Teoria liczb
rozszerzenia całkowite $\mathbb{Z}$, 27-30 marca

Zadanie 1. Niech $\mathbb{Z}[i] \subseteq \mathbb{C}$ będzie pierścieniem liczb całkowitych Gaussa, z Algebry I wiemy, że jest to dziedzina z jednoznacznością rozkładu. Niech $|\alpha|^2$ oznacza normę zespoloną elementu $\alpha \in \mathbb{Z}[i]$. Zauważmy, że $|\alpha|^2 \cdot |\beta|^2 = |\alpha\beta|^2$.

(a) Pokaż, że $|\alpha|^2$ jest liczbą całkowitą nieujemną dla każdego $\alpha \in \mathbb{Z}[i]$,

(b) Pokaż, że $|\alpha|^2 = 0$ wtedy i tylko wtedy, gdy $\alpha = 0$. Pokaż, że $|\alpha|^2 = 1$ wtedy i tylko wtedy, gdy α jest odwracalnym elementem $\mathbb{Z}[i]$.

(c) Zachodzi $(2+i)(2-i) = 5 = (1+2i)(1-2i)$. Dlaczego nie przeczy to jednoznaczności rozkładu?

Zadanie 2. Niech $\mathbb{Z}[i] \subseteq \mathbb{C}$ będzie pierścieniem liczb całkowitych Gaussa. Niech $\mathfrak{p} \subseteq \mathbb{Z}[i]$ będzie ideałem maksymalnym.

(a) Pokaż, że przecięcie $\mathfrak{p} \cap \mathbb{Z}$ jest niezerowe. Wywnioskuj, że $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ dla pewnej liczby $p \in \mathbb{P}$.

(b) Pokaż, że $\mathbb{Z}[i]/\mathfrak{p}$ ma skończenie wiele elementów.

(c) Niech α będzie generatorem $\mathfrak{p}$. Pokaż, że norma zespolona $|\alpha|^2$ jest równa p lub p^2.

(d) Pokaż, że jeśli $|\alpha|^2 = p^2$, to $\mathfrak{p} = p\mathbb{Z}[i]$, a jeśli $|\alpha| = p$, to $p = a^2 + b^2$, gdzie $\alpha = a + bi$.

(e) Pokaż, że jeśli $p \equiv 3 \pmod 4$, to $p\mathbb{Z}[i]$ jest ideałem pierwszym.

(f) Pokaż, że jeśli $p \equiv 1 \pmod 4$, to $p\mathbb{Z}[i] = (a-bi)\mathbb{Z}[i] \cdot (a+bi)\mathbb{Z}[i]$ dla takich a, b, że $p = a^2 + b^2$.

(g) Pokaż, że jeśli $p = 2$, to istnieje dokładnie jeden $\mathfrak{p}$ taki, że $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Znajdź ten ideał.

(h) $\star$ Zdefiniujmy funkcję $\zeta_{\mathbb{Z}[i]}(s)$ dla $s > 1$ poprzez

$$\zeta_{\mathbb{Z}[i]}(s) = \prod_{\mathfrak{p} \subseteq \mathbb{Z}[i],\ \text{maximal ideal}} \frac{1}{1 - N(\mathfrak{p})^{-s}},$$

gdzie $N(\mathfrak{p})$ oznacza liczbę elementów $\mathbb{Z}[i]/\mathfrak{p}$. Użyj wiedzy $\mathfrak{p}$ powyżej, by wykazać, że dla $s > 1$ prawa strona jest zbieżna i mamy $\zeta_{\mathbb{Z}[i]}(s) = \zeta(s) \cdot L(s, \chi)$, gdzie $\zeta(s)$ i $L(s, \chi)$ były zdefiniowane tydzień temu.

Zadanie 3. Niech $A = \mathbb{Z}[\sqrt{-5}]$. Zauważmy, że mamy funkcję $|-|^2 \colon A \to \mathbb{Z}_{\geq 0}$.

(a) Pokaż, że elementy $2, 3, 1 - \sqrt{-5}, 1 + \sqrt{-5}$ są nierozkładalne.

(b) Wywnioskuj, że A nie jest dziedziną z jednoznacznością rozkładu.

Zadanie 4. Niech $f \in \mathbb{Z}[x]$ będzie unormowanym[1] wielomianem o współczynnikach całkowitych. Załóżmy, że $f = g \cdot h$, gdzie g, h są unormowanymi wielomianami o współczynnikach wymiernych. Pokaż, że g i h mają współczynniki całkowite. *Wskazówka: wymnóż przez NWW mianowników.*

Zadanie 5. Liczbę $\alpha \in \mathbb{C}$ nazywamy *całkowitą (nad $\mathbb{Z}$)*, jeśli jest ona pierwiastkiem unormowanego wielomianu o współczynnikach całkowitych. Pokaż, że elementy $\mathbb{Q}$ całkowite w powyższym sensie to $\mathbb{Z}$.

Zadanie 6. Ustalmy liczbę całkowitą $d \neq 0, 1$ bezkwadratową i niech $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ oznacza zbiór wszystkich elementów $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{C}$, które są całkowite nad $\mathbb{Z}$.

(a) Pokaż, że $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.

(b) Pokaż, że każdy element $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ spełnia równanie postaci $x^2 - ax + b = 0$, gdzie $a, b \in \mathbb{Z}$. Wywnioskuj, że jest on postaci $(a_1 + a_2\sqrt{d})/2$, gdzie $a_1, a_2 \in \mathbb{Z}$.

(c) $\star$ Opisz $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. *Odpowiedź będzie zależała od reszty d z dzielenia przez 4.*

[1] Tzn. współczynnik przy najwyższej potędze x jest równy 1.