PAWS 2025: ANALYSIS AND IMPLEMENTATION OF ALGORITHMS IN NUMBER THEORY
PROBLEM SET 3

THOMAS BOUCHET, KATE FINNERTY, ASIMINA S. HAMAKIOTES, YONGYUAN HUANG

Below are the exercises for Problem Set 3. The questions are loosely in ascending order of difficulty. Feel free to skip around and try whatever exercises would be the most helpful for you. Try as many as you can but don't feel like you need to complete them all!

1. Beginner problems

Question 1: Let α be an algebraic number with minimal polynomial $\sum_{i=0}^{n} a_i x^i$. Show that $\mathrm{Tr}(\alpha) = -a_{n-1}$ and $\mathrm{Nm}(\alpha) = (-1)^n a_0$.

Question 2: Let K be the cyclotomic field $\mathbb{Q}(\zeta_5)$, where ζ_5 is a primitive 5th root of unity. Compute

(1) $\mathrm{disc}(1, \zeta_5, \zeta_5^2, 1 + \zeta_5 + \zeta_5^2)$.
(2) $\mathrm{disc}(1, \zeta_5, \zeta_5^2, \zeta_5^3)$.
(3) $\mathrm{disc}\left(1, \zeta_5, \dfrac{\zeta_5^2}{5}, \zeta_5^3\right)$.

Question 3: Let $f(x) = x^3 - x - 1$, and let $\alpha \in \overline{\mathbb{Q}}$ such that $f(\alpha) = 0$. Show that $\{1, \alpha, \alpha^2\}$ is an integral basis of $\mathcal{O}_{\mathbb{Q}(\alpha)}$.

Question 4: Let K be a number field of degree n over $\mathbb{Q}$ and let $\alpha \in K$ be an algebraic number with minimal polynomial of degree m. Show that the following hold.

(1) m divides n.
(2) $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \dfrac{n}{m}\mathrm{Tr}(\alpha)$.
(3) $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha) = (\mathrm{Nm}(\alpha))^{n/m}$.

Question 5: Prove Lemma 3.25 from the Lecture Notes.

Lemma. *Let K be a number field. For all $\alpha \in K$, there exists a nonzero $d \in \mathbb{Z}$ such that $d\alpha \in \mathcal{O}_K$.*

2. Intermediate problems

Question 6: Consider $K = \mathbb{Q}(\sqrt{d})$ for a squarefree integer d.

(1) Compute the discriminant of the polynomial $x^2 - d$.
(2) Calculate the discriminant of $\{1, \sqrt{d}\}$, in two different ways.

(3) Recall Question 1 of Problem Set 2. What is the discriminant of K?

Question 7: Verify using `Magma` that the number of quadratic fields of absolute discriminant x is asymptotic to $\frac{6}{\pi^2}x$, i.e. the number

$$Z(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z}; x) = \#\{L/\mathbb{Q} : [L : \mathbb{Q}] = 2, |\operatorname{disc}(L)| \leq x\}$$

approaches $\frac{6}{\pi^2}x$ as x grows.

Question 8: Prove Lemma 3.31 from the Lecture Notes.

Lemma. *If $\{\omega_1, \ldots, \omega_n\}$ and $\{\omega_1', \ldots, \omega_n'\}$ are two integral bases for the ring of integers $\mathcal{O}_K$ of a number field K, then*

$$\operatorname{disc}(\omega_1, \ldots, \omega_n) = \operatorname{disc}(\omega_1', \ldots, \omega_n').$$

Question 9: Let $K = \mathbb{Q}(\theta)$, where θ is an algebraic integer with minimal polynomial $m_\theta(x) \in \mathbb{Z}[x]$ of degree n. Show that the following hold

(1) $\operatorname{disc}(1, \theta, \ldots, \theta^{n-1}) = \operatorname{disc}(m_\theta(x))$;
(2) if $f = [\mathcal{O}_K : \mathbb{Z}[\theta]]$, then

$$\operatorname{disc}(m_\theta(x)) = \operatorname{disc}(K)f^2,$$

where $\operatorname{disc}(m_\theta(x))$ denotes the discriminant of the polynomial $m_\theta(x)$: if $\theta_1, \ldots, \theta_n$ are the roots of $m_\theta(x)$, then

$$\operatorname{disc}(m_\theta(x)) = \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)^2.$$

Hint: You may find the Vandermonde determinant helpful for part (1). Please also feel free to check out the hint in Exercise 3.38 in the Lecture Notes.

3. Advanced problems

Question 10: Let $K = \mathbb{Q}(\zeta_n)$ be a cyclotomic field. Show that $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$. First consider the case when n is prime.

Question 11: Let $K = \mathbb{Q}(\alpha)$, where α is a root of $X^3 - X - 1$. Let us fix $\alpha_1, \alpha_2, \alpha_3$ the complex roots of $X^3 - X - 1$. The different embeddings of K into $\mathbb{C}$ are the $\sigma_i : \alpha \mapsto \alpha_i$.

We know that the map $\sigma : K \to \mathbb{C}^3$, which sends $x \in K$ to $\sigma(x) = (\sigma_1(x), \sigma_2(x), \sigma_3(x))$, is injective. In this exercise, we use this injectivity to represent elements of K as 3-tuples of complex numbers, and simplify operations. We use the fact that integers are easily recognizable as complex numbers (given that we have enough precision to begin with).

(1) Let L be a number field. Show that if $\beta \in L$ there exists $N \in \mathbb{Z}$ such that $N \cdot \beta \in \mathcal{O}_L$.
(2) Let L be a number field. Show that if $\beta \in \mathcal{O}_L$, then $\frac{\mathcal{N}(\beta)}{\beta} \in \mathcal{O}_L$.
(3) Now, we go back to our case $K = \mathbb{Q}(\alpha)$, where α is a root of $X^3 - X - 1$. Show that any element in $\mathcal{O}_K$ can be written as $a + b\alpha + c\alpha^2$, for $a, b, c \in \mathbb{Z}$.

(4) We introduce the matrix $M = \begin{pmatrix} 1 & \sigma_1(\alpha) & \sigma_1(\alpha)^2 \\ 1 & \sigma_2(\alpha) & \sigma_2(\alpha)^2 \\ 1 & \sigma_3(\alpha) & \sigma_3(\alpha)^2 \end{pmatrix}$. Show that for any $x = a + b\alpha + c\alpha^2 \in K$,

$$(\sigma_1(x), \sigma_2(x), \sigma_3(x))^T = M \cdot (a, b, c)^T.$$

Note that one can also retrieve (a, b, c) in terms of $(\sigma_1(x), \sigma_2(x), \sigma_3(x))$.

(5) Let $x = 201\alpha^2 - 6458\alpha + 11$ and $y = 519\alpha^2 - 457\alpha + 326$ be elements of $\mathcal{O}_K$.

(a) Using `Magma`, Compute $\sigma(x)$ and $\sigma(y)$. You can use the built-in function `Conjugates`.

(b) Compute the component-wise product of $\sigma(x)$ and $\sigma(y)$, and the component-wise division of $\sigma(x)$ by $\sigma(y)$.

(c) Using (4), retrieve the decomposition of $x \cdot y$ in the base $\{1, \alpha, \alpha^2\}$.

(d) Can we do the same for the division? Fix that problem using (2), and find the decomposition of x/y in the base $\{1, \alpha, \alpha^2\}$.

(6) Can you give a few pros and cons of that method compared to the algebraic computation?