przestrzenii jednorodnej dla E, daną przez:

$$[(p_1, p_2)] + P := [(p_1 + P, p_2)] = [(p_1, p_2 + P)]$$

(druga równość wynika z tego, że $(p_1 + P, p_2) - (p_1, p_2 + P) = (-P, P) \in \{(P_1, P_2) : P_1 + P_2 = \mathcal{O}\}$).
Stąd również

$$\phi(p_1 + P_1, p_2 + P_2) = [(p_1 + P_1, p_2 + P_2)] = [(p_1, p_2 + P_2)] + P_1 = [(p_1, p_2)] + P_1 + P_2$$

(b) wystarczy wykazać (c)

(c) niech $q_3 = \phi(q_1, q_2) \in C_3$ – wtedy dla dowolnych $p_i \in C_i$:

$$\phi(p_1, p_2) = \phi(q_1 + (p_1 - q_1), q_2 + (p_2 - q_2)) = \phi(q_1, q_2) + (p_1 - q_1) + (p_2 - q_2) = q_3 + (p_1 - q_1) + (p_2 - q_2)$$

więc ponieważ ϕ jest zdefiniowane nad K, to dla każdego $\sigma \in G_{\overline{K}/K}$:

$$\phi(p_1, p_2)^\sigma = \phi(p_1^\sigma, p_2^\sigma) \quad \Rightarrow (q_3 + (p_1 - q_1) + (p_2 - q_2))^\sigma = q_3 + (p_1^\sigma - q_1) + (p_2^\sigma - q_2) \Rightarrow$$

$$q_3^\sigma + (p_1^\sigma - q_1^\sigma) + (p_2^\sigma - q_2^\sigma) = q_3 + (p_1^\sigma - q_1) + (p_2^\sigma - q_2) \Rightarrow$$

$$(q_3^\sigma - q_3) = (q_1^\sigma - q_1) + (q_2^\sigma - q_2)$$

czyli klasa kohomologii odpowiadająca q_3 jest sumą klas odpowiadających q_1 oraz q_2, czyli $\{C_1\} + \{C_2\} = \{C_3\}$.

10.3 Zgodnie z zadaniem 3.22 każda gładka krzywa C/K genusu 1 jest izomorficzna z pewną krzywą E_0/K (tzn. istnieje izomorfizm $\lambda : C \to E_0$ określony nad $\overline{K}$). Oznaczmy: $\eta(\sigma) = \lambda^\sigma \lambda^{-1} \in H^1(G_{\overline{K}/K}, Isom(E_0))$.

(a) zauważmy, że każdy izomorfizm krzywych $f : E_0 \to E_0$ można jednoznacznie przedstawić w postaci: $f = g \circ \tau_P$, gdzie $g \in Aut(E_0)$ (tzn. g jest izogenią stopnia 1) – wystarczy przyjąć $P = f(\mathcal{O})$. Ponadto wtedy: $\tau_Q \circ g = g \circ \tau_{g^{-1}(Q)}$.
Ustalmy σ i przedstawmy $\eta(\sigma) \in Isom(E_0)$ w postaci: $\eta(\sigma) = \xi(\sigma) \circ \tau_{P(\sigma)}$, gdzie $\xi(\sigma) \in Aut(E_0)$.
Zauważmy, że ξ należy do $H^1(G_{\overline{K}/K}, Aut(E))$ – istotnie:

$$\eta(\sigma\omega) = \eta(\sigma)^\omega + \eta(\omega) \Rightarrow \xi(\sigma\omega) \circ \tau_{P(\sigma\omega)} = \left(\xi(\sigma)^\omega \circ \tau_{P(\sigma)}^\omega\right) \circ \left(\xi(\omega) \circ \tau_{P(\omega)}\right) \Rightarrow$$

$$\xi(\sigma\omega) \circ \tau_{P(\sigma\omega)} = \xi(\sigma)^\omega \circ \xi(\omega) \circ \tau_{(\xi(\sigma)^\omega)^{-1}(P(\sigma)^\omega)} \tau_{P(\omega)} \Rightarrow$$

$$\underbrace{\xi(\sigma\omega)}_{izogenia} \circ \underbrace{\tau_{P(\sigma\omega)}}_{translacja} = \underbrace{\xi(\sigma)^\omega \circ \xi(\omega)}_{izogenia} \circ \underbrace{\tau_\star}_{translacja}$$

więc ze wspomnianej jednoznaczności: $\xi(\sigma\omega) = \xi(\sigma)^\omega \circ \xi(\omega)$.
Stąd $\xi \in H^1(E_0, Aut(E)) = Twist((E, \mathcal{O})/K)$ oraz $\xi = \phi^\sigma \circ \phi^{-1}$ dla pewnego $\overline{K}$-izomorfizmu krzywych $\phi : E \to E_0$.
Zauważmy, że przestrzenie jednorodne E odpowiadają klasom kohomologii $H^1(G_{\overline{K}/K}, Translacje(E)) \cong H^1(G_{\overline{K}/K}, E)$. Wystarczy więc pokazać, że klasa kohomologii izomorfizmu $\phi^{-1} \circ \lambda : C \to E$ ma swój obraz w translacjach, tzn. że dla ustalonego σ funkcja $(\phi^{-1} \circ \lambda)^\sigma (\phi^{-1} \circ \lambda)^{-1}$ jest translacją. Istotnie:

$$(\phi^{-1} \circ \lambda)^\sigma (\phi^{-1} \circ \lambda)^{-1} = (\phi^{-1})^\sigma \circ (\lambda^\sigma \lambda^{-1}) \circ \phi =$$

$$= (\phi^{-1})^\sigma \circ \eta(\sigma) \circ \phi = (\phi^{-1})^\sigma \circ \xi(\sigma) \circ \tau_{P(\sigma)} \circ \phi = (\phi^{-1})^\sigma \phi^\sigma \phi^{-1} \tau_{P(\sigma)} \phi = \tau_{\phi^{-1}(P(\sigma))}$$

10.4 (a) oczywiste

(b) wystarczy przyjąć $\alpha P = \nu(\mu'(p, P), p)$, gdzie $\nu(q, p)$ jest jedynym takim punktem P, że $\nu(p, P) = q$ (tzn. $\mu(p, \nu(q, p)) = q$).
Wtedy $\mu(p, \alpha P) = \mu(p, \nu(\mu'(p, P), p)) = \mu'(p, P), p)$, $\alpha : K \to K$ jest K-izomorfizmem jako złożenie K-izomorfizmów.

