Algebra abstrakcyjna
Lista 11

1. Udowodnić, że jeśli n jest liczbą złożoną, to wielomian $1 + x + \ldots + x^{n-1}$ jest rozkładalny w $\mathbb{Z}_2[x]$. A jeśli n jest liczbą pierwszą, to czy wielomian ten jest nierozkładalny w $\mathbb{Z}_2[x]$?

2. Dla liczb pierwszych p, q niech K będzie ciałem rozkładu wielomianu $x^p - q$ nad $\mathbb{Q}$. Udowodnić, że pierwiastek pierwotny stopnia p z jedynki należy do K oraz $[K : \mathbb{Q}] = p(p-1)$.

3. W ciele K rozważamy podciało generowane przez 1. (Jest to najmniejsze podciało zawarte w K). Wykazać, że jeśli jest ono nieskończone, to jest izomorficzne z $\mathbb{Q}$, a jeśli jest skończone, to jest izomorficzne z $\mathbb{Z}_p$, gdzie p jest liczbą pierwszą.

   Takie minimalne podciała nazywamy **ciałami prostymi**. Liczbę p nazywamy **charakterystyką ciała**. W przypadku $K \supseteq \mathbb{Q}$ przyjmujemy $\mathrm{char}(K) = 0$.

4. Wykazać, że jeśli F jest ciałem skończonym i $\mathrm{char}F = p$, to $|F| = p^n$, gdzie $n = [F : \mathbb{Z}_p]$.

5. Podać przykład ciała nieskończonego charakterystyki $p > 0$.

6. Wykazać, że ciele K wielomian stopnia $n \geqslant 1$ ma co najwyżej n pierwiastków.

7. Wykazać, że w ciele skończonym, dla dowolnej liczby n, istnieje co najwyżej n elementów rzędu będącego dzielnikiem n.

8. Udowodnić, że grupa multiplikatywna ciała skończonego jest cykliczna.

   (*Wskazówka* Korzystając z twierdzenia o strukturze grup abelowych, zauważyć, że jeśli grupa abelowa nie jest cykliczna, to ma podgrupę postaci $\mathbb{Z}_p \oplus \mathbb{Z}_p$, która ma p^2 elementów rzędu dzielącego p; skorzystać z poprzedniego zadania)

9. Generator grupy multiplikatywnej ciała skończonego nazywa się jego **elementem pierwotnym**. Ile elementów pierwotnych ma ciało 9-elementowe? Ile elementów pierwotnych ma ciało 32-elementowe?

10. Udowodnić że w ciele charakterystyki $p > 0$, dla dowolnego $n \geqslant 1$, zachodzi równość

$$(x + y)^{p^n} = x^{p^n} + y^{p^n}.$$

11. Wykazać, że w ciele q-elementowym, $q = p^n$, wielomian $x^{q-1} - 1$ ma rozkład na czynniki liniowe. Udowodnić wzór Wilsona: dla liczby pierwszej p

$$(p-1)! \equiv -1 \pmod{p}.$$

12. Wykazać, że algebraiczne domknięcie ciała skończonego jest nieskończone.

13. Wykazać, że jeśli p jest liczbą pierwszą, to dla każdego $n \geqslant 1$ istnieje wielomian nierozkładalny w $\mathbb{Z}_p[x]$, (*Wskazówka*: Wykorzystać odpowiednio fakt z Zad. 8).

14. Wyznaczyć wszystkie wielomiany stopnia 2 nierozkładalne w $\mathbb{Z}_3[x]$.

15. Wielomian $x^8 - 1$ rozłożyć na czynniki nierozkładalne w pierścieniu $\mathbb{Z}_p[x]$.

16. Na podstawie Zadania 10 z Listy 9, podać konstrukcję ciała 9-elementowego. Każdy element ciała przedstawić w dwóch postaciach: jako potęgi wybranego elementu pierwotnego i jako kombinacji liniowej elementów wybranej bazy; (takie przedstawienie wyznacza jednocześnie działania mnożenia i dodawania w ciele).

    Podać drugą konstrukcję wybierając inny wielomian i pokazać że otrzymane ciała są izomorficzne.

17. Niech K będzie ciałem i $f(x) \in K[x]$. Niech a, b będą dowolnymi pierwiastkami wielomianu $f(x)$. Udowodnić, że jeśli $f(x)$ jest nierozkładalny w $K[x]$, to między ciałami $K(a)$ i $K(b)$ istnieje naturalny izomorfizm będący tożsamością na elementach ciała K i przekształacający a na b.

18. Udowodnić, że jeśli dwa skończone ciała mają tę samą ilość elementów, to są izomorficzne.

    Wynika stąd, że z dokładnością do izomorfizmu istnieje dokładnie jedno ciało p^n-elementowe, dla ustalonej liczby $n \geqslant 1$ i liczby pierwszej p. Takie ciało nazywa się **ciałem Galois** rzędu $q = p^n$ i oznaczane jest symbolem $\mathrm{GF}(p, n)$ lub $\mathbb{F}_q$.