# 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 $\mathbb{Z}_8^*$.

*Rozwiązanie.*
(a) Z definicji, charakter $\chi$ jest multiplikatywny, więc indukuje homomorfizm grup $\chi\colon \mathbb{Z}_p^* \to \mathbb{R}^*$, którego obraz leży w zbiorze pierwiastków z jedynki. W $\mathbb{R}^*$ mamy tylko dwa takie pierwiastki: $\{1, -1\}$. Wobec tego otrzymujemy homomorfizm $\chi\colon \mathbb{Z}_p^* \to \{1, -1\}$. Niech $g$ będzie generatorem $\mathbb{Z}_p^*$. Jeśli $\chi(g) = 1$, to $\chi(g^k) = 1$ dla każdego $k$, więc $\chi$ jest charakterem trywialnym. Zatem $\chi(g) = -1$. Wtedy dla każdej liczby całkowitej nieujemnej $k$ mamy $\chi(g^{2k}) = (\chi(g)^2)^k = 1$ oraz $\chi(g^{2k+1}) = \chi(g^{2k})\chi(g) = -1$. To pokazuje, że $\chi$ jest równy symbolowi Legendre'a.
(b) W grupie $\mathbb{Z}_8^*$ każdy element $a$ spełnia $a^2 \equiv 1 \pmod 8$. Zatem dla każdego charakteru $\chi$ tej grupy i każdego elementu $a \mod 8$ tej grupy mamy $(\chi(a \mod 8))^2 = \chi(a^2 \mod 8) = \chi(1 \mod 8) = 1$. To pokazuje, że $\chi$ jest funkcją $\mathbb{Z}_8^* \to \{-1, 1\}$.

Rozważmy zatem homomorfizmy grup $C_2 \times C_2 \simeq \mathbb{Z}_8^* \to \{-1, 1\} \simeq C_2$. Z ogólnego nonsensu z Algebry I, taki homomorfizm można jednoznacznie zdefiniować, wybierając *dowolne* wartości na generatorach $C_2 \times C_2$. Wybór generatorów nie jest jednoznaczny, weźmy $3 \mod 8$ i $5 \mod 8$ jako generatory. Mamy wtedy $(3 \mod 8) \cdot (5 \mod 8) = 7 \mod 8$. Wybierając kolejno, otrzymujemy charaktery:

| | $\chi(1 \mod 8)$ | $\chi(3 \mod 8)$ | $\chi(5 \mod 8)$ | $\chi(7 \mod 8)$ |
|---|---|---|---|---|
| $\chi_0$ | 1 | 1 | 1 | 1 |
| $\chi_1$ | 1 | 1 | $-1$ | $-1$ |
| $\chi_2$ | 1 | $-1$ | 1 | $-1$ |
| $\chi_3$ | 1 | $-1$ | $-1$ | 1 |

Przypomnijmy, że zachodzi relacja „ortogonalności": dla każdych $a, b \in \mathbb{Z}_8^*$ mamy

$$\sum_\chi \chi(a)\overline{\chi(b)} = \begin{cases} \varphi(8) & \text{jeśli } a = b \\ 0 & \text{jeśli } a \neq b. \end{cases}$$

Biorąc $b = 5$, otrzymujemy funkcję

$$\mathbf{1}_5 = \frac{1}{4}\sum_\chi \chi(5)\chi = \frac{1}{4}\left(\chi_0 - \chi_1 + \chi_2 - \chi_3\right).$$

**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 $\alpha$.*

(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 $p = 5$.*

*Rozwiązanie.*
(a) Załóżmy, że $(\alpha) = (2, 1+\sqrt{-5})$. Wtedy $|\alpha|^2$ jest dzielnikiem zarówno $|2|^2 = 4$ jak i $|1+\sqrt{-5}|^2 = 6$, więc $|\alpha|^2 \in \{1, 2\}$. Jeśli zapiszemy $\alpha = a + b\sqrt{-5}$, to $|\alpha|^2 = a^2 + 5b^2$. Wynika stąd, że $|\alpha|^2 \neq 2$, a więc $|\alpha|^2 = 1$. To pokazuje, że $\alpha$ jest odwracalny w $\mathbb{Z}[\sqrt{-5}]$, zatem $(2, 1+\sqrt{-5}) = \mathbb{Z}[\sqrt{-5}]$. Ale to nie jest prawdą: obliczamy, że $(1+\sqrt{-5})\mathbb{Z}[\sqrt{-5}] = 6\mathbb{Z}[\sqrt{-5}] + (1+\sqrt{-5})\mathbb{Z}$. Zatem każdy element $a+b\sqrt{-5} \in (1+\sqrt{-5})\mathbb{Z}[\sqrt{-5}]$ spełnia zależność $a+b \equiv 0 \mod 2$. Również każdy element $2\mathbb{Z}[\sqrt{-5}]$ spełnia tę zależność. Zatem każdy element $(2, 1+\sqrt{-5})$ spełnia tę zależność, a $1$ jej nie spełnia. Sprzeczność.
(b) Obliczamy, że zachodzą równości ideałów w $\mathbb{Z}[\sqrt{-5}]$:

$$(2, 1+\sqrt{-5})^2 = (4, 2(1+\sqrt{-5}), -4+2\sqrt{-5}) = (4, 2(1+\sqrt{-5}), -6) = (4, 2(1+\sqrt{-5}), 2) = (2).$$

