Teoria liczb
mix, 1-5 czerwca

Zadanie 1 (krzywa, która jest eliptyczna, choć nie wygląda)**.** Rozważmy zbiór rozwiązań

$$S := \left\{(t,u) \in \mathbb{C}^2 \mid u^2 = t^4 - 1\right\}$$

oraz przekształcenie $\pi\colon S \setminus \{(1,0)\} \to \mathbb{C}^2$ zadane wzorem

$$\pi\,(t,u) = \left(\frac{1}{t-1}, \frac{u}{(t-1)^2}\right).$$

(a) Pokaż, że przekształcenie π jest injektywne.

(b) Pokaż, że jego obraz zawiera się w zbiorze $y^2 = f(x)$ dla pewnego wielomianu f *stopnia trzy*, który nie ma pierwiastków wielokrotnych w $\mathbb{C}$. Znajdź f.

(c) Pokaż odwrotnie, że jeśli $(x,y) \in \mathbb{C}^2$ są takie, że $y^2 = f(x)$ oraz $x \neq 0$, to $(x,y) = \pi(t,u)$ dla pewnych $(t,u) \in S$.

Rozwiązanie.
(a) Mając $(x,y) = \pi(t,u)$ możemy obliczyć $t = \frac{1}{x} + 1$ oraz $u = \frac{y}{x^2}$. To implikuje injektywność.
(b) Jeśli $(x,y) = \pi(u,t)$ to obliczamy, że

$$y^2 = \frac{u^2}{(t-1)^4} = \frac{t^4-1}{(t-1)^4}.$$

Podstawmy $t = \frac{1}{x} + 1$. Otrzymujemy

$$y^2 = \frac{\left(\frac{1}{x}+1\right)^4 - 1}{\frac{1}{x^4}} = \frac{(1+x)^4 - x^4}{1} = 4x^3 + 6x^2 + 4x + 1.$$

Pozostaje wziąć $f(x) = 4x^3 + 6x^2 + 4x + 1$ i sprawdzić, że ten wielomian nie ma pierwiastków wielokrotnych. Ale $f'(x) = 12x^2 + 12x + 4 = 4(3x^2 + 3x + 1)$. W pierścieniu $\mathbb{C}[x]$, jeśli $f(x)$ i $f'(x)$ nie są względnie pierwsze, to mają wspólny pierwiastek α. Liczba α nie jest rzeczywista, bo $3x^2 + 3x + 1$ nie ma pierwiastków rzeczywistych. Zatem również sprzężona liczba $\overline{\alpha}$ jest pierwiastkiem obu, więc $3x^2 + 3x + 1$ dzieli $f(x)$. Ale bezpośrednio sprawdzamy, że ta podzielność nie zachodzi.
(c) Niech jak w punkcie (a) $t = \frac{1}{x} + 1$ oraz $u = \frac{y}{x^2}$. Odwracając argument z punktu (b) sprawdzamy, że $u^2 = t^4 - 1$, zatem $(t,u) \in S$.

Uwaga dla zainteresowanych: z geometrii algebraicznej wynika, że jest stosunkowo mało algebraicznych przekształceń π które są „prawie" surjektywne i „prawie" injektywne (w naszym przypadku π jest po prostu injektywne). W szczególności, nie ma takich przekształceń pomiędzy $F(x,y,z) = 0$ oraz $G(t,u,v) = 0$, gdzie F, G są jednorodne i nie są osobliwe w żadnym punkcie. Ale puenta polega na tym, że jeśli ujednorodnimy $u^2 - (t^4 - 1)$, to otrzymamy wielomian $G(t,u,v) = u^2z^2 - (t^4 - z^4)$, który jest osobliwy w punkcie $(1,0,0)$. Z punktu widzenia równania $u^2 - (t^4 - 1) = 0$ ten punkt jest w „nieskończoności", zatem osobliwości nie widać.

Zadanie 2. Niech f będzie wielomianem unormowanym stopnia 3 o współczynnikach w ciele $\Bbbk$, który posiada w $\Bbbk$ pierwiastek wielokrotny.

