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?

Rozwiązanie.
(a) Jeśli $\alpha = a + bi$, gdzie a, b są całkowite, to $|\alpha|^2 = a^2 + b^2$, co jest liczbą całkowitą nieujemną.
(b) Z poprzedniego punktu wynika, że $|\alpha|^2 = 0$ wtedy i tylko wtedy, gdy $a = b = 0$, czyli $\alpha = 0$. Załóżmy teraz, że $|\alpha|^2 = 1$. Niech $\overline{\alpha}$ będzie liczbą sprzężoną do α, wtedy $1 = |\alpha|^2 = \alpha \cdot \overline{\alpha}$. Ponadto $\overline{\alpha}$ leży w $\mathbb{Z}[i]$, zatem jest odwrotnością α w $\mathbb{Z}[i]$. Jeśli zaś α ma odwrotność $\beta \in \mathbb{Z}[i]$, to przykładając $|-|^2$ do równości $\alpha\beta = 1$, otrzymujemy $|\alpha|^2 \cdot |\beta|^2 = 1$. Skoro $|\alpha|^2$, $|\beta|^2$ są całkowite nieujemne, to wynika stąd $|\alpha|^2 = |\beta|^2 = 1$.
(c) Mamy $1 + 2i = i \cdot (2 - i)$ oraz $1 - 2i = i^{-1} \cdot (2 + i)$, zatem te dwa rozkłady różnią się tylko domnożeniem przez element odwracalny.

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.

Rozwiązanie.
(a). Niech $\alpha \in \mathfrak{p}$ będzie dowolnym niezerowym elementem $\mathfrak{p}$. Wtedy $\alpha \cdot \overline{\alpha}$ również leży w $\mathfrak{p}$, a na mocy zadania 1 jest to niezerowa liczba całkowita dodatnia. Zatem $\mathfrak{p} \cap \mathbb{Z}$ jest niezerowe. Z klasyfikacji ideałów w $\mathbb{Z}$ wynika, że $\mathfrak{p} \cap \mathbb{Z} = n\mathbb{Z}$ dla pewnego n. Załóżmy, że $n = ab$. Wtedy

$ab \in \mathfrak{p}$, ale ideał $\mathfrak{p}$ jest pierwszy, więc $a \in \mathfrak{p}$ lub $b \in \mathfrak{p}$. Wynika stąd, że n dzieli a lub n dzieli b. Zachodzi to dla dowolnego wyboru a i b, więc n jest liczbą pierwszą.
(b) Niech $p \in \mathbb{P}$ będzie taka, że $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Wtedy w ideale $\mathfrak{p}$ mamy elementy p oraz pi. Zatem każdy element $\alpha \in \mathbb{Z}[i]$ można przedstawić (być może na więcej niż jeden sposób!) jako kombinację $\alpha = a + bi + \beta$, gdzie $\beta \in p\mathbb{Z} + pi\mathbb{Z} \subseteq \mathfrak{p}$ oraz $a, b \in \mathbb{Z}$, przy czym $0 \leq a, b \leq p-1$. To dowodzi, że $\mathbb{Z}[i]/\mathfrak{p}$ ma co najwyżej p^2 elementów.
(c) Z definicji α, mamy $\mathfrak{p} = \alpha\mathbb{Z}[i]$. Zapiszmy jak powyżej, $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Zatem $p = \alpha\beta$ dla pewnego $\beta \in \mathbb{Z}[i]$. Przykładając normy, uzyskujemy $p^2 = |\alpha|^2 \cdot |\beta|^2$. Zatem $|\alpha|^2$ jest dodatnim dzielnikiem p^2, czyli $|\alpha|^2 \in \{1, p, p^2\}$. Pozostaje wykluczyć możliwość $|\alpha|^2 = 1$. Ale z zadania 1 wynika, że jeśli $|\alpha|^2 = 1$, to α jest odwracalny. Wtedy byłoby $\mathfrak{p} = \alpha\mathbb{Z}[i] = \mathbb{Z}[i]$. To przeczy pierwszości ideału $\mathfrak{p}$, bo z definicji ideał pierwszy nie jest całym pierścieniem. (d) Kontynuując rozumowanie, jeśli $|\alpha|^2 = p^2$, to $|\beta|^2 = 1$, więc β jest odwracalny i stąd

$$p\mathbb{Z}[i] = \alpha\beta\mathbb{Z}[i] = \alpha\mathbb{Z}[i] = \mathfrak{p}.$$