10.5 (a) ?????

(b) Niech $p_0 \in C(\overline{K})$, zaś $\pi : C \to C' = C/E[\phi]$ będzie naturalną projekcją (jest ona określona nad K). Oczywiście każdy punkt na C' jest postaci $\pi(p)$ dla $p \in C$, zaś każdy punkt na E' postaci $\phi(P)$ dla $P \in E$. Zauważmy, że C' ma naturalną strukturę przestrzenii jednorodnej dla E': suma pary punktów $(\pi(p), \phi(P)) \in C' \times E'$ dana jest przez $\mu'(\pi(p), \phi(P)) := \pi(p+P)$, zaś różnica punktów $(p_1, p_2) \in C' \times C'$ to: $\nu'(\pi(p_1), \pi(p_2)) = \phi(p_1 - p_2)$ – jak łatwo zauważyć, suma nie zależy od wyboru p, P, bo jeżeli $(\pi(p), \phi(P)) = (\pi(r), \phi(R))$ to $r = p + Q_1$, $R = P + Q_2$ dla $Q_1, Q_2 \in E[\phi]$ oraz $\pi(r + R) = \pi((p + P) + (Q_1 + Q_2)) = \pi(p + P)$ ("wyzerowaliśmy" działanie $E[\phi]$ na C). Analogicznie stwierdzamy, że odejmowanie jest dobrze zdefiniowane.
Wystarczy obliczyć odpowiadający C' kocykl $\eta_\sigma \in H^1(G_{\overline{K}/K}, E')$:

$$\eta_\sigma = \nu' \left(\pi(p_0)^\sigma, \pi(p_0)\right) = \nu'(\phi(p_0^\sigma), \pi(p_0)) = \phi(p_0^\sigma - p_0)$$

zaś $\phi(p_0^\sigma - p_0)$ jest obrazem kocyklu $(\sigma \mapsto p_0^\sigma - p_0)$ odpowiadającego C, w naturalnym przekształceniu $\phi : WC(E/K) \to WC(E'/K)$.

(c) zgodnie z (*b*), wtedy ten izomo?????

10.6 (a), (b), (c)
Pokażemy, że każda krzywa $C/\mathbb{F}_q$ genusu 1 ma punkt $\mathbb{F}_q$-wymierny (w odrobinę prostszy sposób niż sugeruje autor?). Istotnie, wybierzmy dowolny $Q_0 \in C(\overline{\mathbb{F}_q})$ i potraktujmy (C, Q_0) jako krzywą eliptyczną.

Zauważmy, że każdy niestały morfizm krzwych jest surjekcją, więc w szególności istnieje P_1 taki, że $(1 - Frob_q)(P_1) = Q_0$ (zauważmy, że $1 - Frob_q$ jest rozdzielczy, jest więc niestały). Stąd: $Frob_q(P_1) = P_1 + Q_0 = P_1$, więc $P_1 \in C(\mathbb{F}_q)$.

(d) Zauważmy, że przestrzeń jednorodna $C/\mathbb{F}_q$ krzywej eliptycznej $E/\mathbb{F}_q$ jest nietrywialna wtw. gdy $C(\mathbb{F}_q) = \varnothing$ – ten warunek jednak nigdy nie jest spełniony, więc $WC(E/\mathbb{F}_q) = 0$.

10.7 Niech τ oznacza sprzężenie. Niech $E : y^2 = x^3 + Ax + B$.

(a) Chcemy obliczyć $H^1(G_{\mathbb{C}/\mathbb{R}}, E) = H^1(\{id, \tau\}, E)$. Zauważmy, że $\xi : \{id, \tau\} \to E$ jest kocyklem wtw. gdy $0 = \xi(id) = \xi(\tau \circ \tau) = \xi(\tau)^\tau + \xi(\tau)$ oraz kobrzegiem wtw. gdy $\xi(\tau) = P^\tau - P$ dla pewnego $P \in E(\mathbb{C})$. Stąd $\xi \mapsto \xi(\tau)$ jest izomofizmem między grupą $H^1(G_{\mathbb{C}/\mathbb{R}}, E)$ a G/H, gdzie $G = \{S \in E(\mathbb{C}) : S^\tau = -S\} = \{(x, iy) \in E(\mathbb{C}) : x, y \in \mathbb{R}\}$, $H = \{P^\tau - P \in E(\mathbb{C})\}$. Zauważmy najpierw, że $H = 2G$. Istotnie, jeżeli $S^\tau = -S$, to:

$$2S = (S^\tau)^\tau - S^\tau \in H \qquad \text{więc } 2G \subset H$$

Na odwrót, jeżeli $P^\tau - P \in H$, to wybierając takie R, że $P = 2R$ (grupa $E(\mathbb{C})$ jest podzielna) stwierdzamy, że:

$$P^\tau - P = 2\underbrace{(R^\tau - R)}_{\in G} \in 2G \qquad \text{czyli } H \subset 2G$$

Rozważmy teraz krzywą $E' : -y^2 = x^3 + Ax + B$ (o postaci Weierstrassa $y^2 = x^3 + Ax - B$) – odwzorowanie $\iota : E \to E'$, $\iota(x, y) = (x, -iy)$ jest izomofizmem, przy czym $\iota(G) = E'(\mathbb{R})$. Wiemy, że:

$$E'(\mathbb{R}) = \begin{cases} \mathbb{Z}/2 \times S^1 & \Delta_{E'} = \Delta_E > 0 \\ S^1 & \Delta_{E'} = \Delta_E < 0 \end{cases}$$

wystarczy więc zauważyć, że $S^1/2S^1 = \{1\}$ oraz $(\mathbb{Z}/2 \times S^1)/2(\mathbb{Z}/2 \times S^1) \cong \mathbb{Z}/2$.