(a) Pokaż, że jest dokładnie jeden taki pierwiastek, niech będzie to $x_0 \in \mathbb{k}$.

(b) Pokaż, że zbiór $E(\mathbb{k}) \setminus \{(x_0, 0)\}$ tworzy grupę z działaniem jak na wykładzie. *Wskazówka: dowód łączności jest ten sam i nie potrzeba go powtarzać.*

(c) $\star$ Niech $\mathbb{k}$ będzie ciałem dowolnej charakterystyki, zaś $f(x) = x^3$. Pokaż, że grupa powyżej jest izomorficzna z grupą $\mathbb{G}_{\mathrm{a}}(\mathbb{k}) := (\mathbb{k}, +)$.

(d) $\star$ Niech $\mathbb{k}$ będzie ciałem charakterystyki dwa, zaś $f(x) = x^3 - x$, zatem krzywa ma równanie Weierstrassa $y^2 = x^3 - x$. Pokaż, że grupa powyżej jest izomorficzna z grupą $\mathbb{G}_{\mathrm{m}}(\mathbb{k}) := (\mathbb{k} \setminus \{0\}, \cdot)$.

(e) $\star$ Pokaż, że powyższe dwie możliwości są jedyne, tzn. dla dowolnego f z pierwiastkiem wielokrotnym, grupa $E(\mathbb{k}) \setminus \{(x_0, 0)\}$ powyżej jest izomorficzna z $\mathbb{G}_{\mathrm{m}}(\mathbb{k})$ lub $\mathbb{G}_{\mathrm{a}}(\mathbb{k})$.

Rozwiązanie.
(a) Jeśli x_0 jest pierwiastkiem wielokrotnym $f(x)$, to $f(x) = (x - x_0)^2(x - x_1)$, gdzie $x_1 \in \mathbb{k}$ jest trzecim pierwiastkiem. Nie ma więc innego wielokrotnego pierwiastka.
(b) Możemy zdefiniować 0_E, $-(x_0, y_0) = (x_0, -y_0)$ jak na wykładzie. Przy definiowaniu dodawania jedyny problem jest następujący: może się zdarzyć, że dla pewnych punktów $(x_1, y_1), (x_2, y_2) \in E(\mathbb{k}) \setminus \{(x_0, 0), 0_E\}$ prosta przez $(x_1, y_1), (x_2, y_2)$ przechodzi przez $(x_0, 0)$. Pokażemy, że taka możliwość nie może się zdarzyć. Rozważmy równanie prostej przez $(x_1, y_1), (x_2, y_2)$ i załóżmy, że przechodzi ona również przez $(x_0, 0)$.

Prosta przez $(x_0, 0)$ ma równanie $x = x_0$ lub $y = \mu(x - x_0)$ dla pewnego $\mu \in \mathbb{k}$. W pierwszym przypadku, układ równań $y^2 = f(x)$, $x = x_0$ nie ma rozwiązań poza $(x_0, 0)$, więc $x = x_0$ nie może być równaniem jak powyżej. W drugim przypadku układ równań $y = \mu(x - x_0)$, $y^2 = f(x)$ redukuje się do równania