Jeśli zaś $|\alpha|^2 = p$, to zapiszmy $\alpha = a + bi$. Wtedy $p = |\alpha|^2 = a^2 + b^2$.
(e) W tym przypadku p nie można zapisać jako sumy kwadratów (patrz pierwsza seria zadań), więc na mocy (d) nie może zajść $|\alpha|^2 = p$. Musi być zatem $|\alpha|^2 = p^2$ i $p\mathbb{Z}[i] = \mathfrak{p}$ jest pierwszy.
(f) Z serii pierwszej wiemy, że liczby całkowite a, b takie, że $p = a^2 + b^2$, rzeczywiście istnieją. Wobec tego $p = a^2 + b^2 = a^2 - i^2b^2 = (a - bi)(a + bi)$.
(g) W tym przypadku mamy $2 = (1 + i)(1 - i) = (1 + i)^2 \cdot (-i)$. Wynika stąd, że każdy ideał pierwszy zawierający 2 zawiera też $1+i$. Pozostaje pokazać, że $1+i$ jest ideałem maksymalnym. Załóżmy, że nie, wtedy $1 + i = \alpha\beta$ dla pewnych nieodwracalnych α i β. Zatem

$$2 = |1 + i|^2 = |\alpha|^2 \cdot |\beta|^2.$$

To implikuje, że jedna z norm $|\alpha|^2$, $|\beta|^2$ jest równa 1, więc, na mocy zadania 1, odpowiedni element jest odwracalny. To przeczy wyborowi α, β.
(h) Zanim przystąpimy do rozwiązania podpunktu, zauważmy, że w sytuacji podpunktu (f) mamy $|a + bi|^2 = |a - bi|^2 = p$ jest liczbą pierwszą. Argumentując jak w podpunkcie (g), stwierdzamy, że ideały $(a + bi)\mathbb{Z}[i]$, $(a - bi)\mathbb{Z}[i]$ są pierwsze. Ponadto ideały te są różne. Zaiste, gdyby $(a + bi)\mathbb{Z}[i] = (a - bi)\mathbb{Z}[i]$, to otrzymujemy element

$$\mathbb{Z}[i] \ni \frac{a + bi}{a - bi} = \frac{(a + bi)^2}{|a - bi|^2} = \frac{a^2 - b^2 + 2abi}{p} = \frac{a^2 - b^2}{p} + i \cdot \frac{2ab}{p}.$$

Jednak liczby a i b są niepodzielne przez p, więc p nie dzieli $2ab$, co pokazuje, że ten element nie leży w $\mathbb{Z}[i]$; leży on w $\mathbb{Q}[i] \setminus \mathbb{Z}[i]$. To kończy część przygotowawczą.

Pogrupujmy ideały maksymalne $\mathfrak{p} \subseteq \mathbb{Z}[i]$ względem przecięcia $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Z podpunktów (e) i (f) wynika, że są co najwyżej dwa ideały $\mathfrak{p}$ zawierające daną liczbę p. Ponadto dla każdego z nich zachodzi $N(\mathfrak{p}) \geq p$, bowiem już podzbiór $\mathbb{Z}/(\mathbb{Z} \cap \mathfrak{p}) \subseteq \mathbb{Z}[i]/\mathfrak{p}$ ma p elementów. Stąd, $N(\mathfrak{p})^{-s} \leq p^{-s}$. Zatem iloczyn z treści podpunktu (h) jest bezwzględnie ograniczony z góry przez

$$\prod_{p \in \mathbb{P}} \left(\frac{1}{1 - p^{-s}} \right)^2.$$

Jak wiemy z wykładu, zaprezentowany iloczyn jest zbieżny dla każdego $s > 1$ i jego granicą jest $\zeta(s)^2$. Ta cała część pokazuje, że iloczyn z podpunktu (h) jest zbieżny bezwzględnie.

Pozbywszy się problemów zbieżności, obliczmy ten iloczyn dokładnie. Dla każdego $p \in \mathbb{P}$ rozważmy ideały $\mathfrak{p}$ takie, że $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Dla $p = 2$ na mocy punktu (g) jest jeden taki ideał i ma on normę $N(1+i) = 2$. Dla $p \equiv 3 \pmod 4$ na mocy punktu (e) jest znowu jeden taki ideał i ma on normę $N(p) = p^2$. Dla $p \equiv 1 \pmod 4$ są dwa ideały, oba o normie p. Otrzymujemy więc dla $s > 1$ równość

$$\zeta_{\mathbb{Z}[i]}(s) = \frac{1}{1-2^{-s}} \cdot \prod_{p \equiv 1 \pmod 4} \left(\frac{1}{1-p^{-s}}\right)^2 \cdot \prod_{p \equiv 3 \pmod 4} \frac{1}{1-(p^{-s})^2} =$$

$$\zeta(s) \cdot \prod_{p \equiv 1 \pmod 4} \frac{1}{1-p^{-s}} \cdot \prod_{p \equiv 3 \pmod 4} \frac{1-p^{-s}}{1-(p^{-s})^2} = \zeta(s) \prod_{p \equiv 1 \pmod 4} \frac{1}{1-p^{-s}} \cdot \prod_{p \equiv 3 \pmod 4} \frac{1}{1+p^{-s}} =$$

$$\zeta(s) \cdot L(s, \chi),$$

gdzie ostatnia równość wynika z zadania 3(b) z poprzedniej serii. (Zdumiewająco porządnie się zwinął ten wynik, prawda?)

