Teoria liczb
grupy klas, 12-15 czerwca

W poniższych zadaniach obliczeniowo użyteczne będzie lepsze oszacowanie stałej λ, która pojawiła się na ostatnim wykładzie. Mianowicie niech $\mathbb{Q} \subseteq K$ będzie skończonym rozszerzeniem ciał, gdzie $n = \dim_{\mathbb{Q}} K$, i niech t będzie połową liczby różnych zanurzeń $K \subseteq \mathbb{C}$ takich, że $K \not\subseteq \mathbb{R}$ (przykładowo $t = 1$ dla $K = \mathbb{Q}(i)$, bo K ma dwa zanurzenia. Podobnie, $t = 0$ dla $K = \mathbb{Q}(\sqrt{2})$, bo oba zanurzenia K mają obraz w $\mathbb{R}$). Niech

$$\lambda_K = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^t \sqrt{|\operatorname{disc}(\mathcal{O}_K)|}.$$

Wtedy zachodzi następujące twierdzenie: każdy niezerowy element grupy klas $\mathrm{Cl}(\mathcal{O}_K)$ jest postaci $[I]$, gdzie $I \subseteq \mathcal{O}_K$ jest ideałem takim, że $|\mathcal{O}_K/I| \leq \lambda_K$. W szczególności, zachodzi $|\mathbb{Z}/(\mathbb{Z} \cap I)| \leq \lambda_K$. Stałą λ_K nazywa się czasem *ograniczeniem Minkowskiego dla* K. Stała ta jest z reguły mniejsza niż stała λ z wykładu.
Stałą λ_K można obliczyć online na stronie https://sagecell.sagemath.org/, wpisując zapytanie podobne do

```
QQ[sqrt(-19)].minkowski_bound().n()
```

Zadanie 1. Niech $K = \mathbb{Q}(\sqrt{-d})$, gdzie $d \neq 0, 1$ jest całkowita i bezkwadratowa. Niech $A = \mathcal{O}_K$ będzie pierścieniem liczb całkowitych w K.

(a) Oblicz $\operatorname{disc}(\mathcal{O}_K)$ w zależności od reszty $d \mod 4$.

(b) Oblicz, że $\lambda_K < 2$ dla $-d = 2, 3, 5$ i wywnioskuj, że $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{3}]$, $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ są dziedzinami z jednoznacznością rozkładu.

(c) Wywnioskuj to samo dla $\mathbb{Z}[i]$ oraz $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$. Co dzieje się dla $\mathbb{Z}[\sqrt{-5}]$?

(d) Pokaż, że $\mathcal{O}_{\mathbb{Q}(\sqrt{-19})}$ jest dziedziną z jednoznacznością rozkładu. *To zamyka zadanie I z serii 11-15 maja.*

Rozwiązanie.
(a) Jeśli $-d \equiv 1 \pmod 4$, to $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{-d}}{2}$. Oznaczmy w tym przypadku $\alpha = \frac{1+\sqrt{-d}}{2}$ i mamy $\alpha^2 = \alpha - \frac{1+d}{4}$. W przeciwnym razie $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\sqrt{-d}$ i oznaczmy $\alpha = \sqrt{-d}$, zatem $\alpha^2 = d$. Zapiszmy też $\alpha^2 = b\alpha + c$, gdzie (b, c) są jak powyżej. W obu przypadkach obliczamy, że

$$\operatorname{disc}(\mathcal{O}_K) = \det \begin{pmatrix} \operatorname{Tr}(1) & \operatorname{Tr}(\alpha) \\ \operatorname{Tr}(\alpha) & \operatorname{Tr}(\alpha^2) \end{pmatrix}$$

Macierz elementu 1 w naszych bazach to

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

zatem $\operatorname{Tr}(1) = 2$. Macierz elementu α to

$$\begin{pmatrix} 0 & c \\ 1 & b \end{pmatrix}$$

zatem $\mathrm{Tr}(\alpha) = b$. Wreszcie, macierz elementu α^2 to kwadrat macierzy elementu α, więc jest ona równa

$$\begin{pmatrix} c & bc \\ b & c+b^2 \end{pmatrix}$$

i mamy $\mathrm{Tr}(\alpha^2) = 2c + b^2$. Zatem

$$\mathrm{disc}(\mathcal{O}_K) = \det \begin{pmatrix} 2 & b \\ b & 2c+b^2 \end{pmatrix} = 4c + 2b^2 - b^2 = 4c - b^2.$$