$$\mu^2(x - x_0)^2 - f(x) = 0.$$

Wielomian po lewej stronie ma (co najmniej) dwukrotny pierwiastek x_0. Ponadto ma on pierwiastki x_1, x_2. To niemożliwe, bowiem ma on stopień trzy. Sprzeczność![1]
(c) Mamy $x_0 = 0$. Zauważmy, że jeśli zrobimy to zadanie, to pokażemy w szczególności bijekcję pomiędzy $E(\mathbb{k})$ oraz $\mathbb{k}$, dla nieznanego ciała $\mathbb{k}$, czyli rozwiążemy równanie $y^2 = x^3$ w $\mathbb{k}$. Mówiąc jeszcze inaczej, każdemu elementowi $t \in \mathbb{k}$ musimy przypisać rozwiązanie (albo punkt 0_E). Podobny pomysł pojawił się w zadaniu 2 w serii 11-15 maja.
Mianowicie, zauważmy, że dla każdego $t \in \mathbb{k}$ para $(x, y) = (t^2, t^3)$ jest rozwiązaniem. Odwrotnie, jeśli (x, y) jest rozwiązaniem, to albo $x = 0$ i wtedy $y = 0$, albo $x \neq 0$ i wtedy dla $t := y/x$ mamy $x = y^2/x^2 = t^2$ oraz $y = x \cdot y/x = t^3$. Zatem faktycznie każde rozwiązanie równania $y^2 = x^3$, łącznie z $(0, 0)$, jest postaci (t^2, t^3) dla $t \in \mathbb{k}$. Odwzorowanie $\mathbb{k} \ni t \mapsto (t^2, t^3)$ nie jest jeszcze bijekcją, której szukamy, np. dlatego, że element neutralny 0 przechodzi na „wyrzucony" punkt $(0, 0)$, a nie na 0_E. Rozważmy zatem bijekcję $\varphi\colon \mathbb{k} \to E(\mathbb{k}) \setminus \{(0, 0)\}$ zadaną przez

$$\varphi(t) = \begin{cases} 0_E & \text{jeśli } t = 0 \\ (t^{-2}, t^{-3}) & \text{jeśli } t \neq 0. \end{cases}$$

Pokażemy, że prowadzi ona do izomorfizmu grup. Weźmy zatem $t_1, t_2 \in \mathbb{k}$. Chcemy sprawdzić, że $\varphi(t_1 + t_2) = \varphi(t_1) + \varphi(t_2)$, czyli $0 = -\varphi(t_1 + t_2) + \varphi(t_1) + \varphi(t_2)$, czyli, że punkty

$$\left((t_1 + t_2)^{-2}, -(t_1 + t_2)^{-3}\right), \quad \left(t_1^{-2}, t_1^{-3}\right), \quad \left(t_2^{-2}, t_2^{-3}\right)$$

[1] Jeśli $(x_1, y_1) = (x_2, y_2)$ to powyżej trzeba liczyć x_1 z krotnością dwa. To też prowadzi do sprzeczności.

leżą na jednej prostej. Równanie prostej przez punkty (t_1^{-2}, t_1^{-3}) oraz (t_2^{-2}, t_2^{-3}) jest dane przez

$$(t_2^{-3} - t_1^{-3}) \cdot (x - t_1^{-2}) = (t_2^{-2} - t_1^{-2}) \cdot (y - t_1^{-3}).$$

Pozostaje sprawdzić, że

$$(t_2^{-3} - t_1^{-3}) \cdot \left((t_1 + t_2)^{-2} - t_1^{-2}\right) = (t_2^{-2} - t_1^{-2}) \cdot \left(-(t_1 + t_2)^{-3} - t_1^{-3}\right),$$

o czym Czytelnik może upewnić się samodzielnie.
(d) Charakterystyka dwa w tym podpunkcie służy tylko do zapisania $x^3 - x = x(x^2 - 1) = x(x-1)^2 = x(x+1)^2$. Podstawienie $x \mapsto x - 1$ sprowadza nas do przypadku $f(x) = x^2(x-1)$. Rozważmy ogólniej $f(x) = x^2(x - x_1)$, gdzie $x_1 \in \Bbbk$ jest niezerowym elementem. Tylko tym przypadkiem będziemy się dalej zajmować, w dowolnej charakterystyce. Możemy skorzystać z zadania 2 w serii 11-15 maja.
Rozważmy dowolną parę $(x, y) \in \Bbbk^2$ spełniającą $y^2 = f(x)$. Jeśli $x = 0$, to $y = 0$ i ten punkt „odrzucamy". Jeśli zaś $x \neq 0$, to możemy położyć $t = \frac{y}{x}$ i wtedy $t^2 = \frac{y^2}{x^2} = x - x_1$, więc $x = t^2 + x_1$ oraz $y = x \cdot \frac{y}{x} = xt = t^3 + tx_1$. Znalezienie parametryzacji dającej izomorfizm grup w tym przypadku pozostawiamy Dociekliwemu Czytelnikowi.
(e) Jeśli x_0 jest pierwiastkiem trzykrotnym $f(x)$, to $f(x) = (x - x_0)^3$, zatem zmiana współrzędnych $x \mapsto x + x_0$ prowadzi do $f(x) = x^3$. Jeśli x_0 jest pierwiastkiem dwukrotnym ale nie trzykrotnym $f(x)$, to $f(x) = (x - x_0)^2(x - x_1)$ gdzie $x_1 \neq x_0$. Wtedy zmiana współrzędnych $x \mapsto x + x_0$ przeprowadza f na $x^2(x - x_2)$, gdzie $x_2 = x_1 - x_0 \neq 0$ i znajdujemy się w sytuacji z punktu (d).

