Lista 18+x (ciała skończone)

Ciałem nazywamy zbiór F wraz z wyróżnionymi elementami $0, 1 \in F$ oraz działaniami $\cdot, +$ takimi że $(F, +, 0)$ oraz $(F \setminus \{0\}, \cdot, 1)$ są przemiennymi grupami (tj. działania są przemienne i łączne, 0 i 1 są elementami neutralnymi dodawania i mnożenia odpowiednio, oraz każdy element ma element przeciwny i (za wyjątkiem zera) każdy element ma element odwrotny) i zachodzi prawo rozdzielności, tj. $(a + b) \cdot c = a \cdot c + b \cdot c$. Przykłady ciał to np. liczby rzeczywiste lub wymierne ze zwykłym dodawaniem i mnożeniem.

Zadanie 1. Niech p będzie liczbą pierwszą. Przekonaj się, że zbiór liczb $\{0, 1, \ldots, p-1\}$ z dodawaniem i mnożeniem modulo p stanowi ciało (spróbuj najpierw dla $p = 2, 3, 5$). Ciało to nazywamy ciałem p-elementowym i oznaczamy np. przez $\mathbf{F}_p$.

Zadanie 2. Sprawdź, że jeżeli $a, b \in \mathbf{F}_p$, to $(a + b)^p = a^p + b^p$.

Zadanie 3. Sprawdź że jeżeli F jest ciałem skończonym, to istnieje taka liczba naturalna n, że $n \cdot 1 = 1 + 1 + \ldots + 1 = 0$ (jedynka występuje n razy).

Zadanie 4. Sprawdź, że jeżeli F jest ciałem skończonym, to najmniejsza liczba n taka jak w poprzednim zadaniu jest liczbą pierwszą. Liczbę tę nazywamy *charakterystyką ciała* F.

(Wskazówka: załóżmy że $(pq) \cdot 1 = 0$; ile to jest $(p \cdot 1) \cdot (q \cdot 1)$?)

Zadanie 5. Załóżmy że $a \in F$ i F jest charakterystyki p. Jaki jest rząd a w $(F, +, 0)$? (Wskazówka: $a + a + \ldots + a = (1 + 1 + \ldots + 1) \cdot a$.)

Zadanie 6. Przypomnij sobie, że jeżeli G jest grupą skończoną i q jest liczbą pierwszą, która dzieli rząd G, to G ma element rzędu q.

Zadanie 7. Wywnioskuj z poprzedniego zadania, że jeżeli F jest ciałem skończonym charakterystyki p, to F ma p^k elementów dla pewnego k.

Zadanie 8. Skonstruuj ciało o 4 elementach. (Wskazówka: zacznij od zbioru $\{0, 1, a, b\}$. Narysuj tabelkę działania dodawania i mnożenia i uzupełnij ją – jest tylko jeden sposób, żeby to zrobić.)

Zadanie 9. Rozważmy $\mathbf{F}_3[x]$. Co dostaniemy, jeżeli rozważymy dodawanie i mnożenie tych wielomianów modulo x?

Zadanie 10. Przekonaj się, że $f = x^2 + x + 1 \in \mathbf{F}_2[x]$ nie ma pierwiastków. Wywnioskuj z tego, że jest nierozkładalny (tzn. nie istnieją wielomiany f_1, f_2 takie że $f_1 \cdot f_2 = f$).

Przekonaj się, że elementy $F_2[x]$ stopnia co najwyżej 1, z dodawaniem i mnożeniem modulo f to ciało o czterech elementach.

Zadanie 11. Niech $(R, +, \cdot, 0, 1)$ będzie pierścieniem, tzn. strukturą podobną jak ciało, tylko że być może bez elementów odwrotnych (przykład: liczby $0, \ldots, 5$ z dodawaniem i mnożeniem modulo 6).

Pokaż, że jeżeli R nie ma dzielników zera, tzn. niezerowych elementów a, b takich że $a \cdot b = 0$, i jest skończony, to charakterystyka R jest pierwsza (patrz zadanie 5.).

Sprawdź, że jeżeli R nie ma dzielników zera, to dla każdego $a \neq 0$ funkcja $x \mapsto a \cdot x$ jest różnowartościowa.

Wywnioskuj stąd, że jeżeli R jest skończony bez dzielników zera, to jest ciałem.

Zadanie 12. Przypomnij sobie, że $f = x^2 + 1 \in \mathbf{F}_3[x]$ nie ma pierwiastków, a więc jest nierozkładalny.

Spróbuj się przekonać, że wielomiany stopnia co najwyżej 1 z dodawaniem i mnożeniem modulo f tworzą ciało o 9 elementach.