

Zestaw 4¹

Zadanie 1.

Niech $K=\mathbf{Q}(\xi_n)$ oraz niech $\Phi_n(x) \in \mathbf{Z}[x]$ będzie wielomianem minimalnym dla ξ_n nad $\mathbf{Q}$.

- (a) Rozważmy rozkład $x^n-1 = \Phi_n(x)q(x)$ na iloczyn wielomianów unormowanych, gdzie $q(x) \in \mathbf{Z}$. Dowieść, że $q(x)$ jest iloczynem wielomianów unormowanych nad $\mathbf{Z}$, które dzielą x^d-1 w $\mathbf{Z}[x]$ dla pewnych dzielników właściwych $d|n$.
- (b) Korzystając z (a) dowieść, że w każdym ciele k takim, że $\text{char}(k)$ nie dzieli n (czyli x^n-1 jest wielomianem rozdzielczym nad k) pierwiastkami $\Phi_n(x)$ w k są dokładnie te pierwiastki pierwotne z jedynki stopnia n , które należą do ciała k .
- (c) Niech p będzie liczbą pierwszą, która nie dzieli n (w szczególności p nie dzieli wyróżnika Δ_K) i dlatego $p\mathbf{Z}[\xi_n] = \wp_1\wp_2 \dots \wp_g$ dla różnych ideałów pierwszych $\wp_i$. Korzystając z (b) dla ciał skończonych dowieść, że każde z ciał reszt $\mathbf{Z}[\xi_n]/\wp_i$ jest izomorficzne z $\mathbf{F}_{p^f}$, gdzie f jest rzędem p modulo n (tzn. $n|(p^f-1)$ z minimalnym dodatnim f). Wywnioskować z tego, że $g = \phi(n)/f$ oraz skojarzyć ideały $\wp_i$ z czynnikami nierozkładalnymi wielomianu $\Phi_n(x)$ modulo p .
- (d) Wyznaczyć rozkład prymarny ideału $p\mathbf{Z}[\xi_{12}]$ dla $p = 5, 7, 11, 13$.

Zadanie 2. (rzęd wzrostu grupy klas ciała kwadratowego)

- (a) Niech p będzie liczbą pierwszą, która przystaje do 5 modulo 12. Wykazać, że jeśli $p > 3^n$, to grupa klas ciała $K=\mathbf{Q}(\sqrt{-p})$ zawiera element rzędu większego od n . W szczególności, wynika z tego (i z twierdzenia Dirichleta o liczbach pierwszych w ciągach arytmetycznych), że liczba klas ciała kwadratowego urojonego może być dowolnie duża. **Wskazówka.** Wystarczy rozważyć rozkład prymarny ideału (3) w $\mathcal{O}_K$.
- (b) Niech $d \in \mathbf{Z}_{>0}$ będzie wolna od kwadratu, parzysta i niech $d=a^n-1$ dla pewnych liczb całkowitych $a, n \geq 2$. Wykazać, że wtedy w pierścieniu $\mathbf{Z}[\sqrt{-d}]$ zachodzi równość $(1+\sqrt{-d})=I^n$ dla pewnego ideału I . Dowieść, że klasa ideału I ma rząd równy n w grupie klas ciała $\mathbf{Q}(\sqrt{-d})$.

Zadanie 3. (Euler)

Niech $p=4n-1 \geq 11$ będzie liczbą pierwszą

- (1) Dowieść, że liczba klas ciała $\mathbf{Q}(\sqrt{-p})$ jest równa jeden, wtedy i tylko wtedy, gdy dla każdego całkowitego $0 \leq a \leq n-2$ liczba a^2+a+n jest liczbą pierwszą.

¹Rozwiązując zadania należy korzystać z notatek z wykładu i ćwiczeń. Współpraca jest dopuszczalna, a nawet zalecana, jednakże rozwiązania powinny być opisane własnymi słowami.

- (2) Znaleźć wielomian $f(t) \in \mathbf{Z}[t]$ taki, że $f(a)$ jest liczbą pierwszą dla kolejnych czterdziestu wartości całkowitych a .