(b) [1] Załóżmy, że $\Delta_E > 0$, tzn. $x^3 + Ax + B$ ma 3 różne pierwiastki rzeczywiste. Bez straty ogólności (po translacji) załóżmy, że 0 jest środkowym z nich, tzn. $E : y^2 = x^3 + ax^2 + bx$, gdzie $b < 0$, $a > 0$.
Wtedy zgodnie z podpunktem (*a*): $H^1(G_{\mathbb{C}/\mathbb{R}}, E) = \{0, \xi\}$, gdzie $\xi(\tau) = P_0$ dla dowolnego $P_0 \in G \setminus H$. Zauważmy, że $G/H \cong E'(\mathbb{R})/2E'(\mathbb{R})$ gdzie $E' : -y^2 = x^3 + ax^2 + bx \cong y^2 = x^3 - ax^2 + bx$. Ponadto 0 jest najmniejszym pierwiastkiem $x^3 - ax^2 + bx$, więc punkt $\widetilde{P_0} = (0, 0) \in E'(\mathbb{R})$ należy do drugiej składowej (nie zawierającej $\mathcal{O}$) krzywej i nie jest dwukrotnością żadnego punktu. Stąd można przyjąć $P_0 := \iota^{-1}(\widetilde{P_0}) = (0, 0)$.

[1] Aby znaleźć krzywą odpowiadającą kocyklowi ξ, będziemy wzorowali się na **[Remark X.3.7, AEC]** przy $d = -1$.

Zauważmy, że translacja o P_0 ma postać: $\tau_{P_0}(x,y) = (\frac{b}{x}, -\frac{by}{x^2})$. Stąd działanie $G_{\mathbb{C}/\mathbb{R}}$ na $\mathbb{C}(E)_\xi$ jest dane przez:

$$i^\tau = -i, \qquad x^\tau = \frac{b}{x}, \qquad y^\tau = -\frac{by}{x^2}$$

Chcemy znaleźć podciało $\mathbb{C}(E)_\xi$ stałe wg działania $G_{\mathbb{C}/\mathbb{R}}$. Funkcje $\frac{ix}{y}$ oraz $i(x - b/x)$ są niezmiennicze wg tego działania; dla wygody dalszych obliczeń zmodyfikujmy je następująco:

$$z = \frac{ix}{y}, \qquad w = i(x - b/x)\frac{x^2}{y^2}$$

Analogicznie jak w **[Remark X.3.7, AEC]** stwierdzamy, że równanie przestrzenii jednorodnej odpowiadającej ξ to: (czyli jak???

$$C : -w^2 = 1 + 2az^2 + (a^2 - 4b)z^4$$

Zauważmy jeszcze, że $C(\mathbb{R}) = \varnothing$, gdyż po prawej stronie mamy dodatnio określoną formę dwukwadratową (jej wyróżnik to $(2a)^2 - (a^2 - 4b) = 4b < 0$, zaś współczynnik przy z^4 to $a^2 - 4b > 0$) – przestrzeń ta istotnie nie jest więc trywialna.

10.8 *Uwaga: dla K – ciała liczbowego $\overline{K}_v = \overline{K_v}$.*
Niech $\mathbb{F}$ będzie ciałem reszt ciała lokalnego K_v.
Zauważmy najpierw, że $H^1(G_{\overline{K}/K}, \mu_m) \to H^1(G_{\overline{K}_v/K_v}, \mu_m)$ jest surjekcją. Istotnie, z 90-tego tw. Hilberta oraz ciągu Kummera: $H^1(G_{\overline{K}/K}, \mu_m) \cong K^\times/(K^\times)^m$ i analogicznie w przypadku lokalnym – wystarczy więc wykazać, że $K^\times/(K^\times)^m \to K_v^\times/(K_v^\times)^m$ jest surjekcją. Ale dowolny element $x \in K_v^\times$ jest postaci: $x = \pi^n \cdot y \cdot z$, gdzie $\pi \in K^\times$ jest uniformaizatorem, $y \in K^\times$, zaś $z \in K_v^\times$, $z \equiv 1 \pmod{\pi}$ (każda klasa reszty w $\mathbb{F}$ jest reprezentowana przez element z $K^\times$). Zauważmy, że wielomian $F(X) = X^m - z \in \mathbb{F}[X]$ ma pierwiastek 1 oraz $F'(1) = m \not\equiv 0 \pmod{\pi}$, więc z lematu Hensla: $z = w^m$ dla pewnego $w \in K_v$. Stąd $[x] = [\underbrace{\pi^n \cdot y}_{\in K}]$ w $K_v^\times/(K_v^\times)^m$, udowadniając, że $K^\times/(K^\times)^m \to K_v^\times/(K_v^\times)^m$ jest surjekcją.

Zauważmy wreszcie, że $E[m] \cong \mu_m \times \mu_m$ jako $G_{\overline{K}/K}$-moduły (a więc i jako G_v-moduły) więc $H^1(G_{\overline{K}/K}, E[m]) \to H^1(G_{\overline{K}_v/K_v}, E[m])$ również jest surjekcją.
Stąd w diagramie:

$$\begin{array}{ccc} H^1(G_{\overline{K}/K}, E[m]) & \twoheadrightarrow & H^1(G_{\overline{K}/K}, E)[m] \\ \downarrow & & \downarrow \\ H^1(G_{\overline{K}_v/K_v}, E[m]) & \twoheadrightarrow & H^1(G_{\overline{K}_v/K_v}, E)[m] \end{array}$$

występują trzy surjekcje. Funkcja $H^1(G_{\overline{K}/K}, E[m]) \to H^1(G_{\overline{K}_v/K_v}, E)[m]$ jest surjekcją i złożeniem dwóch funkcji – zewnętrzna z nich również musi być surjekcją.

