ALGEBRAICZNA TEORIA LICZB

ZESTAW 1

ZADANIE 1 Dowiedź, że pierścień $\mathbb{Z}[\sqrt{10}]$ nie jest dziedziną z jednoznacznością rozkładu. Znajdź element $\mathbb{Z}[\sqrt{10}]$, który jest nierozkładalny, ale nie jest pierwszy.

(*Wsk. Rozłóż* 6 *na iloczyny elementów nierozkładalnych.*)

ZADANIE 2 (a) Wykaż, że $\mathbb{Z}[\sqrt{-2}]$ jest dziedziną Euklidesa. (*Wsk.: Niech* $x/y = a + b\sqrt{-2}$ *dla* $a, b \in \mathbb{Q}$. *Wybrać* $q = c + d\sqrt{-2}$ *w ten sposób, aby* $|c - a| \leqslant 1/2$ *oraz* $|d - b| \leqslant 1/2$.)

(b) Znajdź jedności w pierścieniu $\mathbb{Z}[\sqrt{-2}]$.

ZADANIE 3 Wyznacz wszystkie rozwiązania całkowite równania Bacheta $x^3 - y^2 = 2$.

ZADANIE 4 Niech $p > 2$ będzie liczbą pierwszą.

(a) Wykaż, że $w^2 \equiv -2 \pmod p$ ma rozwiązanie wtedy i tylko wtedy, gdy $p \equiv 1, 3 \pmod 8$.

(Wsk. skorzystaj ze wzorów na symbole Legendre'a: $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$, $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$*.)*

(b) Wywnioskuj z (a), że jeżeli $p = x^2 + 2y^2$ dla pewnych $x, y \in \mathbb{N}$, to $p \equiv 1, 3 \pmod 8$.

(c) Wykaż, że jeżeli $p \equiv 1, 3 \pmod 8$, to $p = x^2 + 2y^2$ dla pewnych $x, y \in \mathbb{Z}$.

(Wsk. Znajdź korzystając z (a) elementy $\alpha, \beta \in \mathbb{Z}[\sqrt{-2}]$ *takie, że* $p|\alpha\beta$*, ale* $p \nmid \alpha, \beta$*. Skorzystaj z jednoznaczności rozkładu.)*

ZADANIE 5 Załóżmy, że $x, y, z \in \mathbb{N}$ spełniają $xy = z^2 + 1$. Wykaż, że istnieją $a, b, c, d \in \mathbb{N}$ takie, że

$$x = a^2 + b^2, \qquad y = c^2 + d^2, \qquad z = ac + bd.$$

(*Wsk. jeżeli* R *jest DJR oraz* $A, B, C, D \in R \setminus \{0\}$ *spełniają* $AB = CD$*, to* $A = a_1a_2$, $B = b_1b_2$, $C = a_1b_2$, $D = a_2b_1$ *dla pewnych* $a_1, a_2, b_1, b_2 \in R$).

ZADANIE 6 Niech L/K będzie skończonym rozszerzeniem ciał. NORMĘ oraz ŚLAD elementu $\alpha \in L$ definiujemy jako:

$$N_{L/K}(\alpha) = \prod_{\sigma: L \hookrightarrow \overline{K}} \sigma(\alpha), \qquad \mathrm{tr}_{L/K}(\alpha) = \sum_{\sigma: L \hookrightarrow \overline{K}} \sigma(\alpha),$$

gdzie iloczyn/suma brana jest po wszystkich K-liniowych zanurzeniach $\sigma : L \hookrightarrow \overline{K}$.

(a) Wykaż, że $N_{L/K}(\alpha), \mathrm{tr}_{L/K}(\alpha) \in K$.

(*Wsk. Wykaż to najpierw w przypadku, gdy* L/K *jest rozszerzeniem Galois. W ogólnym przypadku rozważ domknięcie Galois rozszerzenia.*)

(b) Wykaż, że $N_{L/K}(\alpha) = (-1)^n a_d^{n/d}$ oraz $\mathrm{tr}_{L/K}(\alpha) = \frac{n}{d} \cdot (-a_{d-1})$, gdzie

$$\min_K(\alpha)(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_0, \qquad n = [L : K].$$

(c) Wykaż, że $\mathrm{tr}_{L/K}(\alpha) = \mathrm{tr}\, f_\alpha$, $N_{L/K}(\alpha) = \det f_\alpha$, gdzie $f_\alpha : L \to L$ jest K-liniowym przekształceniem danym jako:

$$f_\alpha(x) = \alpha \cdot x.$$

(Wsk. Dla $L = K(\alpha)$ *masz do dyspozycji „ładną" bazę ☺ W ogólnym przypadku rozważ bazę* $L/K(\alpha)$ *i „zrób" z niej bazę* L/K*.)*