(c) Argumentujemy tu jak w rozwiązaniu zadania 2(a) serii 4 (tej na 27-30 kwietnia).
(d) Weźmy element $c + b\sqrt{-5} \in \mathfrak{p}$ nie leżący w $p\mathbb{Z}[\sqrt{-5}]$. Zatem jedna z liczb $c$, $b$ jest niepodzielna przez $p$. Jeśli $p$ dzieli $b$, to $c \in \mathfrak{p}$, ale $c$ jest niepodzielna przez $p$, sprzeczność z $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Zatem $b$ jest niepodzielna przez $p$. Niech $b' \in \mathbb{Z}$ będzie taka, że $bb' \equiv -1 \mod p$, powiedzmy $bb' = -1 + kp$ dla $k \in \mathbb{Z}$. Wtedy $b'(c + b\sqrt{-5}) - kp\sqrt{-5} = b'c - \sqrt{-5}$ jest żądanym elementem; $a = b'c$. Mamy też $a^2 + d = (a - \sqrt{-5})(a + \sqrt{-5}) \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, więc $-5 \equiv a^2 \pmod p$, co dowodzi części o reszcie kwadratowej.
(e) Jeśli $-5 \equiv a^2 \pmod p$, to mamy $a^2+5 = (a-\sqrt{-5})(a+\sqrt{-5}) \in p\mathbb{Z}[\sqrt{-5}]$, ale $a \pm \sqrt{-5} \notin p\mathbb{Z}[\sqrt{-5}]$. To z definicji znaczy, że $p\mathbb{Z}[\sqrt{-5}]$ nie jest ideałem pierwszym.
(f) Jeśli $p = 5$ lub $p = 2$, to $-5$ jest resztą kwadratową. Załóżmy, że $p \neq 2, 5$. Z prawa wzajemności mamy

$$\left(\frac{-5}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}} (-1)^{\frac{5-1}{2} \cdot \frac{p-1}{2}} \left(\frac{p}{5}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{5}\right).$$

Pozostaje sprawdzić, kiedy jest to jedynka. Jeśli $p \equiv 1 \pmod 4$, to wyrażenie jest jedynką wtedy i tylko wtedy, gdy $p \equiv 1, 4 \pmod 5$. Jeśli zaś $p \equiv 3 \pmod 4$, to wyrażenie jest jedynką wtedy i tylko wtedy, gdy $p \equiv 2, 3 \pmod 5$.

**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 $p = 5$.

*Rozwiązanie.*
(a) Obliczamy na ideałach w $\mathbb{Z}[\sqrt{-5}]$:

$$(a - \sqrt{-5}, p) \cdot (a + \sqrt{-5}, p) = (a^2 + 5, p(a - \sqrt{-5}), p(a + \sqrt{-5}), p^2).$$

Wynika z niej, że $(a-\sqrt{-5}, p)\cdot(a+\sqrt{-5}, p) \subseteq (p)$. Ponadto $2p\sqrt{-5} = p(a+\sqrt{-5})-p(a-\sqrt{-5})$ należy do produktu ideałów, więc również $10p = 2p\sqrt{-5}\cdot(-\sqrt{-5})$ należy do niego. Ale $\mathrm{NWD}(10p, p^2) = p$ z założenia, więc $p \in (10p, p^2) \subseteq (a - \sqrt{-5}, p) \cdot (a + \sqrt{-5}, p)$. To dowodzi, że

$$(a - \sqrt{-5}, p) \cdot (a + \sqrt{-5}, p) \supseteq (p).$$

(b) Weźmy ideał maksymalny $\mathfrak{m}$ zawierający $(a - \sqrt{-5}, p)$ i dowolny element $b + c\sqrt{-5} \in \mathfrak{m}$, który nie leży w $(a - \sqrt{-5}, p)$. Wtedy element

$$b + ac = b + c\sqrt{-5} + c(a - \sqrt{-5}),$$

także leży w $\mathfrak{m}$ i nie leży w $(a - \sqrt{-5}, p)$. W szczególności, mamy $b + ac \notin p\mathbb{Z}$. Ale liczba $p$ jest pierwsza, więc jeśli $b+ac$ jest niepodzielna przez $p$, to $1 \in (p, b+ac)$. To pokazuje, że $1 \in \mathfrak{m}$, a więc $\mathfrak{m}$ nie jest maksymalny. Sprzeczność. Dowodzi to, że $(a - \sqrt{-5}, p)$ jest maksymalny. Analogiczny dowód działa dla drugiego ideału.
(c) Mamy $(a-\sqrt{-5})\cdot(a+\sqrt{-5}) \in (p) \subseteq \mathfrak{q}$, więc z pierwszości $\mathfrak{q}$ mamy $a-\sqrt{-5} \in \mathfrak{q}$ lub $a+\sqrt{-5} \in \mathfrak{q}$. Jeśli $a - \sqrt{-5} \in \mathfrak{q}$, to ideał maksymalny $(a - \sqrt{-5}, p)$ jest zawarty w $\mathfrak{q}$. Z maksymalności wynika, że $(a - \sqrt{-5}, p) = \mathfrak{q}$. Podobnie argumentujemy w przypadku $a + \sqrt{-5} \in \mathfrak{q}$.
(d) Wynika to z poprzedniego podpunktu.
(e) Mamy $\sqrt{-5}^2 \in (5)$, więc każdy ideał pierwszy zawierający $5$ zawiera też $\sqrt{-5}$. Ponadto $(5, \sqrt{-5})$ jest ideałem maksymalnym, co można sprawdzić jak w podpunkcie (b). To kończy dowód.

**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 $d \not\equiv 1 \pmod 4$.

*Rozwiązanie.*

(Tu nie podajemy dokładnego rozwiązania. Omówię je na wykładzie, ale można sprawę podsumować stwierdzeniem „wszystko działa jak w poprzednich zadaniach dla $d = 5$”.)