10.9 Zauważmy najpierw, że $[K(T) = K] = m^2 - 1$ dla $T \in E[m]$ jest możliwe tylko dla $m \in \mathbb{P}$ i wtedy $K(T) = K(E[m])$. Istotnie, z **Faktu** z zadania 10.11 b) mamy: $[K(T) : K] = \#\{\sigma(T) : \sigma \in G_{\overline{K}/K}\}$. Ponadto punkty T oraz $\sigma(T)$ mają ten sam rząd. Oznacza to, że wszystkie punkty w $E[m]$ są sprzężone i mają ten sam rząd, co jest możliwe tylko dla $m \in \mathbb{P}$.

(a) zgodnie z **[AEC, Theorem X.1.1]** mamy:

$$\alpha(P) = e_m(\delta_E(P), T) = \delta_K(f_T(P))$$

(b) Zauważmy najpierw, że $\prod_\sigma f_{\sigma(T)} = h^m$ (gdzie σ przebiegają $Gal(L/K)$) dla pewnego $h \in K(E)^*$. Istotnie,

$$div(\prod_\sigma f_{\sigma(T)}) = m\sum_\sigma((T^\sigma) - (\mathcal{O})) = mD$$

gdzie $deg(D) = 0$, $sum(D) = \sum_\sigma T^\sigma = \sum_{P\in E[m]} P = \mathcal{O}$ (elementy $(\mathbb{Z}/m)^2$ sumują się do zera) oraz $D \in Div_K(E)$. Stąd $D = div(H)$ dla pewnego $H \in K(E)^*$ oraz:

$$\prod_\sigma f_{\sigma(T)} = cH^m$$

dla pewnego $c \in \overline{K}^*$. Wykażemy, że $c \in (K^*)^m$. Istotnie, podstawiając $[m]P$ dla $P \in E(K)$ i korzystając ze wzoru: $f_T \circ [m] = g_T^m$:

$$\left(\prod_\sigma g_{\sigma(T)}(P)\right)^m = cH([m]P)^m \Rightarrow c = \left(\frac{\prod_\sigma g_{\sigma(T)}(P)}{H([m]P)}\right)^m \in (K^*)^m$$

więc wystarczy przyjąć $h = \sqrt[m]{c}H \in K^*(E)$.
Stąd dla $P \in E(K)$:

$$N_{L/K}(\alpha(P)) = \prod_\sigma \sigma(f_T(P)) = \prod_\sigma f_{\sigma(T)}(P) = h(P)^m \in (K^*)^m$$

(c) niech $P = [m]R$ i oznaczmy: $a = \alpha(P) \in L^*$.
Wtedy $\alpha(R)^m = \alpha([m]R) = \alpha(P) = a \in L^*$, a ponadto $R \in L([m]^{-1}E(L))$, więc: $\alpha(R) = f_T(R) \in L([m]^{-1}E(L))$.

Stąd $L(\sqrt[m]{a}) \subset L([m]^{-1}E(L))$. Ale zgodnie z **[VIII.Proposition 1.5]** $L([m]^{-1}E(L))$ jest niezramifikowane w $v \notin S$. Rozszerzenie $L(\sqrt[m]{a})/L$ jest jednak niezramifikowane w v wtw. gdy $ord_v(a) \equiv 0 \pmod m$.

(d) (na podstawie [Ireland, Rosen - Classical Introduction to Modern Number Theory, 19 §2, Lemma 3])
Oznaczmy $\alpha := x(T)$. Niech $E : y^2 = f(x)$, $f(x) = x^3 + Ax + B$. Załóżmy, że $P \in E(K)$, $P \in \ker\alpha$. Wtedy $x(P) - \alpha \in (L^\times)^2$, czyli

$$x(P) - \alpha = (r + s\alpha + t\alpha^2)^2. \qquad (*)$$

Z drugiej strony, korzystając z relacji $\alpha^3 = -A\alpha - B$:

$$(r + s\alpha + t\alpha^2)\cdot(s - t\alpha) = e\alpha + f \qquad (**)$$

dla pewnych $e, f \in K$. Podnosząc $(**)$ do kwadratu i podstawiając $(*)$:

$$(x(P) - \alpha)\cdot(s - t\alpha)^2 = (e\alpha + f)^2.$$

Zauważmy, że $t \neq 0$ (w przeciwnym wypadku $1, \alpha, \alpha^2$ byłyby liniowo zależne nad K). Dzieląc przez t:

$$(x(P) - \alpha)\cdot(s' - \alpha)^2 = (e'\alpha + f')^2$$

dla pewnych $s', e', f' \in K$. Zauważmy, że α spełnia zatem wielomian:

$$g(x) := (x - x(P))\cdot(x - s')^2 + (e'x + f')^2$$

więc wielomian ten musi być podzielny przez $f(x)$. Porównując stopnie i współczynniki przy najwyższych potęgach stwierdzamy, że

$$f(x) = g(x) = (x - x(P))\cdot(x - s')^2 + (e'x + f')^2.$$

Geometrycznie oznacza to, że prosta $y = e'x + f'$ przecina $E : y^2 = f(x)$ w dwóch punktach: $(x(P), \pm y(P))$ oraz (dwukrotnie) (s', u) dla pewnego $u \in K$. Stąd $P = \pm 2(s', u)$, co oznacza, że $P \in 2E(K)$ oraz kończy dowód.

(e) Krótka postać Weierstrassa dla E to: $E : y^2 = x^3 - 16x + 16$. Minimalny wyróżnik E to $\Delta_E = 37$. Ponadto $E(\mathbb{Q})_{tors} = 0$.

