PIERŚCIEŃ GAUSSA $\mathbb{Z}[i]$
I Uniwersytecki Obóz Olimpiady Matematycznej

Michał Szachniewicz

grudzień 2016, Bardo

1. Pokaż, że:
   (a) norma w $\mathbb{Z}[i]$, $N(\alpha) = \alpha \cdot \overline{\alpha}$, jest multiplikatywna;
   (b) jedyne elementy odwracalne w $\mathbb{Z}[i]$ to $1, -1, i, -i$;
   (c) jeśli $\alpha|\beta$ i $\beta|\alpha$ to $\alpha \sim \beta$;
   (d) Pokaż, że jeśli $\alpha|\beta$ to $N(\alpha)|N(\beta)$.

2. Pokaż, że w $\mathbb{Z}[i]$ można dzielić z resztą. To znaczy, że jeśli $\alpha, \beta \in \mathbb{Z}[i]$ i $\beta \neq 0$, to istnieje taka para liczb φ, δ, że:
$$\alpha = \varphi\beta + \delta \text{ oraz } N(\delta) < N(\beta).$$
   Zrób to w następujący sposób:
   (a) wybierz jakąś liczbę z $\mathbb{Z}[i]$, blisko $\frac{\alpha}{\beta}$ z $\mathbb{Q}[i]$, i podstaw pod nią φ;
   (b) Zauważ, że $N(\alpha - \varphi\beta) = N(\beta)N(\alpha\beta^{-1} - \varphi)$ i pokaż, że $N(\alpha\beta^{-1} - \varphi) < 1$.

   Czy dzielenie z resztą w $\mathbb{Z}[i]$ jest jednoznaczne?

3. Pokaż, że jeśli zbiór $I \subseteq \mathbb{Z}[i]$ jest zamknięty ze względu na dodawanie i mnożenie przez elementy $\mathbb{Z}[i]$, to istnieje $\delta \in \mathbb{Z}[i]$, że $I = \{\gamma : \exists\varphi\ \gamma = \delta\varphi\}$, co będziemy zonaczać (δ). Skorzystaj z poprzedniego zadania.

4. Będziemy pisać $\langle\alpha, \beta\rangle \sim \gamma$, gdy γ jest dzielnikiem α, β, oraz spełnione jest:
$$\forall\delta(\delta|\alpha \wedge \delta|\beta) \Rightarrow \delta|\gamma$$
   Udowodnij, że:
   (a) jeśli $\langle\alpha, \beta\rangle \sim \gamma$ oraz $\langle\alpha, \beta\rangle \sim \vartheta$, to $\gamma \sim \vartheta$;
   (b) każde dwie liczby α, β mają taką liczbę γ, że $\langle\alpha, \beta\rangle \sim \gamma$ (wsk.: skorzystaj z zadania 3).

   Jaką rolę pełni $\langle\alpha, \beta\rangle$ w $\mathbb{Z}[i]$?

5. Pokaż, że w $\mathbb{Z}[i]$ zachodzi zasadnicze twierdzenie artmetyki:
$$\text{Jeśli } \langle\alpha, \beta\rangle \sim 1 \text{ oraz } \beta|\alpha\gamma, \text{ to } \beta|\gamma.$$
   Wskazówka: zastanów się jak dowodzi się tego twierdzenia w $\mathbb{Z}$. Pomyśl, co pociąga to twierdzenie, w świecie $\mathbb{Z}[i]$.

6. Rozważ następujące dwie definicje pierwszości w $\mathbb{Z}[i]$:
$$\text{jeżeli } \gamma = \alpha\beta, \text{ to } \alpha \sim 1 \text{ lub } \beta \sim 1;$$
$$\text{jeżeli } \gamma|\alpha\beta, \text{ to } \gamma|\alpha \text{ lub } \gamma|\beta.$$
   Pokaż, że są one równoważne.

7. Pokaż, że w $\mathbb{Z}[i]$ rozkład na czynniki pierwsze jest jednoznaczny z dokładnością do relacji stowarzyszenia i kolejności wyrazów.

8. Udowodnij następujące fakty:
   (a) π liczbą pierwszą w $\mathbb{Z}[i]$ wtedy i tylko wtedy gdy $\overline{\pi}$ liczbą pierwszą w $\mathbb{Z}[i]$;
   (b) jeżeli $N(\pi)$ pierwsze w $\mathbb{N}$, to π pierwsze w $\mathbb{Z}[i]$;
   (c) jeśli π pierwsze w $\mathbb{Z}[i]$, to istnieje p pierwsze w $\mathbb{N}$, że $\pi | p$.
9. Pokaż, że jeśli p jest liczbą pierwszą w $\mathbb{N}$, to:
   (a) jeśli $p = 4k + 1$, to p nie jest pierwsza w $\mathbb{Z}[i]$;
   (b) jeżeli $p = 4k + 3$, to p jest pierwsza w $\mathbb{Z}[i]$.
10. Znajdź wszystkie liczby naturalne jakie mozna zapisać w postaci sumy dwóch kwadratów.
11. Spróbuj wykorzystać $\mathbb{Z}[i]$ w następujących zadaniach:
   (a) Jeśli trójka liczb całkowitych, względnie pierwszych (a, b, c) spełnia równanie pitagorasa, to pokaż, że:
   $$a = \pm(u^2 - v^2),\ b = \pm 2uv,\ c = \pm(u^2 + v^2)$$
   dla pewnych u, v względnie pierwszych.
   (b) Rozwiąż równanie $y^2 = x^3 - 1$ w liczbach całkowitych.
   (c) Zbadaj równanie $x^2 + y^2 = z^n$, przy dowolnym n.
   (d) Pokaż, że równanie $n = a^2 + b^2$ może mieć dowolnie dużo rozwiązań w liczbach całkowitych (n jest naturalne).
12. Zastanów się jakie własności były kluczowe, żeby w $\mathbb{Z}[i]$ zachodziły twierdzenia z zadania piątego, czy siódmego. Czy własności te zachodzą np. w $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}\ :\ a, b \in \mathbb{N}\}$?