Teoria liczb
elementy całkowite, 24-27 kwietnia

Zadanie 1. Niech $K \subseteq \mathbb{C}$ będzie ciałem i niech $d = \dim_{\mathbb{Q}} K$.

(a) Niech $\alpha \in K$ i niech e będzie stopniem jego wielomianu minimalnego. Uzasadnij, że e dzieli d. W szczególności zachodzi $e \leq d$.

(b) Jaki stopień może mieć wielomian minimalny liczby postaci $\sqrt{n} + \sqrt{m}$, gdzie $n, m \in \mathbb{Z}$?

Rozwiązanie.
(a) Niech $L = \mathbb{Q}(\alpha)$. Wtedy $\dim_{\mathbb{Q}} L = e$, jak wiemy z wykładu. Ponadto K jest przestrzenią liniową nad L, więc $d = \dim_{\mathbb{Q}} K = (\dim_{\mathbb{Q}} L) \cdot (\dim_L K) = e \cdot (\dim_L K)$.
(b) Z poprzedniego podpunktu, możliwości to 1, 2 oraz 4. Stopnie jeden oraz dwa są realizowane na przykład przez $\sqrt{1} + \sqrt{1}$, $\sqrt{1} + \sqrt{2}$ odpowiednio. Stopień 4 jest realizowany na przykład przez $\sqrt{2} + \sqrt{3}$, bowiem $\sqrt{2}$, $\sqrt{3}$, $\sqrt{2 \cdot 3}$ są liniowo niezależne nad $\mathbb{Q}$, patrz następne zadanie, a więc również liczby

$$1, \quad \sqrt{2} + \sqrt{3}, \quad 5 + 2\sqrt{6}, \quad 11\sqrt{2} + 9\sqrt{3}$$

są liniowo niezależne. To pokazuje, że stopień wielomianu minimalnego $\sqrt{2} + \sqrt{3}$ to co najmniej cztery. Z (a) wynika, że to co najwyżej cztery.

Zadanie 2. Niech $n_1, \ldots, n_k$ będą liczbami całkowitymi takimi, że dla $i \neq j$ liczba $n_i n_j$ nie jest kwadratem liczby całkowitej. Celem tego zadania jest pokazanie, że $\sqrt{n_1}, \ldots, \sqrt{n_k}$ są liniowo niezależne nad $\mathbb{Q}$.

(a) Jaki jest minimalny wielomian $\sqrt{n_i n_j}$ dla $i \neq j$?

(b) Niech $K = \mathbb{Q}(\sqrt{n_1}, \ldots, \sqrt{n_k})$. Pokaż, że $\mathrm{Tr}(\sqrt{n_i n_j}) = 0$ dla każdych $i \neq j$, gdzie ślad jest liczony w K.

(c) Niech $d = \dim_{\mathbb{Q}} K$. Załóżmy, że $\sum_{i=1}^{k} q_i \sqrt{n_i} = 0$ dla pewnych $q_i \in \mathbb{Q}$. Weźmy $j \in \{1, \ldots, k\}$. Oblicz, że

$$dq_j n_j = \mathrm{Tr}\left(\sqrt{n_j} \sum_{i=1}^{k} q_i \sqrt{n_i}\right) = 0$$

i wywnioskuj, że $q_j = 0$. Zatem $\sqrt{n_1}, \ldots, \sqrt{n_k}$ są liniowo niezależne.

(d) Niech $p_1, \ldots, p_r$ będą parami różnymi liczbami pierwszymi i niech $L = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_r})$. Pokaż, że $\dim_{\mathbb{Q}} L = 2^r$. *Wskazówka: wypisz bazę złożoną z pierwiastków.*

Rozwiązanie.
(a) Z założenia, liczba $\sqrt{n_i n_j}$ nie jest całkowita, więc jej wielomian minimalny ma stopień co najmniej dwa. Ponadto spełnia ona wielomian $x^2 - n_i n_j$. Zatem to on jest minimalny.
(b) Z wykładu wiemy, że $\mathrm{Tr}(\sqrt{n_i n_j}) = -a_{\deg(f)-1} \cdot \dim_{\mathbb{Q}(\sqrt{n_i n_j})} K$, gdzie $a_{\deg(f)-1}$ jest współczynnikiem przy $x^{\deg(f)-1}$ w wielomianie minimalnym $f = x^2 - n_i n_j$. Zatem $a_1 = 0$, więc i ślad jest zerowy.
(c) Z definicji, $\mathrm{Tr}(-)$ jest funkcją $\mathbb{Q}$-liniową (ale nie K-liniową!!). Ponadto $\mathrm{Tr}(q_j n_j) = dq_j n_j$, bo w dowolnej bazie ciała K macierz mnożenia przez $q_j n_j \in \mathbb{Q}$ jest diagonalna. Zatem z jednej strony

$$\mathrm{Tr}\left(\sqrt{n_j} \sum_{i=1}^{k} q_i \sqrt{n_i}\right) = \sum_{i=1}^{k} q_i \,\mathrm{Tr}\left(\sqrt{n_i n_j}\right) = dq_j n_j.$$