Niech α będzie pierwiastkiem $x^3 - 16x + 16$, $T = (\alpha, 0) \in E[2]$ oraz $L = \mathbb{Q}(\alpha)$. Można wykazać, że:

* wielomian $x^3 - 16x + 16$ ma trzy rzeczywiste pierwiastki: $\alpha_1 \approx -4,42$, $\alpha_2 \approx 1,07$, $\alpha_3 \approx 3,35$. Odpowiadają one trzem włożeniom rzeczywistym ciała L, $\sigma_i : L \hookrightarrow \mathbb{R}$, $\sigma_i(\alpha) = \alpha_i$. L jest zatem ciałem totalnie rzeczywistym oraz $\mathcal{O}_L^\times \cong \mathbb{Z}/2 \times \mathbb{Z}^2$,
* $\mathcal{O}_L = \mathbb{Z} \oplus \frac{1}{2}\alpha\mathbb{Z} \oplus \frac{1}{4}\alpha^2\mathbb{Z}$,
* $h_L = 1$,
* $2 = u_2 \cdot p_2^3$ oraz $37 = u_{37} \cdot p_{37}^2 \cdot q_{37}$ dla pewnych $u_2, u_{37} \in \mathcal{O}_L^\times$ oraz elementów pierwszych $p_2, p_{37}, q_{37} \in \mathcal{O}_L$. Zauważmy przy tym, że $N_{L/\mathbb{Q}}(p_2) = 2$, $N_{L/\mathbb{Q}}(p_{37}) = N_{L/\mathbb{Q}}(q_{37}) = 37$. Elementy p_2, p_{37}, q_{37} można jawnie wypisać jako:

$$p_2 = \frac{1}{4}\alpha^2 + \frac{1}{2}\alpha - 2,$$
$$p_{37} = \frac{1}{4}\alpha^2 + \frac{1}{2}\alpha + 1,$$
$$q_{37} = -\frac{1}{2}\alpha^2 - \frac{1}{2}\alpha + 3.$$

Stąd $S = \{p_2, p_{37}, q_{37}\}$. Załóżmy, że $a \in L^\times$, $N_{L/\mathbb{Q}}(a) \in (\mathbb{Q}^\times)^2$ oraz $2|ord_v(a)$ dla $v \notin S$. Wtedy:

$$a \equiv u \cdot p_2^{a_2} \cdot p_{37}^{a_{37}} \cdot q_{37}^{b_{37}} \pmod{(L^\times)^2}$$

dla pewnego $u \in \mathcal{O}_L^\times$ oraz $a_2, a_{37}, b_{37} \in \{0, 1\}$. Biorąc normę:

$$1 \equiv N_{L/\mathbb{Q}}(u) \cdot 2^{a_2} \cdot 37^{a_{37}+b_{37}} \pmod{(\mathbb{Q}^\times)^2},$$

co jest równoważne temu, że $N_{L/\mathbb{Q}}(u) = 1$, $2|a_2$, $2|a_{37} + b_{37}$. SAGE podaje, że

$$\mathcal{O}_L^\times = \langle \pm 1 \rangle \times \langle u_1 \rangle \times \langle u_2 \rangle,$$

gdzie $N_{L/\mathbb{Q}}(u_1) = 1$, $N_{L/\mathbb{Q}}(u_2) = -1$. Stąd:

$$\{a \in L^\times/(L^\times)^2 : N_{L/\mathbb{Q}}(a) \in (\mathbb{Q}^\times)^2, \quad 2|ord_v(a) \text{ dla } v \notin S\} = \langle u_1 \rangle \times \langle p_{37}q_{37} \rangle \cong \mathbb{Z}/2 \times \mathbb{Z}/2.$$

Zauważmy, że $\alpha((0,4)) = u_1(L^\times)^2$. Wykażemy, że $p_{37}q_{37}(L^\times)^2 \notin \alpha(E(\mathbb{Q}))$. Załóżmy nie wprost, że

$$x(P) - \alpha = p_{37}q_{37} \cdot w^2$$

dla pewnego $P \in E(\mathbb{Q})$, $w \in L^\times$. Łatwo zauważyć, że $\sigma_1(p_{37}q_{37}) \approx -16,8$ oraz $\sigma_2(p_{37}q_{37}) \approx 3,5$. Stąd:

$$x(P) - \sigma_1(\alpha) \approx x(P) + 4,42 \approx -16,8\sigma_1(w)^2 \Rightarrow x(P) < -4,42$$

$$x(P) - \sigma_2(\alpha) \approx x(P) - 1,07 \approx 3,5\sigma_1(w)^2 \Rightarrow x(P) > 1,07$$

– sprzeczność! Stąd $im(\alpha) = \langle u_1 \rangle$ oraz $E(\mathbb{Q})/2E(\mathbb{Q}) = \langle (0,4) \rangle \cong \mathbb{Z}/2$.

10.10 Ciąg dokładny $0 \to \overline{K}^* \to \overline{K}(C)^* \to Div(C) \to Pic(C) \to 0$ indukuje ciąg dokładny

$$0 \to coker(\overline{K}^* \to \overline{K}(C)^*) = \overline{K}(C)^*/\overline{K}^* \to Div(C) \to Pic(C) \to 0$$

który z kolei indukuje długi ciąg kohomologii:

$$\ldots \to Div_K(C) \to Pic_K(C) \to H^1(G_{\overline{K}/K}, \overline{K}(C)^*/\overline{K}^*) \to \ldots$$

Zauważmy, że z dokładności ciągu $Div_K(C) \to Pic_K(C)$ jest surjekcją wtw. gdy odwzorowanie $Pic_K(C) \to H^1(G_{\overline{K}/K}, \overline{K}(C)^*/\overline{K}^*)$ jest zerowe.

Lemat Jeżeli C/L jest krzywą genusu 1 oraz $C(L) \neq \varnothing$ (tzn. C jest krzywą eliptyczną) to $Div_L(C) \to Pic_L(C)$ jest surjekcją.
Dowód: Zgodnie z zadaniem 2.13 $Div_L^0(C) \to Pic_L^0(C)$ jest surjekcją. Niech $\mathcal{O} \in C(L)$. Wtedy dla dowolnego $[D] \in Pic_L(C)$, $deg\, D = m$ mamy: $[D - m(\mathcal{O})] \in Pic_L^0(C)$, więc $[D - m(\mathcal{O})] = [W]$ dla pewnego $W \in Div_L^0(C)$ oraz $[D] = [\underbrace{W + m(\mathcal{O})}_{\in Div_L(C)}]$, co kończy dowód.

Stąd, i z założeń zadania, odwzorowania $Pic_{K_v}(C) \to H^1(G_{\overline{K}_v/K_v}, \overline{K}(C)_v^*/\overline{K}_v^*)$ są zerowe dla wszystkich v.