Podstawiając wartości liczbowe, stwierdzamy, że $\mathrm{disc}(\mathcal{O}_K) = -4d$, jeśli $-d \not\equiv 1 \pmod 4$ oraz $\mathrm{disc}(\mathcal{O}_K) = -d$, jeśli $-d \equiv 1 \pmod 4$. *Można zobaczyć, że końcowy wynik $4c - b^2$ to kwadrat różnicy wartości pierwiastków równania $x^2 - bx + c$, sławetna "Delta".*

(b) Przykładowo dla $\mathbb{Z}[\sqrt{3}]$ mamy $t = 0$ oraz $\mathrm{disc}(\mathbb{Z}[\sqrt{3}]) = 4 \cdot 3$, więc stała Minkowskiego λ_K wynosi $\frac{2!}{2^2} \cdot \sqrt{4 \cdot 3} = \sqrt{3} < 2$. Z twierdzenia wynika, że każdy niezerowy element grupy klas jest postaci $[I]$, gdzie I jest ideałem takim, że $|\mathcal{O}_K/I| < 2$. Ale jedynym ideałem spełniającym ten warunek jest $\mathcal{O}_K = I$, który jest główny. Zatem grupa klas jest jednoelementowa.

(c) Obliczenia są podobne. Przedyskutujmy przypadek $\mathbb{Z}[\sqrt{-5}]$. Stała Minkowskiego wynosi $\frac{4}{\pi}\sqrt{5} < 3$, więc wystarczy rozważyć klasy $[I]$ takie, że $\mathbb{Z}[\sqrt{-5}]/I$ jest dwuelementowym pierścieniem. Takie ideały niegłówne faktycznie istnieją, patrz zadanie 2 z serii 17-20 kwietnia.

(d) Obliczamy, że $\lambda_{\mathbb{Q}(\sqrt{-19})}$ wynosi $\frac{2}{\pi}\sqrt{19} < 3$. Pozostaje rozważyć, czy istnieją ideały I takie, że $\mathcal{O}_{\mathbb{Q}(\sqrt{-19})}/I$ ma dwa elementy. Jeśli istnieją, to te elementy to 0 oraz 1. W szczególności, musi zachodzić

$$\frac{1+\sqrt{-19}}{2} \in I \quad \text{lub} \quad \frac{1+\sqrt{-19}}{2} - 1 \in I.$$

W szczególności zachodzi też $N\left(\frac{1+\sqrt{-19}}{2}\right) \in I$ lub $N\left(\frac{1+\sqrt{-19}}{2} - 1\right) \in I$. Obliczamy, że

$$N\left(\frac{1+\sqrt{-19}}{2}\right) = \frac{1+\sqrt{-19}}{2} \cdot \frac{1-\sqrt{-19}}{2} = 5$$

$$N\left(\frac{1+\sqrt{-19}}{2} - 1\right) = N\left(\frac{-1+\sqrt{-19}}{2}\right) = \frac{-1+\sqrt{-19}}{2} \cdot \frac{-1-\sqrt{-19}}{2} = 5,$$

więc w obu przypadkach $5 \in I$. Skoro również $2 \in I$, to $1 = 5 - 2 \cdot 2 \in I$, zatem I jest całym pierścieniem, w szczególności $|\mathcal{O}_{\mathbb{Q}(\sqrt{-19})}/I| \neq 2$, sprzeczność. Zatem żądane ideały I nie istnieją.

Zadanie 2. Załóżmy, że dla pewnego ciała K zachodzi $\lambda_K \leq 2$. Niech $n = \dim_{\mathbb{Q}} K$. Pokaż, że grupa klas ciała K ma co najwyżej $2^n - 1$ elementów.

Rozwiązanie.

(To zadanie nie wchodzi w wymagania egzaminacyjne.)

Z wyniku Minkowskiego wynika, że każda nietrywialna klasa w $\mathrm{Cl}\,\mathcal{O}_K$ jest równa $[I]$, gdzie $|\mathcal{O}_K/I| \leq 2$. Jeśli $|\mathcal{O}_K/I| = 1$, to $I = \mathcal{O}_K$ jest główny, więc $[I]$ jest trywialna. Możemy więc założyć, że $|\mathcal{O}_K/I| = 2$. W szczególności, wynika stąd, że $2 \in I$.

Z twierdzenia o jednoznaczności rozkładu z wykładu wynika, że $2\mathcal{O}_K = \mathfrak{p}_1^{a_1} \dots \mathfrak{p}_r^{a_r}$, gdzie $a_i \in \mathbb{Z}_+$ spełniają $\sum a_i \leq n$. Skoro $2 \in I$, to $2\mathcal{O}_K$, a zatem z tego samego twierdzenia wynika $I = \mathfrak{p}_1^{b_1} \dots \mathfrak{p}_r^{b_r}$, gdzie $b_i \neq a_i$.

