Algebra liniowa 2 R, Konwersatorium 1 (ciała skończone)

Definicja. Jeżeli K jest ciałem, to jego *charakterystyka* to najmniejsza taka liczba naturalna n, że $n \cdot 1 := \underbrace{1+1+\ldots+1}_{n} = 0$, lub 0, jeżeli taka liczba nie istnieje.

Na przykład charakterystyka $\mathbf{Q}, \mathbf{R}$ i $\mathbf{C}$ to 0, a charakterystyka ciała $\mathbf{F}_p$ to p.

Zadanie 1. Pokaż że charakterystyka ciała zawsze jest liczbą pierwszą.

Zadanie 2. Załóżmy że $K \subseteq L$ jest rozszerzeniem ciał (tzn. K i L są ciałami i działania w K są obcięciami działań w L do K).

Uzasadnij że L jest przestrzenią liniową nad K.

Zadanie 3. Załóżmy że K jest ciałem charakterystyki p. Pokaż, że K jest przestrzenią liniową nad $\mathbf{F}_p$.

Zadanie 4. Wywnioskuj z poprzednich zadań, że jeżeli K jest ciałem skończonym, to K ma p^k elementów dla pewnej liczby pierwszej p i pewnej dodatniej liczby całkowitej k. (*Wskazówka: utożsam $1_K \in K$ z $1 \in \mathbf{F}_p$ dla odpowiednio dobranego p, a następnie wybierz bazę K nad $\mathbf{F}_p$.*)

Zadanie 5. Załóżmy że R jest *dziedziną*, to znaczy zbiorem z działaniami $+, \cdot$ spełniającymi aksjomaty ciała, z wyjątkiem aksjomatu o odwrotności, ale takim że $xy = 0$ implikuje $x = 0$ lub $y = 0$.

a) Pokaż że przy ustalonym $x \neq 0$, funkcja $y \mapsto xy$ jest różnowartościowa (*wskazówka: rozważ y_1, y_2 takie że $xy_1 = xy_2$* i odejmij stronami).
b) Zakładając że R jest skończony, pokaż że funkcja z poprzedniego podpunktu jest „na”.
c) Wywnioskuj stąd, że każda skończona dziedzina jest ciałem.

Uwaga: tak naprawdę trzeba zakładać przemienności mnożenia! Tzw. małe twierdzenie Wedderburna mówi, że (w skończonym przypadku!) przemienność wynika z pozostałych aksjomatów. Ale jego dowód jest trudniejszy.

Zadanie 6. Znajdź ciało czteroelementowe (tzn. określ na zbiorze czteroelementowym działania dodawania i mnożenia tak, żeby otrzymać ciało, na przykład zadając tabelkę działań).

Zadanie 7. Sprawdź że wielomian $x^3 + x + 1$ jest nierozkładalny nad ciałem $\mathbf{F}_3$ (tzn. że nie ma niestałych wielomianów $P(x)$ i $Q(x)$ takich że $P \cdot Q = x^3 + x + 1$).

Wskazówka: zauważ, że wystarczy sprawdzić, że nie ma pierwiastków.

Zadanie 8. Wywnioskuj z poprzedniego zadania, że zbiór $\{ ax^2 + bx + c \mid a, b, c \in \mathbf{F}_3 \}$ z działaniami określonymi tak, że $x^3 + x + 1 = 0$ (czyli $x^3 = -x - 1 = 2x + 2$) jest ciałem o $3^3 = 27$ elementach.

Zadanie 9. Naśladując dwa poprzednie zadania, dla każdej liczby pierwszej p znajdź ciało o p^p elementach.