Ponadto ciąg dokładny $1 \to \overline{K}^* \to \overline{K}(C)^* \to \overline{K}(C)^*/\overline{K}^* \to 1$ indukuje ciąg dokładny kohomologii:

$$\ldots \to H^1(G_{\overline{K}/K}, \overline{K}(C)^*) \to H^1(G_{\overline{K}/K}, \overline{K}(C)^*/\overline{K}^*) \xrightarrow{\delta} H^2(G_{\overline{K}/K}, \overline{K}^*) \to \ldots$$

gdzie $H^1(G_{\overline{K}/K}, \overline{K}(C)^*) = 0$ na mocy uogólnienia Noether 90 tw. Hilberta. Z dokładności ciągu wynika więc, że δ jest zanurzeniem. Otrzymujemy więc diagram:

$$\begin{array}{ccccccc}
Div_K(C) & \longrightarrow & Pic_K(C) & \xrightarrow{f} & H^1(G_{\overline{K}/K}, \overline{K}(C)^*/\overline{K}^*) & \xrightarrow{\delta} & H^2(G_{\overline{K}/K}, \overline{K}^*) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \iota \\
\prod_v Div_{K_v}(C) & \longrightarrow & \prod_v Pic_{K_v}(C) & \xrightarrow{0} & \prod_v H^1(G_{\overline{K}_v/K_v}, \overline{K}_v(C)^*/\overline{K}_v^*) & \longrightarrow & \prod_v H^2(G_{\overline{K}_v/K_v}, \overline{K}_v^*)
\end{array}$$

którego wiersze nie muszą już być dokładne, jednak jest przemienny (co szybko sprawdza się od razu z definicji grup i homomorfizmów), a ponadto δ oraz ι są iniekcjami (ι jest iniekcją na mocy tw. Brauera–Noether–Hasse). Stąd $\iota \circ \delta \circ f = 0 \Rightarrow f = 0$, co daje tezę.

10.11 (a) wybierzmy dowolny punkt $p_0 \in C(\overline{K})$. Wystarczy zauważyć, że:

$$m\{C/K\} = 0 \text{ w grupie } WC(E/K) \Leftrightarrow \qquad \exists_{P \in E(\overline{K})} \qquad [m](p_0^\sigma - p_0) = P^\sigma - P \Leftrightarrow$$

(E jest podzielna więc $P = [m]Q$ dla pewnego Q)

$$\Leftrightarrow \qquad \exists_{Q \in E(\overline{K})} \qquad [m](p_0^\sigma - p_0) = [m](Q^\sigma - Q) \Leftrightarrow \qquad \exists_{Q \in E(\overline{K})} \qquad [m]((p_0 - P)^\sigma - (p_0 - P)) = \mathcal{O} \Leftrightarrow$$

(przyjmując $p = p_0 - P$)

$$\Leftrightarrow \qquad \exists_{p \in C(\overline{K})} \qquad [m](p^\sigma - p^\sigma) = \mathcal{O} \Leftrightarrow \qquad \exists_{p \in C(\overline{K})} p^\sigma - p^\sigma \in E[m]$$

(b) zauważmy najpierw następujący:

Fakt $[K(p) : K] = \#\{p^\sigma : \sigma \in G_{\overline{K}/K}\}$.

Niech indeks C/K będzie równy n, $[K(p) : K] = n$. Wtedy $D_0 = \sum_{\sigma : K(p) \hookrightarrow K} (p^\sigma)$ jest określony nad K, dodatni i stopnia n.
Ponadto dowolny dodatni dywizor określony nad K jest postaci:

$$D = \sum_{j=1}^{k} a_j \sum_{\sigma : K(p_i) \hookrightarrow K} (p_i^\sigma), \qquad a_j \in \mathbb{Z}_+$$

Ale istnieje dokładnie $[K(p_i) : K]$ zanurzeń $\sigma : K(p_i) \hookrightarrow K$, więc

$$deg\, D = \sum_{j=1}^{k} a_j [K(p_i) : K] \geqslant \sum_{j=1}^{k} a_j n \geqslant n$$

(b*) udowodnimy następującą własność indeksu:
indeks dzieli stopień każdego dywizora w $Div_K(C)$**.**
Dowód: Niech $D_0 \in Div_K(C)$ będzie dodatnim dywizorem stopnia n, będącego indeksem krzywej C. Niech $D \in Div_K(C)$ będzie stopnia k oraz $r = NWD(k, n)$ – wtedy $an + bp = r$ dla pewnych $a, b \in \mathbb{Z}$ oraz $D_1 := aD_0 + bD \in Div_K(C)$ jest stopnia r. Zauważmy, że z twierdzenia Riemanna–Rocha: $\dim \mathcal{L}(D_1) = deg\, D_1 = r > 0$, więc D_1 jest liniowo zależny z pewnym dodatnim dywizorem $D_2 \in Div_K(C)$ (istotnie, jeżeli $f \in \mathcal{L}(D_1) \cap K(C)$, to $div(f) + D_1 \geqslant 0$). Ale D_2 jest stopnia r, więc z minimalności n musi być: $r = n$, czyli $NWD(k, n) = n$ oraz $n|k$.

(c) Niech $p \in C(L)$, $[L:K]=n$, $\{p^\sigma : \sigma \in G_{\overline{K}/K}\} = \{p^{\sigma_1}, \ldots, p^{\sigma_n}\}$. Zdefiniujmy: $P = \sum_{i=1}^n (p - p^{\sigma_i})$. Wtedy dla dowolnego $\sigma \in G_{\overline{K}/K}$: $\sigma_L = \sigma_j$ dla pewnego j, więc $\{\sigma \circ \sigma_i : i = 1, \ldots, n\} = \{\sigma_i : i = 1, \ldots, n\}$

$$\begin{aligned}
[n](p^\sigma - p) &= [n](p^\sigma - p) - \sum_{i=1}^n (p^{\sigma\sigma_i} - p) + \sum_{i=1}^n (p^{\sigma_i} - p) = \\
&= \sum_{i=1}^n \left((p^\sigma - p) - (p^{\sigma\sigma_i} - p)\right) + \sum_{i=1}^n (p^{\sigma_i} - p) = \\
&= \sum_{i=1}^n (p^\sigma - p^{\sigma\sigma_i}) + \sum_{i=1}^n (p^{\sigma_i} - p) = \\
&= P^\sigma - P
\end{aligned}$$

więc $[n](p^\sigma - p)$ jest kobrzegiem oraz $n\{C/K\} = 0$ w grupie $WC(E/K)$, czyli rząd $\{C/K\}$ w grupie $WC(E/K)$ dzieli n.