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.

Rozwiązanie.

Norma $|\alpha|^2$ dla $\alpha = a + b\sqrt{-5}$ wynosi $|\alpha|^2 = a^2 + 5b^2$. Liczby a, b są całkowite, więc wynika stąd, że nie ma w A elementów o normie 2 lub normie 3 oraz że jedyne elementy o normie 1 to ± 1.

(a) Jeśli $2 = \alpha\beta$ to otrzymujemy $4 = |2|^2 = |\alpha|^2 \cdot |\beta|^2$. Norma nie jest równa 2, więc któraś z norm $|\alpha|^2$, $|\beta|^2$ jest równa jeden, zatem element α lub β jest odwracalny. To pokazuje, że 2 jest nierozkładalny, podobnie argumentujemy w pozostałych przypadkach.

(b) Zachodzi $2 \cdot 3 = (1-\sqrt{-5})(1+\sqrt{-5})$. Elementy po obu stronach są nierozkładalne. Gdyby A była dziedziną z jednoznacznością rozkładu, to elementy te byłyby pierwsze, więc musiałaby np. zachodzić podzielność 3 dzieli $1-\sqrt{-5}$ lub 3 dzieli $1+\sqrt{-5}$. Żadna z tych podzielności nie zachodzi, gdyż $|3|^2 = 9 > 6 = |1 \pm \sqrt{-5}|^2$.

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.*

Rozwiązanie.

Niech n_g będzie najmniejszą liczbą całkowitą dodatnią taką, że $n_g \cdot g \in \mathbb{Z}[x]$. Jeśli współczynniki wielomianu $n_g \cdot g$ są wszystkie podzielne przez pewną liczbę całkowitą $k > 1$, to w szczególności wiodący współczynnik, równy n_g, jest podzielny przez k, a ponadto $\frac{n_g}{k} \cdot g$ ma współczynniki całkowite. To przeczy definicji n_g. Zatem liczba k jak powyżej nie istnieje.

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

Zdefiniujmy podobnie n_h dla wielomianu h. Zachodzi równość $n_g \cdot g \cdot n_h \cdot h = (n_g n_h) \cdot f$. Załóżmy, że $n_g n_h > 1$ i weźmy liczbę pierwszą p dzielącą $n_g n_h$. Wtedy zachodzi

$$0 \equiv (n_g n_h) \cdot f = (n_g \cdot g) \cdot (n_h \cdot h) \pmod{p}.$$

Na mocy dyskusji o liczbie k powyżej, istnieje współczynnik $n_g \cdot g$ niepodzielny przez p. Załóżmy, że najmniejszą potęgą x, przy której stoi taki współczynnik jest x^{e_g}. Podobnie zdefiniujmy x^{e_h} dla wielomianu h. Wtedy współczynnik przy $x^{e_g+e_h}$ w $(n_g \cdot g) \cdot (n_h \cdot h)$ jest też niepodzielny przez p (dlaczego?). To daje sprzeczność. Wynika z niej, że $n_g n_h = 1$, czyli $n_g = n_h = 1$ i g, h mają współczynniki całkowite.

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 $\mathbb{Z}$.

Rozwiązanie.

Weźmy element całkowity i zapiszmy go jako a/b, gdzie $a, b \in \mathbb{Z}$ są liczbami względnie pierwszymi. Skoro element a/b spełnia wielomian unormowany, to zachodzi

$$\left(\frac{a}{b}\right)^d + n_{d-1}\left(\frac{a}{b}\right)^{d-1} + \ldots + n_0 = 0$$

dla pewnych $n_{d-1}, \ldots, n_0$ całkowitych. Domnażając przez b^d, otrzymujemy

$$a^d + n_{d-1} b a^{d-1} + \ldots + n_0 b^d = 0,$$

zatem b dzieli a^d. Ale a i b są względnie pierwsze, więc podzielność $b \mid a^d$ implikuje, że $b = \pm 1$. Wobec tego a/b jest liczbą całkowitą. *Uwaga: powyższy dowód nie używał niczego o $\mathbb{Z}$ poza jednoznacznością rozkładu; uogólnia się on do dowolnej dziedziny z jednoznacznością rozkładu.*

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.*

Rozwiązanie.

(To zadanie pojawi się w następnej serii.)