Algebra 2R, lista 3

Wiktor Kuchta

2/5b

Załóżmy, że $m \mid n$.

Wielomian $X^{p^n} - X$ jest rozkładalny w $L \cong \mathbb{Z}_{p^n}$, każdy element ciała jest jego pierwiastkiem. Zbiór pierwiastków $X^{p^m} - X$ jest równy $K = Fix(x \mapsto x^{p^m})$, a zatem jest ciałem zawartym w L. Wiemy, że $X^{p^m-1} - X$ ma różne pierwiastki w ciele o charakterystyce p, więc $|K| = p^m$.

Każde element ciała o mocy p^m jest pierwiastkiem $X^{p^m} - X$, więc istnieje dokładnie jedno podciało takiej mocy.

2/6

Załóżmy nie wprost, że istnieje wielomian nierozkładalny $f \in F[X]$ stopnia $m > 1$. Należy on do $K = F(p^{n!})[X]$ dla pewnego n. Wielomian f dzieli $w = X^{p^{n!m}} - X$. Pierwiastki w to ciało $Fix(x \mapsto x^{p^{n!m}})$ mocy $p^{n!m}$ zawarte w pewnym $F(p^{k!}) \subset F$. Skoro w się rozkłada na czynniki liniowe w F, to f także. Sprzeczność.

2/7

Funkcja Frobeniusa f jest automorfizmem każdego z podciał $F(p^{n!})$. Każdy $x \in F$ należy do pewnego $F(p^{n!})$, więc $f^{-1}(x) \in F(p^{n!}) \subseteq F$.

Dla każdego $x \in F(p^n)$ mamy $f^n(x) = x^{p^n} = x$, więc $x \in Fix(f^n)$, czyli $F(p^n) \subseteq Fix(f^n)$. Zbiór $Fix(f^n)$ to dokładnie pierwiastki $x^{p^n} - x$, których jest co najwyżej p^n. Zatem $F(p^n) = Fix(f^n)$.