Z drugiej strony, mamy z założenia $\sum_{i=1}^{k} q_i\sqrt{n_i} = 0$, więc po lewej stronie mamy $\mathrm{Tr}(0) = 0$. Zatem $dq_j n_j = 0$. Skoro $n_j n_i$ nie jest kwadratem dla $i \neq j$, to $n_j \neq 0$, czyli z $dq_j n_j = 0$ wynika $q_j = 0$. Uzyskujemy to dla każdego j, więc elementy $\sqrt{n_1}, \ldots, \sqrt{n_k}$ są liniowo niezależne.
(d) Dla każdych $a_1, \ldots, a_r \in \{0, 1\}$ liczba $\sqrt{p_1^{a_1} \ldots p_r^{a_r}}$ leży w L. Zbiór tych liczb jest liniowo niezależny nad $\mathbb{Q}$ na mocy poprzedniego podpunktu. Co więcej, rozpina on ciało L, co sprawdzamy bezpośrednio. Zatem jest on bazą, czyli $\dim_{\mathbb{Q}} L = 2^r$.

Zadanie 3. Niech $K \subseteq \mathbb{C}$ będzie ciałem takim, że $\dim_{\mathbb{Q}} K = d$ jest skończony. Elementowi α przypisujemy *normę* $N(\alpha)$ tego elementu jako wyznacznik macierzy $M(\alpha) \in \mathbb{M}_{d\times d}(\mathbb{Q})$, która definiuje mnożenie przez α w K; jest to definicja analogiczna do definicji śladu z wykładu.

(a) Pokaż, że $N(\alpha)N(\beta) = N(\alpha\beta)$ dla każdych $\alpha, \beta \in K$.

(b) Pokaż, że jeśli $\alpha \in \mathcal{O}_K$ to $N(\alpha) \in \mathbb{Z}$.

(c) Pokaż, że jeśli $K = \mathbb{Q}(\sqrt{-d})$, gdzie $d > 1$ jest liczbą bezkwadratową, to $N(\alpha) = |\alpha|^2$ dla każdego $\alpha \in K$.

(d) Pokaż, że jeśli $K = \mathbb{Q}(\sqrt{d})$, gdzie $d > 1$ jest liczbą bezkwadratową, to może się zdarzyć, że $N(\alpha) < 0$.

Rozwiązanie.
Niech dla $\gamma \in K$ macierz $M(\gamma) \in \mathbb{M}_{d\times d}(\mathbb{Q})$ oznacza macierz mnożenia przez γ w K, traktowanego jako przekształcenie liniowe. Wtedy $N(\gamma) = \det M(\gamma)$.
(a) Mamy $M(\alpha\beta) = M(\alpha)M(\beta)$ bezpośrednio z definicji, zatem

$$N(\alpha\beta) = \det(M(\alpha\beta)) = \det(M(\alpha))\det(M(\beta)) = N(\alpha)N(\beta).$$

(b) Argumentujemy podobnie jak na wykładzie: jeśli $K = \mathbb{Q}(\alpha)$, to bierzemy bazę 1, α, $\ldots$,α^{d-1} tego ciała. Załóżmy, że $f = x^d + a_{d-1}x^{d-1} + \ldots + a_0 \in \mathbb{Q}[x]$ jest wielomianem minimalnym dla elementu α. Skoro α jest całkowity, to z argumentu z lematu Gaussa wiemy, że $f \in \mathbb{Z}[x]$. Zatem $\alpha \cdot \alpha^{d-1} = \alpha^d = -a_{d-1}\alpha^{d-1} - \ldots - a_0$.

Macierz mnożenia przez α w bazie 1, α, $\ldots$, α^{d-1} wynosi

$$M(\alpha) = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & 0 & \ldots & 0 & -a_2 \\ 0 & 0 & 1 & \ldots & 0 & -a_3 \\ & & \ldots & & & \\ 0 & 0 & \ldots & 0 & 1 & -a_{d-1} \end{pmatrix}$$

