Algebra 2R lista 2

Wiktor Kuchta

2/3D

Załóżmy, że $f\colon K \to K$ jest niezerowym endomorfizmem ciała K. Niech $Fix(f) = \{x \in K : f(x) = x\}$.

Jeśli $x, y \in Fix(f)$, tzn. $f(x) = x$ i $f(y) = y$, to z homomorficzności:

- $f(0) = 0$,
- $f(1) = 1$,
- $f(-x) = -f(x) = -x$,
- $f(x^{-1}) = (f(x))^{-1} = x^{-1}$,
- $f(x + y) = f(x) + f(y) = x + y$,
- $f(xy) = f(x)f(y) = xy$,

więc $Fix(f)$ zawiera 0 i 1 oraz jest zamknięte na negację, odwracanie, dodawanie i mnożenie. Zatem $Fix(f)$ jest podciałem K.

2/4

Załóżmy, że K jest ciałem skończonym charakterystyki p.

(a)D

Niech $K = F(q)$, $q = p^k$, $f \in K[X]$ to wielomian nierozkładalny stopnia m.

Wtedy stopień rozszerzenia K o pierwiastek a wynosi $[K(a) : K] = m$, więc $a \in K(a) \cong F(q^m)$. Ciało rozkładu f nad K jest rozszerzeniem $K[X]/(f)$ (takie ciało mamy po pierwszym kroku konstrukcji ciała rozkładu). Rozszerzenie z K do $K[X]/(f)$ jest stopnia m. Wiemy, że potęgi a^k dla $0 \leqslant k < m$ są liniowo niezależne, więc $K(a)$ jest stopnia m nad K i z jedyności ciał skończonych o danej mocy $K(a) \cong K[X]/(f)$.

W $F(q^m)$ dla każdego $x \neq 0$ zachodzi $x^{q^m-1} = 1$, więc $X^{q^m-1} - 1 \in (f)$. Zatem f dzieli $X^{q^m-1} - 1$, gdzie $q^m - 1 \equiv p^{mk} - 1 \not\equiv 0 \pmod{p}$.

(b)

Mamy $n = p^0 n_1$, $p \nmid n_1$. Uwaga (3.3) mówi, że każdy pierwiastek W_n ma krotność $p^0 = 1$. Skoro f dzieli W_n, to każdy jego pierwiastek jest też jednokrotny.

2/5aD

Niech $K \subseteq L$ to ciała skończone, $|K| = p^m$, $|L| = p^n$. L jest przestrzenią wektorową nad K i $|L| = |K|^{[L:K]} = p^{m[L:K]}$, więc $n = m[L : K]$.