Dowód istnienia ciał $\mathbb{Z}_{p^n}$ — w zadaniach

Niech $K[\alpha]$ oznacza ciało K z dorzuconym elementem α, wszystkimi jego potęgami oraz sumami wszystkich tak otrzymanych elementów.

Konstrukcja ciała $\mathbb{Z}_9$

Na ćwiczeniach było powiedziane, że ciało $\mathbb{Z}_9$ definiujemy jako $\mathbb{Z}_3[\alpha]$, gdzie α spełnia warunek $\alpha^2 = -1$. Teraz sprawdźmy po kolei, że tak jest rzeczywiście dobrze.

1. Udowodnij, że wewnątrz zbioru $\mathbb{Z}_3[\alpha]$ można dodawać i mnożyć. Wywnioskuj prawdziwość wszystkich aksjomatów, na razie oprócz aksjomatu o elemencie odwrotnym.

2. Udowodnij, że $\mathbb{Z}_3[\alpha]$ ma dokładnie 9 elementów.

3. Udowodnij, że jeśli $a \neq 0$ lub $b \neq 0$, to $(a + b\alpha)(a - b\alpha)$ jest niezerowym elementem $\mathbb{Z}_3$.

4. Udowodnij, że $\mathbb{Z}_3[\alpha]$ jest ciałem.

Konstrukcja ciała $\mathbb{Z}_{25}$

5. Niech α będzie dodatkowym elementem spełniającym warunek $\alpha^2 = -1 \in \mathbb{Z}_5$. Udowodnij, że $\mathbb{Z}_5[\alpha]$ **nie** jest ciałem! *(Wskazówka: czy w tym przypadku teza zadania 3 jest prawdziwa?)*

6. Wykaż, że jeśli $c \in \mathbb{Z}_5$ nie jest kwadratem żadnego elementu z $\mathbb{Z}_5$, oraz jeśli dołożymy do $\mathbb{Z}_5$ element β o własności $\beta^2 = c$, to w otrzymanym zbiorze $\mathbb{Z}_5[\beta]$ teza zadania 3 jest prawdziwa.

7. Udowodnij, że $\mathbb{Z}_5[\beta]$ jest ciałem (25-elementowym), jeśli $\beta^2 = 2 \in \mathbb{Z}_5$.

Konstrukcja ciała $\mathbb{Z}_{p^2}$

8. *(Uogólnienie zadania 1)* Udowodnij, że dodawać i mnożyć można wewnątrz dowolne zbioru postaci $K[\alpha]$. Wywnioskuj prawdziwość wszystkich aksjomatów oprócz tego o elemencie odwrotnym.

9. Udowodnij, że dla dowolnej liczby pierwszej p istnieje element $c \in \mathbb{Z}_p$ niebędący kwadratem żadnego elementu $\mathbb{Z}_p$.

10. Udowodnij, że dla dowolnej liczby pierwszej p istnieje ciało mające dokładnie p^2 elementów.

Ciąg dalszy nastąpi.