Wybór liczb b_i determinuje I. W szczególności wynika stąd, że mamy co najwyżej $(a_1+1)(a_2+1)\dots(a_r+1)$ możliwych wyborów I. Dla dowolnych liczb całkowitych $b, c > 0$ zachodzi $(b+1)(c+1) > b+c+1$, wobec tego dla każdego a_i zachodzi $a_i + 1 \leq (1+1)^{a_i}$, więc

$$(a_1+1)(a_2+1)\dots(a_r+1) \leq (1+1)^{\sum a_i} \leq 2^n.$$

Ponadto wybór $b_i = a_i$ oraz wybór $b_i = 0$ dają ideały $2\mathcal{O}_K$ oraz $\mathcal{O}_K$, oba główne. Zatem te dwa wybory prowadzą do tego samego elementu grupy klas. To pokazuje, że różnych klas jest co najwyżej $2^n - 1$.

Zadanie 3. Niech $K = \mathbb{Q}(\sqrt{-31})$ i niech $A = \mathcal{O}_K$.

(a) Oblicz stałą Minkowskiego dla K.

(b) Pokaż, że ideał $3A$ jest maksymalny. *Wskazówka: rozważ iloraz lub oblicz bezpośrednio, że każdy element spoza ideału jest odwracalny modulo ideał.*

(c) Pokaż, że $2A = \mathfrak{m}_1 \cdot \mathfrak{m}_2$, gdzie $\mathfrak{m}_1 \neq \mathfrak{m}_2$ są różnymi ideałami maksymalnymi. Pokaż, że nie są one główne.

(d) Wywnioskuj z oszacowania Minkowskiego, że grupa klas A ma trzy elementy.

Rozwiązanie.
(a) Korzystając z obliczenia wyróżnika w zadaniu 1, mamy $\lambda_K = \frac{2}{\pi}\sqrt{31} < \frac{2}{3}\sqrt{36} = 4$.
(b) Niech $\alpha = \frac{1+\sqrt{-31}}{2}$. Skoro $-31 \equiv 1 \pmod 4$, to jak wiemy z poprzednich zadań, pierścień A jest równy $\mathbb{Z}[\alpha] = \mathbb{Z} \oplus \mathbb{Z}\alpha$. Niech $a, b \in \mathbb{Z}$. Element $a + b\alpha = a + \frac{b}{2} + \frac{b\sqrt{-31}}{2}$ ma normę zespoloną równą

$$\left(a + \frac{b}{2}\right)^2 + b^2\frac{31}{4} = a^2 + ab + 8b^2.$$

Załóżmy, że $3A$ nie jest maksymalny i niech $I \neq A$ będzie ideałem takim, że $3A \subsetneq I$. Zatem ideał I posiada element postaci $a + b\alpha$, gdzie $a \not\equiv 0 \pmod 3$ lub $b \not\equiv 0 \pmod 3$. Norma $a^2 + ab + 8b^2 = |a + b\alpha|^2$ jest równa $(a + b\alpha)(a - b\alpha + b)$, więc ta norma jest elementem I.

Twierdzimy, że norma $a^2 + ab + 8b^2$ jest niepodzielna przez 3. Faktycznie,

$$a^2 + ab + 8b^2 \equiv (a-b)^2 + b^2 \pmod 3.$$

Kwadraty dają resztę 0 lub 1 modulo 3, więc jeśli $0 \equiv (a-b)^2 + b^2 \pmod 3$, to $a - b \equiv 0 \pmod 3$ oraz $b \equiv 0 \pmod 3$. Stąd $a \equiv b \equiv 0 \pmod 3$, sprzeczność z wyborem a, b. Zatem norma $a^2 + ab + 8b^2$ jest niepodzielna przez 3. Skoro zarówno $3 \in I$ jak i $a^2 + ab + 8b^2 \in I$, to $1 \in I$, sprzeczność.
(c) Niech $\mathfrak{m}_1 = (2, \alpha)$. Obliczmy, że $\alpha^2 = \alpha - 8$. Weźmy dowolny element tego ideału. Jest on postaci