Zadanie 4. (zadanie dla pana Bazylego Klockiewicza)

- (a) Niech będą dane macierze kwadratowe $A = [a_{ij}] \in M_{m,m}(K)$ i $B = [b_{ij}] \in M_{n,n}(K)$ o współczynnikach w dowolnym ciele K . Definiujemy iloczyn tensorowy $A \otimes B \in M_{mn,mn}(K)$ macierzy A i B jako macierz blokową

$$\begin{bmatrix} Ab_{11} & Ab_{12} & \dots & Ab_{1n} \\ Ab_{21} & Ab_{22} & \dots & Ab_{2n} \\ \vdots & \vdots & & \vdots \\ Ab_{n1} & Ab_{n2} & \dots & Ab_{nn} \end{bmatrix}.$$

Sprawdzić, że jeżeli $C \in M_{m,m}(K)$ oraz $D \in M_{n,n}(K)$, to $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$. Wyprowadzić wzór $\det(A \otimes B) = (\det A)^n (\det B)^m$.

- (b) Niech K i L będą ciałami liczbowymi stopni m i n , odpowiednio i takimi, że $(\Delta_K, \Delta_L) = 1$. Dowieść, że wtedy $\Delta_{KL} = \Delta_K^n \Delta_L^m$. Niech

$$\delta(M) = \frac{\log |\Delta_M|}{[M : \mathbf{Q}]}.$$

Wykazać, że dla ciał K i L z tego zadania $\delta(KL) = \delta(K) + \delta(L)$.

- (c)* Niech $K = \mathbf{Q}(\xi_m)$ będzie m -tym ciałem cyklotomicznym. Korzystając z (a) i z (b) oraz z twierdzeń z wykładu wyprowadzić wzór na wyróżnik ciała K

$$\Delta_K = \frac{(-1)^{\phi(m)} m^{\phi(m)}}{\prod_{p|m} p^{\frac{\phi(m)}{p-1}}}.$$

Zadanie 5. Niech p będzie liczbą pierwszą.

- (a) Niech $u \in \mathbf{Z}$ będzie liczbą względnie pierwszą z p i niech $\Lambda \subset \mathbf{Z}^2$ będzie kratą w $\mathbf{R}^2$ złożoną z wszystkich par $(a, b) \in \mathbf{Z}^2$ takich, że $b \equiv au \pmod{p}$. Wykazać, że $\text{vol}(\mathbf{R}^2/\Lambda) = p$.
- (b) Załóżmy, że $u^2 + v^2 \equiv -1 \pmod{p}$ i niech $\Lambda \subset \mathbf{Z}^4$ będzie kratą w $\mathbf{R}^4$ złożoną z wszystkich czwórek $(a, b, c, d) \in \mathbf{Z}^4$ takich, że $c \equiv ua + vb \pmod{p}$ oraz $d \equiv ub - va \pmod{p}$. Wykazać, że wtedy $\text{vol}(\mathbf{R}^4/\Lambda) = p^2$.

Zadania dodatkowe

Zadanie 6.

Dla liczby całkowitej $m \geq 2$ symbolem $\mathbf{Q}(\xi_m)^+$ oznaczmy podciało w $\mathbf{Q}(\xi_m)$, które odpowiada podgrupie $\{1, -1\}$ grupy Galois $G(\mathbf{Q}(\xi_m)/\mathbf{Q}) = (\mathbf{Z}/m)^\times$. Pokazać, że $\mathbf{Q}(\xi_m)^+ = \mathbf{Q}(\xi_m + \xi_m^{-1})$ oraz, że każde zanurzenie ciała $\mathbf{Q}(\xi_m)^+$ w $\mathbf{C}$ ma obraz zawarty w $\mathbf{R}$. Ciało $\mathbf{Q}(\xi_m)^+$ nazywamy *maksymalnym podciałem rzeczywistym w $\mathbf{Q}(\xi_m)$* . Dowieść, że pierścieniem liczb całkowitych ciała $\mathbf{Q}(\xi_m)^+$ jest $\mathbf{Z}[\xi_m + \xi_m^{-1}]$.

Zadanie 7.

