Zadania o ciałach skończonych

Wszystkie ciała w poniższych zadaniach są skończone charakterystyki p. Patrz [Browkin, str 81]

Jeśli $a \in L$, $K \subset L$ i nie ma właściwych podciał L zawierających a i K, to piszemy $L = K(a)$.

1 Jeśli $K_1 \subset K_2$, to $|K_2| = |K_1|^d$.

2 Jeśli K jest ciałem, to $|K| = p^n$ dla pewnej liczby pierwszej.

3 Jeśli $|K| = q$, to dla dowolnego niezerowego elementu $a \in K$ mamy $a^{q-1} = 1$. Grupa multiplikatywna ciała jest cykliczna.

4 Jeśli K jest skończonym ciałem, to istnieje element ciała a nie należący do właściwego podciała, tzn $K = \mathbb{F}_p(a)$. (Za a można wziąć generator grupy cyklicznej.)

5 W ciele q-elementowym wielomian $x^q - x$ rozkłada się na różne czynniki liniowe.

6 Jeśli $|K_1| = p^m$, $|K_2| = p^n$, $K_1 \subset K_2$, to $m|n$.

7 Jeśli $|K_1| = p^m$, $|K_2| = p^n$ i $m|n$ to isnieje włożenie $K_1 \to K_2$.

8 Jeśli $|K_1| = |K_2| = p^n$ to $K_1 \simeq K_2$.

9 Jeśli K_1 i K_2 są podciałami ciała L i $|K_2| = |K_1|^d$, to $K_1 \subset K_2$.

10 Jeśli K_1 i K_2 są równolicznymi podciałami ciała L to $K_1 = K_2$.

11 Niech K ma p^n elementów. Przekształcenie $a \mapsto a^p$ jest homomorfizmem $K \to K$ (oznaczane ϕ od Frobeniusa).

12 Niech K ma p^n elementów. Zbiór rozwiązań równania $x^{p^k} - x$ jest podciałem K. Jeśli wielomian $x^{p^k} - x$ rozkłada się na czynniki liniowe w K, to k dzieli n. Wywnioskować, że dla każdego k istnieje ciało o p^k elementach.

13 Wszystkie podciała w K są postaci $K^{\phi^k} = \{a \in K \mid \phi^k(a) = a\}$. Niech $|\mathbb{F}_p(a)| = p^n$. Wykazać

$$\phi^k(a) = a \iff n|k.$$

14 Niech K ma p^n elementów i $n = st$, gdzie s i t są względnie pierwsze. Dane elementy $a, b \in K$ takie, że $|\mathbb{F}_p(a)| = p^s$ i $|\mathbb{F}_p(b)| = p^t$. Wtedy $\mathbb{F}_p(a+b) = K$. (Zbadać własności wielomianu $f_k(x) = \phi^k(x) - x$.)

15 Niech K ma p^n elementów. Rozłóżmy wielomian $x^{p^n} - x$ na nierozkładalne czynniki w $\mathbb{F}_p[x]$. Każdy element K jest pierwiastkiem dokładnie jednego czynnika. Jeśli $\mathbb{F}_p(a) = K$, to czynnik, którego a jest pierwiastkiem ma stopień n.

16 Niech K ma p^n elementów. Rozłóżmy wielomian $x^{p^n} - x$ na nierozkładalne czynniki w $\mathbb{F}_p[x]$. Jeden z czynników jest stopnia n i nie ma czynników wyższego stopnia.

17 Niech n_i będzie ciągiem liczb naturalnych takich, że $n_i | n_{i+1}$ oraz $\forall n \in \mathbb{N}\ \exists i \in \mathbb{N}\ n | n_i$. Niech K_i będzie ciałem o p^{n_i} elementach. Ustalmy włożenia $K_i \hookrightarrow K_{i+1}$. Niech $K = \bigcup K_i$. Udowodnić, że K jest algebraicznie domknięte.

18 Opisać grupę automorfizmów domknięcia algebraicznego $\mathbb{F}_p$.