Teoria liczb
rozszerzenia całkowite $\mathbb{Z}$, 3-13 kwietnia

Zadanie 1. 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) Opisz $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. *Odpowiedź będzie zależała od reszty d z dzielenia przez 4.*

Zadanie 2 (Pierścień Eisensteina)**.** Niech $d = -3$ i rozważmy pierścień $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\omega_3]$, gdzie $\omega_3 = \cos(2\pi/3) + i\sin(2\pi/3) = \frac{-1+i\sqrt{3}}{2}$. Możesz założyć, że pierścień ten jest dziedziną z jednoznacznością rozkładu.

(a) Oblicz kwadrat normy zespolonej elementu $a + b\omega_3$, gdzie $a, b \in \mathbb{Z}$.

(b) Niech $\mathfrak{p} \subseteq \mathbb{Z}[\omega_3]$ będzie ideałem maksymalnym. Pokaż, że $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ dla pewnej liczby pierwszej p. Wywnioskuj, że jeśli α jest generatorem $\mathfrak{p}$, to $|\alpha|^2 = p$ lub $|\alpha|^2 = p^2$.

(c) Pokaż, że jeśli $p \equiv 2 \pmod 3$, to w sytuacji powyżej $\mathfrak{p}$ jest generowany przez p. *Wskazówka: kongruencje w $\mathbb{Z}$.*

(d) Załóżmy, że $p \equiv 1 \pmod 3$. Pokaż, że istnieje liczba n taka, że $n \not\equiv 1 \pmod p$ oraz $n^3 \equiv 1 \pmod p$. Wywnioskuj, że w $\mathbb{Z}[\omega_3]$ mamy $(n-1)(n-\omega_3)(n-\omega_3^2) \in p\mathbb{Z}[\omega_3]$. Wywnioskuj, że p nie jest elementem pierwszym, a zatem w sytuacji powyżej mamy $|\alpha|^2 = p$. Wreszcie, wyciągnij wniosek, że $p = a^2 + ab + b^2$ dla pewnych całkowitych a, b.

Zadanie 3. Niech $p \in \mathbb{P}$. Niech $\omega_p := \exp(2\pi i/p) = \cos(2\pi/p) + i\sin(2\pi/p) \in \mathbb{C}$ będzie pierwiastkiem z jedynki stopnia p. Niech $F(x) := x^{p-1} + \ldots + x + 1 \in \mathbb{Z}[x]$ będzie wielomianem.

(a) Pokaż, że $F(\omega_p) = 0$ oraz $F(1) = p$. Załóżmy, że F jest rozkładalny na wielomiany $G, H \in \mathbb{Q}[x]$. Pokaż, że po ewentualnym domnożeniu przez stałą można założyć, że G, H mają współczynniki całkowite. Pokaż, że można dodatkowo założyć, że $G(1) = 1$.

(b) Pokaż, że $F \equiv (x-1)^{p-1} \pmod p$. Wywnioskuj, że $G \equiv (x-1)^s \pmod p$ dla pewnego s. Z równości $G(1) = 1$ wywnioskuj, że $s = 0$, zatem $G = 1$. To pokazuje, że F jest nierozkładalny, więc jest wielomianem minimalnym ω_p.

(c) Pokaż, że jeśli nie założymy, że p jest pierwsza, to może się zdarzyć, że F jest rozkładalny.

(d) Oblicz $\sum_{i=0}^{p-1} \omega_p^{ai}$ w zależności od liczby całkowitej a.

Zadanie 4. Niech $p \in \mathbb{P}$ będzie liczbą nieparzystą. Niech $\omega_p := \exp(2\pi i/p) = \cos(2\pi/p) + i\sin(2\pi/p) \in \mathbb{C}$ będzie pierwiastkiem z jedynki stopnia p.

(a) Pokaż, że jeśli $p = 3$ to $\omega_p - \omega_p^2 = \sqrt{-3}$.

(b) Dla liczby całkowitej a, zdefiniujmy *sumę Gaussa* $g_a := \sum_{t=1}^{p-1} \left(\frac{t}{p}\right) \omega_p^{at}$. Pokaż, że $g_a = \left(\frac{a}{p}\right) g_1$.

(c) Używając (b), pokaż, że suma $\sum_{a=0}^{p-1} g_a g_{-a}$ jest równa $(-1)^{\frac{p-1}{2}}(p-1)g_1^2$.

(d) Oblicz bezpośrednio, że $\sum_{a=0}^{p-1} g_a g_{-a} = \sum_{a=0}^{p-1} \sum_{x,y} \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) \omega_p^{a(x-y)}$. Pokaż, że to wyrażenie wynosi $p(p-1)$ i wywnioskuj, że $g_1^2 = (-1)^{\frac{p-1}{2}} p$. To pokazuje, że zawsze mamy $\sqrt{(-1)^{\frac{p-1}{2}} p} = \pm g_1 \in \mathbb{Z}[\omega_p]$!