(d) wystarczy wykazać, że jeżeli $p \in \mathbb{P}$ oraz p nie dzieli periodu, to nie dzieli też indeksu. Załóżmy, że L/K jest rozszerzeniem Galois spełniającym $C(L) \neq \varnothing$ oraz niech $[L:K] = p^\alpha \cdot m$ dla $p \nmid m$. Niech L/M będzie rozszerzeniem odpowiadającym p-podgrupie Sylowa grupy $Gal(L/K)$ – wtedy $p \nmid |Gal(M/K)| = m$.
Niech $\xi \in H^1(G_{\overline{K}/K}, E)$ będzie kocyklem odpowiadającym C. Wtedy:

- z jednej strony naturalne odwzorowanie $Gal(\overline{K}/M) \to Gal(\overline{K}/K)$ indukuje odwzorowanie $H^1(Gal(\overline{K}/K), E) \to H^1(Gal(\overline{K}/M), E)$ oraz rząd ξ w grupie $H^1(G_{\overline{K}/K}, E)$ jest podzielny przez rząd ξ w grupie $H^1(G_{\overline{K}/M}, E)$; oznacza to, że p nie dzieli rzędu ξ w grupie $H^1(G_{\overline{K}/M}, E)$.
- z drugiej strony naturalne odwzorowanie $Gal(\overline{K}/M) \to Gal(L/M)$ indukuje odwzorowanie $H^1(Gal(L/M), E) \to H^1(Gal(\overline{K}/M), E)$. Ale $Gal(L/M)$ jest p-grupą, więc rząd ξ w grupach $H^1(G_{L/M}, E)$ oraz $H^1(G_{\overline{K}/M}, E)$ musi być potęgą p.

Stąd rząd ξ w grupie $H^1(Gal(\overline{K}/M), E)$ musi być równy 1, więc $\{C/M\}$ jest trywialne w $WC(E/M)$, co jest możliwe tylko gdy $C(M) \neq \varnothing$. Ponieważ p nie dzieli $[M:K]$, to nie dzieli też indeksu.

(f) niech m będzie periodem $C \in Ш(E/K)$. Wtedy zgodnie z (a) istnieje $p \in C$ taki, że $\forall_\sigma \quad [m](p^\sigma - p) = \mathcal{O}$ na E. Zauważmy, że $E \cong Pic^0(C)$, przy czym izomorfizm dany jest przez: $P \mapsto (P + p) - (p)$. Stąd w $Pic(C)$ mamy: $m(p) = m(p^\sigma)$, więc dywizor $m(p)$ należy do $Pic_K(C)$. Z zadania 10.10 wiemy, że istnieje $D \sim m(p)$, $D \in Div_K(C)$. Stąd pewien dywizor w $Div_K(C)$ ma stopień m, więc (z podpunktu (b*)) wiemy, że $indeks | m$. Z podpunktu (c) mamy: $m | indeks$, więc ostatecznie $period = m = indeks$.

10.12 (a)

(b)

(c) Niech $p > 5$ (dla $p = 2, 3, 5$ łatwo sprawdzić). Zgodnie z lematem Hensla, wystarczy wykazać, że istnieją $(x, y, z) \not\equiv (0, 0, 0) \pmod p$ spełniające równanie $\pmod p$. Grupa $(\mathbb{Z}/p)^\times$ jest cykliczna, niech g będzie jej generatorem. Jeżeli $p \equiv 2 \pmod 3$, to każdy element $\mathbb{Z}/p$ jest sześcianem: $x \equiv x^{1+2(p-1)} \equiv (x^{(2p-1)/3})^3$. Załóżmy, że $p \equiv 1 \pmod 3$ – wtedy podgrupa sześcianów to:

$$S = \{x^3 : x \in \mathbb{Z}/p\} = \{g^{3k} : k = 0, 1, \ldots\}$$

i ma ona moc $(p-1)/3$ oraz trzy warstwy: S, gS, g^2S. Jeżeli 3 oraz 4 należą do tej samej warstwy, to $3/4 \in S$, $3/4 = a^3$ oraz trójka $(x, y, z) = (1, -a, 0)$ spełnia równanie $3x^3 + 4y^3 + 5z^3 = 0$. Analogicznie, jeżeli do tej samej warstwy należą 4 oraz 5 lub 3 oraz 5. Załóżmy, że $3, 4, 5$ należą do różnych warstw – wtedy podstawiając w równaniu $3x^3 + 4y^3 + 5z^3 = 0$: $a = 3x^3, b = 4y^3, c = 5z^3$ dostajemy równanie: $a + b + c = 0$, gdzie a, b, c mają należeć do różnych warstw S. Załóżmy nie wprost, że równanie to nie ma rozwiązań. Wtedy:

- $1 + 3 - 4 = 0$, więc $-4 \in S$ lub $-4 \in 3 \cdot S$, czyli $4 \in S$ lub $4 \in 3 \cdot S$
- $1 + 4 - 5 = 0$, więc $4 \in S$ lub $4 \in -5 \cdot S = 5 \cdot S$.

Ale $3 \cdot S \neq 5 \cdot S$, więc musi być $4 \in S$ oraz $3, 5 \notin S$. To oznacza, że $2^2 \in S$, więc $2 \in S$ (jeżeli $x^2 = g^{2k}$ jest sześcianem, to $3 | k$, więc x jest sześcianem). Ale $2 + 3 = 5$ oraz $2 \cdot S \neq 3 \cdot S \neq 5 \cdot S \neq 2 \cdot S$. To kończy dowód.