Zadanie 3. Niech E będzie krzywą eliptyczną zadaną równaniem $y^2 = f(x)$, gdzie f ma współczynniki w ciele $\mathbb{Z}_p$. Zadajmy endomorfizm Frobeniusa dla ciała $K \supseteq \mathbb{Z}_p$ jako $F\colon K^2 \to K^2$, $F(x, y) = (x^p, y^p)$.

(a) Pokaż, że F obcina się do endomorfizmu zbioru $\{(x, y) \in K^2 \mid y^2 = f(x)\} \subseteq E(K)$. Uznajmy, że $F(0_E) = 0_E$.

(b) Pokaż, że $E(\mathbb{Z}_p) = \ker(F - \mathrm{id})$ jako podzbiory $E(\overline{\mathbb{Z}_p})$, gdzie po prawej stronie dodajemy endomorfizmy krzywej eliptycznej.

Rozwiązanie.
(a) Niech $f(x) = x^3 + ax + b$, gdzie $a, b \in \mathbb{Z}_p$. Skoro a, b leżą w $\mathbb{Z}_p$, to $a^p = a$ oraz $b^p = b$ jako elementy K. Załóżmy, że $(x_0, y_0) \in K^2$ spełniają $y_0^2 = f(x_0)$. Wtedy

$$(y_0^p)^2 = (y_0^2)^p = \left(x_0^3 + ax_0 + b\right)^p = ((x_0)^3)^p + (ax_0)^p + b^p = (x_0^p)^3 + ax_0^p + b, \tag{1.1}$$

gdzie kluczowa równość wynika z tego, że K ma charakterystykę p, więc dla dowolnych jego elementów $k_1, k_2 \in K$ zachodzi $(k_1 + k_2)^p = k_1^p + k_2^p$. Z równania (1.1) wynika, że (x_0^p, y_0^p) również spełniają równanie $y^2 = f(x)$, czego należało dowieść.
(b) Ten podpunkt polega na rozwinięciu definicji. Mianowicie $\ker(F - \mathrm{id})$ składa się z tych elementów $(x_0, y_0) \in E(\overline{\mathbb{Z}_p})$ które spełniają $(F - \mathrm{id})(x_0, y_0) = 0_E$, czyli $F(x_0, y_0) = (x_0, y_0)$. Wreszcie, mamy $F(x_0, y_0) = (x_0^p, y_0^p)$. Zatem ustaliliśmy, że $\ker(F - \mathrm{id}) \subseteq E(\overline{\mathbb{Z}_p})$ składa się dokładnie z tych $(x_0, y_0) \in E(\overline{\mathbb{Z}_p})$, dla których $x_0^p = x_0$ oraz $y_0^p = y_0$.
Z twierdzenia Bezout, w ciele $K = \overline{\mathbb{Z}_p}$ równanie $x^p = x$ ma co najwyżej p rozwiązań. Ponadto dla każdego elementu $a \in \mathbb{Z}_p \subseteq K$ zachodzi $a^p = a$, czyli elementy $\mathbb{Z}_p$ są jego rozwiązaniami. To pokazuje, że element $a \in K$ spełnia $a^p = a$ wtedy i tylko wtedy, gdy $a \in \mathbb{Z}_p$. To kończy dowód.