Algebra 2R, lista 4

Wiktor Kuchta

4/1

Pierwiastki F_m to dokładnie m-te pierwiastki pierwotne z jedynki, tzn.

$$F_m(x) = \prod_{\substack{1\leqslant k\leqslant m \\ \gcd(k,m)=1}} \left(x - \exp(2\pi i\frac{k}{m})\right).$$

Łatwo sprawdzić, że

$$\begin{aligned}
F_1(x) &= x - 1,\\
F_2(x) &= x + 1,\\
F_3(x) &= (x - \exp(\tfrac{4}{3}\pi i))(x - \exp(-\tfrac{4}{3}\pi i)) = x^2 - 2x\cos\tfrac{4\pi}{3} + 1\\
&= x^2 + x + 1.
\end{aligned}$$

Natomiast dla $m > 1$

$$F_{2^m}(x) = \prod_{1\leqslant k\leqslant 2^{m-1}} \left(x - \exp(2\pi i\frac{2k-1}{2^m})\right),$$

bo $\{1, 3, \ldots, 2^m - 1\}$ to wszystkie liczby naturalne $\leqslant 2^m$ względnie pierwsze z 2^m. Zauważmy, że

$$\exp(2\pi i\frac{2k-1}{2^m})^{2^{m-1}} = \exp(\pi i\frac{2k-1}{2^{m-1}}2^{m-1}) = \exp(\pi i(2k-1)) = \exp(-\pi i) = -1,$$

czyli 2^m-te pierwiastki pierwotne z 1 to 2^{m-1}-e pierwiastki z -1. Jest ich 2^{m-1}, więc są to wszystkie takie pierwiastki i $F_{2^m}(x) = x^{2^{m-1}} + 1$. W szczególności

$$\begin{aligned}
F_4(x) &= x^2 + 1,\\
F_8(x) &= x^4 + 1,\\
F_{16}(x) &= x^8 + 1.
\end{aligned}$$

Ze wzoru

$$W_m(x) = x^m - 1 = \prod_{d|m} F_d(x)$$

otrzymujemy

$$\begin{aligned}
F_{15}(x) &= \frac{x^{15}-1}{F_1(x)F_3(x)F_5(x)} = \frac{(x^5)^3 - 1^3}{F_3(x)(x^5-1)} = \frac{x^{10}+x^5+1}{x^2+x+1}\\
&= x^8 - x^7 + x^5 - x^4 + x^3 - x + 1.
\end{aligned}$$

Dla homomorfizmu ilorazowego $j\colon \mathbb{Z} \to \mathbb{Z}_3$, $j(F_m)$ to wielomian F_m, w którym nałożono j na współczynniki.

Wielomiany F_1 i F_2 są liniowe, a więc nierozkładalne. Można sprawdzić, że $F_4(x) = x^2 + 1$ nie ma pierwiastków w $\mathbb{Z}_3$, a może się rozłożyć tylko na czynniki liniowe, więc jest nierozkładalny.

Niech a to 2^m-ty pierwotny pierwiastek z jedynki w pewnym rozszerzeniu $\mathbb{Z}_3$. Element a generuje rozszerzenie stopnia n, gdzie n to najmniejsza liczba taka, że $2^m | 3^n - 1$. Dla $m = 3$ jest to $n = 2$, dla $m = 4$ jest to $n = 4$. W obu przypadkach wielomian minimalny a nad $\mathbb{Z}_3$ ma stopień mniejszy od stopnia F_{2^m}, więc są one rozkładalne.

Mamy $x^{15} - 1 = (x^5 - 1)^3$, więc pierwiastki F_{15} w $\hat{\mathbb{Z}}_3$ są pierwiastkami $x^5 - 1$. Zatem wielomian minimalny każdego pierwiastka F_{15} nad $\mathbb{Z}_3$ ma stopień co najwyżej $5 < \deg F_{15} = 8$. Możemy podzielić F_{15} przez ten wielomian minimalny, otrzymując nietrywialny rozkład F_{15} nad $\mathbb{Z}_3$.

4/3

Załóżmy, że $[L : K] = 2$, $a \in L \setminus K$. Mamy $[L : K(a)][K(a) : K] = 2$ i stąd $[K(a) : K] = 2$, bo inaczej $K(a)$ byłoby równe K. Zatem $L = K(a)$ jest algebraicznym rozszerzeniem K. Element a ma wielomian minimalny W_a stopnia 2 nad K. Ale $W_a(x) = (x - a)g(x)$, gdzie g jest liniowy z pierwiastkiem w L, więc W_a rozkłada się na czynniki liniowe. Zatem z rozszerzenie $K \subseteq L$ jest normalne.

4/5

Załóżmy, że $K \subset L \subset \hat{K}$ i rozszerzenie $K \subset L$ jest radykalne.

Każdy homomorfizm, który jest identycznością na L, jest w szczególności identycznością na K, więc $G(\hat{K}/K) \supseteq G(\hat{K}/L)$.

Każdy automorfizm $f\colon \hat{K} \to \hat{K}$ stały na K permutuje pierwiastki wielomianów z $K[X]$. Wielomian minimalny nad K elementu radykalnego nad K ma tylko jeden pierwiastek, więc jest on zachowywany przez f. Każdy element L jest radykalny nad K, więc każdy taki f jest identycznością na L. Zatem $G(\hat{K}/K) \subseteq G(\hat{K}/L)$.