Teoria liczb
rozszerzenia całkowite $\mathbb{Z}$ ciąg dalszy, 17-20 kwietnia

Zadanie 1. (a) Niech $p \in \mathbb{P}$. Niech $\chi\colon \mathbb{Z} \to \mathbb{R}$ będzie nietrywialnym charakterem Dirichleta modulo p o wartościach rzeczywistych. Pokaż, że $\chi(a) = \left(\frac{a}{p}\right)$.

(b) Znajdź wszystkie charaktery Dirichleta dla grupy $\mathbb{Z}_8^*$. Niech $\mathbf{1}_5\colon \mathbb{Z} \to \mathbb{C}$ będzie funkcją daną przez

$$\mathbf{1}_5(a) = \begin{cases} 1 & a \equiv 5 \pmod 8 \\ 0 & \text{w pozostałych przypadkach.} \end{cases}$$

Wyraź $\mathbf{1}_5$ jako kombinację liniową charakterów dla grupy $\mathbb{Z}_8^*$.

Zadanie 2. Niech $A = \mathbb{Z}[\sqrt{-5}]$. W serii 4 sprawdziliśmy, że nie jest to dziedzina z jednoznacznością rozkładu.

(a) Pokaż, że ideał $(2, 1+\sqrt{-5})$ w A nie jest generowany przez jeden element, zatem A nie jest dziedziną ideałów głównych. *Wskazówka: rozważ $|\alpha|^2$ hipotetycznego generatora α.*

(b) Oblicz, że $(2, 1+\sqrt{-5})^2$ jest ideałem generowanym przez element 2.

(c) Niech $\mathfrak{p}$ będzie niezerowym ideałem pierwszym w A. Uzasadnij, że $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ dla liczby pierwszej p.

(d) Załóżmy, że $\mathfrak{p}$ nie jest generowany przez p. Pokaż, że istnieje liczba całkowita $a \in \mathbb{Z}$ taka, że $a - \sqrt{-5} \in \mathfrak{p}$. Wywnioskuj, że -5 jest resztą kwadratową modulo p. *Wskazówka: weź dowolny element z $\mathfrak{p} \setminus p\mathbb{Z}[\sqrt{-5}]$ i jego wielokrotność.*

(e) Pokaż, że odwrotnie, jeśli -5 jest resztą kwadratową modulo p, to istnieje $a \in \mathbb{Z}$ taka, że $(a-\sqrt{-5})(a+\sqrt{-5}) \in p\mathbb{Z}[\sqrt{-5}]$, więc $p\mathbb{Z}[\sqrt{-5}]$ nie jest ideałem pierwszym.

(f) Scharakteryzuj liczby pierwsze p takie, że -5 jest resztą kwadratową modulo p. *Wskazówka: prawo wzajemności reszt. Uważaj na przypadek $p = 5$.*

Zadanie 3. Niech $A = \mathbb{Z}[-\sqrt{-5}]$, niech $p \neq 2$ będzie liczbą pierwszą taką, że -5 jest resztą kwadratową modulo p i niech $a \in \mathbb{Z}$ będzie liczbą taką, że $a^2 \equiv 5 \pmod p$.

(a) Załóżmy, że $p \neq 5$. Pokaż, że zachodzi równość ideałów

$$(a - \sqrt{-5}, p) \cdot (a + \sqrt{-5}, p) = (p). \tag{1.1}$$

(b) W sytuacji powyżej, pokaż, że $(a - \sqrt{-5}, p)$ oraz $(a + \sqrt{-5}, p)$ są ideałami maksymalnymi w $\mathbb{Z}[\sqrt{-5}]$. *Wskazówka: bezpośrednio: załóż, że nie jest maksymalny, weź większy ideał maksymalny $\mathfrak{m}$ i z elementu $\mathfrak{m} \setminus (a - \sqrt{-5}, p)$ wygeneruj jedynkę.*

(c) Niech $\mathfrak{q}$ będzie dowolnym ideałem pierwszym zawierającym element p. Z równości (1.1) wywnioskuj, że $a - \sqrt{-5} \in \mathfrak{q}$ lub $a + \sqrt{-5} \in \mathfrak{q}$, zatem $\mathfrak{q} = (a - \sqrt{-5}, p)$ lub $\mathfrak{q} = (a + \sqrt{-5}, p)$.

(d) Złóż poprzednie podpunkty w całość: pokaż, że dla każdej liczby pierwszej $p \neq 5$ takiej, że $p\mathbb{Z}[\sqrt{-5}]$ nie jest pierwszym ideałem, jedyne ideały pierwsze zawierające p to $(p, a - \sqrt{-5})$, $(p, a + \sqrt{-5})$.

(e) Uzasadnij, że $(5, \sqrt{-5})$ jest jedynym ideałem pierwszym zawierającym $p = 5$.

Zadanie 4 ($\star$). Uogólnij poprzednie dwa ćwiczenia z $\sqrt{-5}$ do ogólnego $\sqrt{-d}$ dla d bezkwadratowego. Jeśli chcesz, możesz założyć, że $d < 0$ oraz $d \not\equiv 1 \pmod 4$.