Pozostaje policzyć jej wyznacznik. Zamieniając kolejno wiersze pierwszy i drugi, drugi i trzeci, $\ldots$, $(d-1)$-wszy i d-ty, zmieniamy wyznacznik o $(-1)^{d-1}$ i otrzymujemy macierz górnietrójkątną

$$\begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & 0 & \ldots & 0 & -a_2 \\ 0 & 0 & 1 & \ldots & 0 & -a_3 \\ & & \ldots & & & \\ 0 & 0 & \ldots & 0 & 1 & -a_{d-1} \\ 0 & 0 & 0 & \ldots & 0 & -a_0 \end{pmatrix}$$

która ma wyznacznik $-a_0$. Zatem wyjściowa macierz $M(\alpha)$ ma wyznacznik $(-1)^d a_0$, gdzie a_0 jest wyrazem wolnym wielomianu minimalnego α. Jeśli zaś $K \neq \mathbb{Q}(\alpha)$, to wybieramy bazę $b_1, \ldots, b_r$ ciała K traktowanego jako przestrzeń liniowa nad $L = \mathbb{Q}(\alpha)$. Jak w zadaniu 1(a), bazą K nad $\mathbb{Q}$ jest wtedy ciąg $\{b_i\alpha^j \mid 1 \leq i \leq r, 0 \leq j \leq d-1\}$. W tej bazie macierz $M(\alpha)$ składa się z r kopii macierzy powyżej, ułożonych diagonalnie (sprawdź!). Obliczamy zatem, że norma $N(\alpha)$ wynosi $((-1)^{\deg(f)}a_0)^r$, gdzie a_0 jest wyrazem wolnym wielomianu minimalnego f elementu α. To jest element całkowity.
(c) Niech $\alpha = a + b\sqrt{-d}$. Jeśli $b = 0$, to $N(\alpha) = a^2 = |a|^2$. Jeśli $b \neq 0$, to wielomian minimalny α to $(x-\alpha)(x-\overline{\alpha}) = x^2 - (\alpha+\overline{\alpha})x + \alpha\overline{\alpha}$. Zatem $N(\alpha) = (-1)^2\alpha\overline{\alpha} = |\alpha|^2$.
(d) Weźmy przykładowo element $\alpha = \sqrt{d}$. Jego wielomianem minimalnym jest $x^2 - d$, więc $N(\alpha) = -d$.

Zadanie 4. Niech $\mathbb{Q} \subseteq K \subseteq L$ będą ciałami i niech $\alpha \in K$. Porównaj ślad oraz normę α traktowanego jako element K oraz jako element L.

Rozwiązanie.

Niech Tr^K, Tr^L oznaczają ślad w K oraz L odpowiednio; podobnie N^K, N^L. Mamy wtedy

$$\mathrm{Tr}^L(\alpha) = \mathrm{Tr}^K(\alpha)\dim_{\mathbb{K}} L \qquad \text{oraz} \qquad N^L(\alpha) = (N^K(\alpha))^{\dim_K L}.$$

Wzroy te wynikają na przykład z obliczeń śladu i normy jak w zadaniu 4(b).

Zadanie 5. Niech p będzie nieparzystą liczbą pierwszą.

(a) Niech $\alpha \in \mathbb{Z}[\omega_p]$, gdzie ω_p jest pierwiastkiem p-tego stopnia z jedynki. Uzasadnij, że stopień wielomianu minimalnego α dzieli liczbę $p-1$.

(b) ($\star$, dla osób po Algebrze II) Załóżmy, że α jest stopnia dwa. Pokaż, że α jest $\mathbb{Q}$-liniową kombinacją 1 oraz $\sqrt{(-1)^{\frac{p-1}{2}}p}$. *Wskazówka: zadanie 4 serii 5 (tej z 3-13 kwietnia).*

Rozwiązanie.

(a) Z zadania 3 serii 5 wynika, że $\dim_{\mathbb{Q}} \mathbb{Q}(\omega_p) = p-1$. Zatem teza wynika z zadania 1(a) bieżącej serii.
(b) Ciało $\mathbb{Q}(\omega_p)$ jest ciałem rozkładu wielomianu $x^p - 1$, więc rozszerzenie $\mathbb{Q} \subseteq \mathbb{Q}(\omega_p)$ jest Galois z grupą Galois $\mathbb{Z}_{p-1}$. Ta grupa ma dokładnie jedną podgrupę indeksu dwa, więc $\mathbb{Q}(\omega_p)$ zawiera jedyne ciało K takie, że $\dim_{\mathbb{Q}} K = 2$. Z założenia, ciało $\mathbb{Q}(\alpha)$ jest stopnia dwa, więc $\mathbb{Q}(\alpha) = K$ jest tym jedynym podciałem.
Z zadania 4 serii 5 wynika, że $\sqrt{(-1)^{\frac{p-1}{2}}p}$ jest elementem w $\mathbb{Q}(\omega_p)$. Jest on stopnia dwa, więc $\mathbb{Q}(\sqrt{(-1)^{\frac{p-1}{2}}p}) = K = \mathbb{Q}(\alpha)$. To znaczy, że α jest $\mathbb{Q}$-liniową kombinacją 1 i $\sqrt{(-1)^{\frac{p-1}{2}}p}$.