Sposób II:
Rozumujemy analogicznie i zakładamy, że $3, 4, 5$ należą do różnych warstw S. Wtedy $60 = 3 \cdot 4 \cdot 5 \in S \cdot (gS) \cdot (g^2S) = S$, $60 \equiv k^3$ oraz $(x, y, z) = (k, -5, 4)$ jest rozwiązaniem równania $3x^3 + 4y^3 + 5z^3 \equiv 0 \pmod p$.

10.16 Załóżmy, że $rank(E(K)) < \infty$ – wtedy $|E(K)/2E(K)| < \infty$, więc podobnie jak w **[AEC, lemat redukcyjny VIII.1.1.1]** mamy $|E(L)/2E(L)| < \infty$. Niech $Gal(L/K) = \{id, \sigma\}$ (gdzie $\sigma(\sqrt{D}) = -\sqrt{D}$). czyli ?

Niech $\iota : E_D(K) \to E(L)$, $\iota(x, y) = (x, \sqrt{D}y)$, zaś $B := im\,\iota = \{P \in E(L) : P = -P^\sigma\}$. Oczywiście $E(K) = \{P \in E(L) : P = P^\sigma\}$.
Zauważmy, że jeżeli $P \in E(K) \cap B$, to $P^\sigma = P = -P$, więc $2P = \mathcal{O}$ oraz $|E(K) \cap B| \leqslant |E[2]| < \infty$. Stąd:

$$rank(E(K) + B) = rank(E(K)) + rank(B) = rank(E(K)) + rank(E_D(K))$$

Ponadto dla dowolnego $P \in E(L)$:

$$2P = \underbrace{(P + P^\sigma)}_{\in E(K)} + \underbrace{(P - P^\sigma)}_{\in B}$$

więc $2E(L) \subset E(K) + B$, co daje surjekcję $E(L)/2E(L) \twoheadrightarrow E(L)/(E(K) + B)$ oraz $|E(L)/(E(K) + B)| \leqslant |E(L)/2E(L)| < \infty$. Ale jeżeli iloraz grupy abelowej i jej podgrupy jest skończony, to mają one tą samą rangę, więc:

$$rank(E(L)) = rank(E(K) + B) = rank(E(K)) + rank(E_D(K))$$

10.20 Parę (A, Γ), gdzie A – grupa abelowa, zaś Γ jest alternującą, niezdegenerowaną formą dwuliniową będziemy nazywali **S-grupą**.
Zapiszmy A w postaci iloczynu p-grup Sylowa: $A \cong \bigoplus_p A_p$ – wtedy dla $p \neq q$ grupy A_p oraz A_q są "ortogonalne" wg iloczynu Γ, tzn. dla $x \in A_p, y \in A_q$ mamy $\Gamma(x, y) = 0$. Istotnie, jeżeli $\text{rząd}(x) = p^\alpha$, $\text{rząd}(y) = q^\beta$, to $p^\alpha\Gamma(x, y) = \Gamma(p^\alpha x, y) = 0$ w grupie $\mathbb{Q}/\mathbb{Z}$, więc $\text{rząd}(\Gamma(x, y))$ dzieli p^α i analogicznie $\text{rząd}(\Gamma(x, y))$ dzieli q^β, więc $\Gamma(x, y) = 0$.
Stąd $(A_p, \Gamma|_{A_p \times A_p})$ jest również S-grupą. Możemy więc bez straty ogólności założyć, że A jest p-grupą. Niech

$$A = \langle x_1 \rangle \oplus \langle x_2 \rangle \ldots \oplus \langle x_n \rangle \cong (\mathbb{Z}/p^{\alpha_1}) \times \ldots \times (\mathbb{Z}/p^{\alpha_{n-1}}) \times (\mathbb{Z}/p^{\alpha_n})$$

$(\alpha_1 \leqslant \ldots \leqslant \alpha_n)$. Wykażemy indukcyjnie wg n, że $A \cong (\mathbb{Z}/p^{a_1})^2 \times \ldots \times (\mathbb{Z}/p^{a_n})^2$.
Załóżmy nie wprost, że $\alpha_{n-1} \leqslant \alpha_n - 1$. Wtedy $p^{\alpha_{n-1}} x_n \neq 0$, ale:

$$\Gamma(p^{\alpha_{n-1}} x_n, x_j) = \Gamma(x_n, p^{\alpha_{n-1}} x_j) = \Gamma(x_n, 0) = 0$$

dla każdego $j < n$, więc $\Gamma(p^{\alpha_{n-1}} x, \cdot) = 0$ oraz Γ byłoby zdegenerowane. Sprzeczność oznacza, że $\alpha_{n-1} = \alpha_n$.

Analogicznie stwierdzamy, że $\Gamma(x_{n-1}, x_n) = \frac{a}{p^{\alpha_n}}$ dla $p \nmid a$ (mamy $p^{\alpha_n}\Gamma(x_{n-1}, x_n) = 0$, zaś gdyby $\Gamma(x_{n-1}, x_n) = \frac{a}{p^{\alpha_n - 1}}$ to $\Gamma(p^{\alpha_n - 1} x, \cdot) = 0$). Bez straty ogólności (po przeskalowaniu x_{n-1}): $\Gamma(x_{n-1}, x_n) = \frac{1}{p^{\alpha_n}}$.
Oznaczmy przez B "dopełnienie ortogonalne" $\langle x_{n-1} \rangle \oplus \langle x_n \rangle$ tzn. $B = \{y \in A : \beta(x_{n-1}, y) = \beta(x_n, y) = 0\}$ – wtedy:

$$A = B \oplus^\perp (\langle x_{n-1} \rangle \oplus \langle x_n \rangle)$$

(suma ta jest "ortogonalna") jako że dla każdego $a \in A$:

$$b := a - \left(p^{\alpha^n} \beta(x_n, a)\right) x_{n-1} - \left(p^{\alpha^n} \beta(x_{n-1}, a)\right) x_n$$

należy do B oraz $a = \underbrace{\star x_{n-1} + \star x_n}_{\in \langle x_{n-1} \rangle \oplus \langle x_n \rangle} + \underbrace{b}_{\in B}$.
Z ortogonalności $(B, \Gamma_{B \times B})$ jest również S-grupą, więc wystarczy zastosować do niej hipotezę indukcyjną.