ALGEBRAICZNA TEORIA LICZB
ZESTAW 7 – Grupa klas

- grupa klas pierścienia Dedekinda: $Cl(R) :=$ niezerowe ideały ułamkowe/główne ideały ułamkowe,

  FAKT $\quad K$ – ciało liczbowe $\Rightarrow \#Cl(\mathcal{O}_K) < \infty$

- TWIERDZENIE (MINKOWSKI) Niech K – ciało liczbowe stopnia n o sygnaturze (r_1, r_2) i wyróżniku D.

  W każdej klasie ideałów znajduje się ideał (całkowity) o normie $\leqslant \sqrt{|D|}\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}$.

ZADANIE 1 Niech $K = \mathbb{Q}(\sqrt{223})$.

(a) Obliczyć grupę jedności $\mathcal{O}_K$ i grupę klas $Cl(\mathcal{O}_K)$.

(b) Które z równań diofantycznych: $X^2-223Y^2 = \pm 11$, $X^2-223Y^2 = \pm 11\cdot 19$, $X^2-223Y^2 = \pm 11^2$ ma rozwiązania całkowite?

ZADANIE 2 Oblicz grupę klas dla $\mathbb{Q}(\sqrt[3]{2})$.

ZADANIE 3 (a) Znajdź liczbę klas dla $\mathbb{Q}(\sqrt{-5})$.

(b) Rozwiąż w liczbach całkowitych równanie $y^3 - x^2 = 5$.

ZADANIE 4 Niech $d \in \mathbb{Z}_{>0}$ będzie wolna od kwadratu, parzysta i niech $d = a^n - 1$ dla pewnych liczb całkowitych $a, n \geqslant 2$.

(a) Wykazać, że w pierścieniu $\mathbb{Z}[\sqrt{-d}]$ zachodzi równość $(1 + \sqrt{-d}) = I^n$ dla pewnego ideału I.

(b) Dowieść, że klasa ideału I ma rząd równy n w grupie klas ciała $\mathbb{Q}(\sqrt{-d})$.

Wsk. jeżeli $I^k = (b + \sqrt{-d}c)$, to $a^k = b^2 + dc^2$. Gdyby $c = 0$, to $2|k$ oraz $(a) = I^2$.

ZADANIE 5 *(Euler)* Niech $p = 4n - 1 \geqslant 11$ będzie liczbą pierwszą. Dowieść, że liczba klas ciała $\mathbb{Q}(\sqrt{-p})$ jest równa jeden, wtedy i tylko wtedy, gdy dla każdego całkowitego $0 \leqslant a \leqslant n - 2$ liczba $a^2 + a + n$ jest liczbą pierwszą.

ZADANIE 6 Niech będzie dana macierz kwadratowa $A \in M_{n,n}(\mathbb{R})$, $A = [a_{ij}]_{ij}$. Rozważmy n form liniowych $L_i(x) = \sum_{j=1}^{n} a_{ij}x_j$ dla $x = (x_1, x_2, \ldots, x_n) \in \mathbb{R}$ oraz $1 \leqslant i \leqslant n$. Niech będą dane dodatnie liczby rzeczywiste $\lambda_1, \lambda_2, ..., \lambda_n$ takie, że $\lambda_1\lambda_2...\lambda_n \geqslant |detA| > 0$. Wykazać, że istnieją liczby całkowite $y_1, y_2, ..., y_n$ nie wszytkie równe zero i takie, że $|L_i(y_1, y_2, \ldots, y_n)| \leqslant \lambda_i$ dla każdego $1 \leqslant i \leqslant n$.

Wsk. zastosuj twierdzenie Minkowskiego do zbioru $X = \{x \in \mathbb{R}^n : \forall_i |L_i(x)| \leqslant \lambda_i\}$. Jak wygląda ten zbiór?