Niech będzie dana macierz kwadratowa $A \in M_{n,n}(\mathbf{R})$. Rozważmy n form liniowych $L_i(x) = \sum_{j=1}^n a_{ij}x_j$ dla $x = (x_1, x_2, \dots, x_n) \in \mathbf{R}^n$ oraz $1 \leq i \leq n$. Niech będą dane dodatnie liczby rzeczywiste $\lambda_1, \lambda_2, \dots, \lambda_n$ takie, że $\lambda_1 \lambda_2 \dots \lambda_n \geq |\det A| > 0$. Wykazać, że istnieją liczby całkowite $y_1, y_2, \dots, y_n$ nie wszystkie równe zero i takie, że $|L_i(y_1, y_2, \dots, y_n)| \leq \lambda_i$ dla każdego $1 \leq i \leq n$.

Zadanie 8*

Niech $\{F_n\}_n$ będzie ciągiem Fibonacciego, tzn. $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$, dla $n > 1$. Niech p będzie liczbą pierwszą. Mówimy, że $d \in \mathbf{Z}_{>0}$ jest okresem ciągu Fibonacciego modulo p , jeśli dla wszystkich $m, n \geq 0$, takich, że $n \equiv m \pmod d$ jest $F_n \equiv F_m \pmod p$.

- (1) Dowieść, że taki okres istnieje. Dowieść, że każdy okres modulo p jest wielokrotnością okresu minimalnego.
- (2) Obliczyć minimalne okresy ciągu Fibonacciego dla $p = 2, 3, 5, 7, 11, 13, 17$.
- (3) Niech $K = \mathbf{Q}(\alpha)$, gdzie α jest pierwiastkiem wielomianu $t^2 - t - 1 \in \mathbf{Z}[t]$. Dowieść, że $F_n = \text{Tr}_{K/\mathbf{Q}}(\frac{\alpha^n}{2\alpha-1})$, dla każdego $n \geq 0$.
- (4) Znaleźć regularność w rozkładzie wielomianu $t^2 - 5 \in \mathbf{Z}[t]$ modulo p dla $p = 2, 3, 5, 7, 11, 13, 17$.
- (5) Co można dowieść o minimalnym okresie ciągu Fibonacciego modulo p ?

Zadanie 9*

Wyznaczyć pierścień liczb całkowitych ciała dwukwadratowego $K = \mathbf{Q}(\sqrt{2}, \sqrt{3})$. **Wskazówka.** Zauważyć, że $\sqrt{6} \in \mathcal{O}_K$. Na początek pokazać, że $\alpha \in K$ jest liczbą algebraiczną całkowitą, wtedy i tylko wtedy, gdy $\text{Tr}_{K/\mathbf{Q}(\sqrt{2})}(\alpha)$ oraz $N_{K/\mathbf{Q}(\sqrt{2})}(\alpha)$ są liczbami algebraicznymi całkowitymi. Następnie pokazać, że w ostatnim zdaniu można zastąpić $\sqrt{2}$ liczbą $\sqrt{3}$ lub $\sqrt{6}$ bez zmiany wartości logicznej zdania. Za pomocą bardzo podobnej metody można dowieść:

Twierdzenie.

Niech d, e będą różnymi liczbami całkowitymi, które są wolne od kwadratów oraz niech $f = de/NWD(d, e)^2$. Niech $K = \mathbf{Q}(\sqrt{d}, \sqrt{e}) = \mathbf{Q}(\sqrt{d}, \sqrt{e}, \sqrt{f})$ będzie ciałem dwukwadratowym wyznaczonym przez d, e i f . Wtedy bazą całkowitą pierścienia $\mathcal{O}_K$ jest:

- (1) $1, \sqrt{d}, \sqrt{e}, \frac{\sqrt{e} + \sqrt{f}}{2}$, jeśli $d \equiv 3 \pmod 4$ oraz $e, f \equiv 2 \pmod 4$
- (2) $1, \frac{1 + \sqrt{d}}{2}, \sqrt{e}, \frac{\sqrt{e} + \sqrt{f}}{2}$, jeśli $d \equiv 1 \pmod 4$ oraz $e, f \equiv 2$ lub $3 \pmod 4$
- (3) $1, \frac{1 + \sqrt{d}}{2}, \frac{1 + \sqrt{e}}{2}, (\frac{1 + \sqrt{d}}{2})(\frac{1 + \sqrt{f}}{2})$, jeśli $d, e, f \equiv 1 \pmod 4$.

* Przeprowadzić dowód tego twierdzenia.

WESOŁYCH ŚWIĄT