Wiktor Kuchta

5/1D

Załóżmy, że $\mathrm{char}(K) = p > 0$, $K \subset L$ jest rozszerzeniem algebraicznym ciał oraz $a \in L \setminus K$.

W 4/5 pokazaliśmy, że wielomian nierozkładalny nierozdzielczy f daje się zapisać jako $g(X^p)$. Wielomian g też jest nierozkładalny, więc iterując ten proces możemy otrzymać $f(X) = h(X^{p^l})$, gdzie h jest nierozkładalny rozdzielczy.

Wielomian minimalny $W_a(X)$ jest równy $h(X^{p^l})$ dla pewnego $l > 0$ i wielomianu h rozdzielczego nierozkładalnego. Zatem $h(a^{p^l}) = W_a(a) = 0$. Wielomian minimalny $W_{a^{p^l}}$ dzieli h, więc a^{p^l} rozdzielczy.

5/3aD

Załóżmy, że $a \in L$ jest algebraiczny nad K, $L = K[a]$ i $W(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$ jest wielomianem minimalnym a nad K.

Przyjmujemy, że wielomian charakterystyczny macierzy A to $\varphi_A(x) = \det(A - tI)$. Wtedy wyraz wolny tego wielomianu to $\varphi_A(0) = \det A$ i jeśli $\deg \varphi_A = n$, to współczynnik przy x^{n-1} to $(-1)^{n-1} \operatorname{tr} A$.

Stopień $[K(a) : K]$ wynosi $\deg W = n$, więc taki też jest stopień wielomianu charakterystycznego φ_{f_a}. Dla dowolnego wielomianu P mamy $P(f_a)(x) = P(a) \cdot x$, więc wielomian minimalny endomorfizmu f_a nad K to dokładnie wielomian minimalny a nad K. Wielomian minimalny f_a nad K dzieli φ_{f_a}, a skoro są tego samego stopnia, to $W = (-1)^n \varphi_{f_a}$.

Zatem $\mathrm{Tr}_{L/K} = \operatorname{tr} f_a = (-1)^n(-1)^{n-1}a_{n-1} = -a_{n-1}$, $\mathrm{N}_{L/K} = \det f_a = (-1)^n a_0$.

5/4aD

Funkcja Frobeniusa Fr należy do $G = G(F(p^n)/F(p))$, bo homomorfizmy ciał są stałe na podciałach prostych, w tym wypadku $F(p)$. Punkty stałe Fr^k to dokładnie pierwiastki $X^{p^k} - X$, których jest co najwyżej p^k. Zatem Fr^k może być identycznością na $F(p^n)$ tylko dla $k \geqslant n$, tzn. $\operatorname{ord} Fr \geqslant n$. Z drugiej strony rząd elementu dzieli rząd grupy, który z tw. Artina szacujemy $|G| = [F(p^n) : F(p^n)^G] \leqslant [F(p^n) : F(p)] = n$. Zatem $\operatorname{ord} Fr = n = |G|$ i Fr jest generatorem.