$$2(a + b\alpha) + (c + d\alpha)\alpha = (2a - 8d) + (2b + c + d)\alpha,$$

zatem $\mathfrak{m}_1 = 2\mathbb{Z} \oplus \mathbb{Z}\alpha$. Iloraz $A/\mathfrak{m}_1$ ma więc dwa elementy, zatem jest ciałem, czyli $\mathfrak{m}_1$ jest maksymalny. Niech $\mathfrak{m}_2 = (2, \overline{\alpha}) = (2, -\alpha + 1)$, gdzie $\overline{\alpha}$ oznacza sprzężenie zespolone. Iloraz $A/\mathfrak{m}_1$ jest izomorficzny z $A/\mathfrak{m}_2$, więc również ideał $\mathfrak{m}_2$ jest maksymalny. Ponadto $1 \in \mathfrak{m}_1 + \mathfrak{m}_2$, więc w szczególności $\mathfrak{m}_1 \neq \mathfrak{m}_2$. Obliczamy teraz

$$\mathfrak{m}_1 \cdot \mathfrak{m}_2 = (2, \alpha) \cdot (2, -\alpha + 1) = \big(4, 2(-\alpha + 1), 2\alpha, -\alpha^2 + \alpha\big) = (4, -2\alpha + 2, 2\alpha, 8) = (2).$$

(d) Z oszacowania Minkowskiego wynika, że każdy niezerowy element grupy kals jest postaci $[I]$, gdzie $|A/I| \leq 3$. Jeśli $|A/I| = 3$, to $|\mathbb{Z}/(\mathbb{Z} \cap I)|$ jest dzielnikiem trójki, więc $3 \in I$. Ale wtedy z punktu (b) mamy $I = 3A$ oraz $|A/I| = |A/3A| = 3^2$, sprzeczność. Podobnie, $|A/I| = 1$ prowadzi do sprzeczności. Zatem $|A/I| = 2$ i $2 \in I$.

Z punktu (c) wiemy, że $2A = \mathfrak{m}_1 \cdot \mathfrak{m}_2$. Z twierdzenia o rozkładzie oraz z tego, że $2A \subseteq I$ wynika, że $I = \mathfrak{m}_1^{b_1}\mathfrak{m}_2^{b_2}$, gdzie $b_1, b_2 \leq 1$. Sprawdzamy wszystkie przypadki (można tę procedurę skrócić, nieco finezyjniej argumentując). Jeśli $b_1 = b_2 = 1$, to $I = 2A$ i $|A/I| = 2^2$, sprzeczność. Jeśli $b_1 = b_2 = 0$, to $I = A$ i ponownie sprzeczność. Jeśli $b_1 = 1$, $b_2 = 0$, to $I = \mathfrak{m}_1$. Podobnie, jeśli $b_1 = 0$, $b_2 = 1$, to $I = \mathfrak{m}_2$. Wnioskujemy stąd, że grupa klas ma co najwyżej trzy elementy.

Skoro $\mathfrak{m}_1$ nie jest główny, to ta grupa jest nietrywialna. Skoro $2A = \mathfrak{m}_1 \cdot \mathfrak{m}_2$, to w grupie klas zachodzi $[\mathfrak{m}_1] \cdot [\mathfrak{m}_2] = 1_{\mathrm{Cl}\, A}$. Jeśli $[\mathfrak{m}_1] = [\mathfrak{m}_2]$, to $[\mathfrak{m}_1]^2 = 1_{\mathrm{Cl}\, A}$, więc ideał $\mathfrak{m}_1^2$ byłby główny. Ale $\mathfrak{m}_1^2 = (4, 2\alpha, \alpha^2) = (4, 2\alpha, \alpha - 8) = (4, 2\alpha, \alpha) = (4, \alpha)$ i można, na przykład korzystając z norm elementów, sprawdzić, że nie jest to ideał główny. Zatem $[\mathfrak{m}_1] \neq [\mathfrak{m}_2]$. Stąd wynika, że $\mathrm{Cl}\, A = \{[\mathfrak{m}_1], [\mathfrak{m}_2], 1_{\mathrm{Cl}\, A}\}$ jest trójelementowa.

Zadanie 4. $\star$ Niech $\mathbb{Q} \subseteq K$ będzie skończonym rozszerzeniem.

(a) Niech I będzie niezerowym ideałem w $\mathcal{O}_K$. Pokaż, że istnieje m takie, że I^m jest główny, załóżmy, że $I^m = \alpha\mathcal{O}_K$.

(b) Niech $L = K(\sqrt[m]{\alpha})$. Pokaż, że ideał $I\mathcal{O}_L$ jest główny.

(c) Pokaż, że istnieje skończone rozszerzenie $K \subseteq L$ takie, że dla każdego niezerowego ideału $I \subseteq \mathcal{O}_K$ ideał $I\mathcal{O}_L$ jest główny.

Rozwiązanie.

(To zadanie nie było rozpoczęte na ćwiczeniach. Rozwiązanie do przemyślenia dla chętnych.)