Algebra 2R lista 3

Wiktor Kuchta

1/5e

Niech $\Phi\colon \mathbb{C}(X) \to \mathbb{C}(X)$, $\Phi(f) = f\left(\frac{X}{X-1}\right)$. Aby to była poprawna definicja, musimy pokazać, że Φ jest określone na całej dziedzinie, tzn. $\frac{X}{X-1}$ nie jest pierwiastkiem żadnego niezerowego wielomianu $w \in \mathbb{C}[X]$. Funkcja $z \mapsto \frac{z}{z-1}$ jest inwolucją, a zatem bijekcją $\mathbb{C} \setminus \{1\}$. Zatem $w\left(\frac{X}{X-1}\right)$ ma dokładnie tyle samo różnych pierwiastków co w, być może poza 1. To oznacza, że $w\left(\frac{X}{X-1}\right)$ jest zerem dokładnie wtedy, co w.

Pokazaliśmy, że homomorfizm ewaluacji $\varphi_{\frac{X}{X-1}}\colon \mathbb{C}[X] \to \mathbb{C}(X)$ jest różnowartościowy, zatem rozszerza się on do jedynego homomorfizmu z ciała ułamków $\mathbb{C}[X]$. Tym homomorfizmem jest dokładnie Φ. Powyższy argument z inwolucją pokazuje też, że $\Phi(\Phi(f)) = f$, zatem Φ jest automorfizmem.

Wiemy z 1/5d, że każdy $W \in \mathbb{Q}[X_1, X_2]$ zerujący się w (X^3, X^2) jest podzielny przez $X_1^2 - X_2^3$.

Weźmy wielomian $W \in \mathbb{Q}[X_1, X_2]$ taki, że $W\left(\frac{X^3}{(X-1)^3}, \frac{X^2}{(X-1)^2}\right) = 0$. Wtedy skoro Φ jest identycznością na $\mathbb{Q}$, to mamy

$$\begin{aligned}\Phi\left(W\left(\frac{X^3}{(X-1)^3}, \frac{X^2}{(X-1)^2}\right)\right) &= W\left(\Phi\left(\frac{X^3}{(X-1)^3}\right), \Phi\left(\frac{X^2}{(X-1)^2}\right)\right)\\ &= W(X^3, X^2) = 0.\end{aligned}$$

Zatem W jest podzielny przez $X_1^2 - X_2^3$.

3/3aD

Załóżmy, że $K \supset F(p)$ jest skończonym rozszerzeniem ciała $F(p)$, charakterystyki p. Załóżmy, że $a \in K$ jest pierwiastkiem pierwotnym stopnia m z jedynki.

Pierwotnym pierwiastkom stopnia m w $F(p^n)$ odpowiadają elementy rzędu m w $F(p^n)^*$. Rząd elementu dzieli rząd grupy, zatem takie pierwiastki istnieją tylko jeśli m dzieli $p^n - 1$.

Ustalmy najmniejsze n takie, że $m \mid p^n - 1$. Ciało $F(p)(a)$ musi być mocy co najmniej p^n, inaczej nie mogłoby ono zawierać pierwiastka pierwotnego stopnia m z jedynki.

Niech g to generator $F(p^n)^*$. Niech $r = g^{\frac{p^n-1}{m}}$, wtedy

$$\operatorname{ord}(r) = \operatorname{ord}\left(g^{\frac{p^n-1}{m}}\right) = \frac{\operatorname{ord}(g)}{\gcd\left(\frac{p^n-1}{m}, \operatorname{ord}(g)\right)} = \frac{p^n-1}{\gcd\left(\frac{p^n-1}{m}, p^n-1\right)} = \frac{p^n-1}{\frac{p^n-1}{m}} = m.$$

Potęgi $r^0, r^1, \ldots, r^{m-1}$ to wszystkie pierwiastki stopnia m z jedynki, więc wśród ich jest a. Zatem $F(p^n) = F(p)(a)$. Stopień a nad $F(p)$ to $[F(p^n) : F(p)] = n$.

3/4aD

Niech $x = \sqrt{2} + \sqrt{3}$.

$$x^2 = 5 + 2\sqrt{6}$$
$$x^2 - 5 = 2\sqrt{6}$$
$$x^4 - 10x^2 + 25 = 24$$
$$x^4 - 10x^2 + 1 = 0$$

Więc znaleźliśmy wielomian zerujący się w $\sqrt{2} + \sqrt{3}$.

$\mathbb{Q}(\sqrt{2} + \sqrt{3})$ jest podciałem $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Zauważmy, że

$$\frac{1}{\sqrt{2} + \sqrt{3}} = \frac{\sqrt{2} - \sqrt{3}}{2 - 3} = \sqrt{3} - \sqrt{2},$$

więc w $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ są $2\sqrt{3}$ i dalej $\sqrt{2}$. Zatem mamy też zawieranie w drugą stronę $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Wiemy z dowodu 1/8, że $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$. Wielomian $x^4 - 10x^2 + 1$ jest unormowany stopnia 4, zatem jest minimalny dla x nad $\mathbb{Q}$.

3/5D

Liczba

$$a = \sum_{k=1}^{\infty} 2^{-k!}$$

ma w zapis dwójkowy taki, że n-ta cyfra po przecinku jest jedynką dokładnie kiedy n jest silnią pewnej liczby.

Załóżmy, że a algebraiczna stopnia d. Weźmy $C > 0$. Niech $q_n = 2^{n!}$. Dla pewnego m mamy $q_m^{-m} < C q_m^{-d}$. Niech $p = q_m \sum_{k=1}^{m} 2^{-k!}$. Wtedy

$$a - \frac{p}{q_m} = a - \sum_{k=1}^{m} \frac{1}{2^{k!}} = \sum_{k=m+1}^{\infty} \frac{1}{2^{k!}} < \frac{1}{q_m^m},$$

bo $q_m^{-m} = 2^{-m!m}$ ma w zapisie binarnym jedynkę na $(m!m)$-tym miejscu po przecinku, a ostatnia suma ma pierwszą jedynkę dopiero na $(m+1)!$-tym miejscu po przecinku. Otrzymujemy sprzeczność z lematem Liouville'a, zatem a nie jest algebraiczna.