Algebraic number theory — Exercise sheet 1

`https://www.maths.tcd.ie/~mascotn/teaching/2026/MAU34109/index.html`

Version: September 28, 2026

Submit your answers in class or to neumayec@tcd.ie by Thursday October 8, 1pm.

Exercise 1.1: A polynomial of degree 3 (100 pts)

Let $F(x) = x^3 - 4x + 1 \in \mathbb{Q}[x]$. We admit without proof that $F(x)$ has three real roots, which are approximately -2.11, 0.25, and 1.86.
Let $K = \mathbb{Q}(\alpha)$, where α is a root of $F(x)$, and let $\beta = \alpha^2 - 4 \in K$.

1. (5 pts) Prove that $F(x)$ is irreducible over $\mathbb{Q}$.
2. (5 pts) Why is it important that $F(x)$ be irreducible over $\mathbb{Q}$ for the definition of K?
3. (5 pts) What is the extension degree $[K : \mathbb{Q}]$?
4. (10 pts) What is the signature of K?
5. (10 pts) Write down the matrix of multiplication by α with respect to the $\mathbb{Q}$-basis of K of your choice (clearly say which basis you are using).
6. (20 pts) Hence or otherwise, determine $\mathrm{Tr}_{\mathbb{Q}}^{K}(\beta)$ and $N_{\mathbb{Q}}^{K}(\beta)$. Your results must be exact; approximations are not good enough (unless you somehow manage to prove that they are exact).
7. (15 pts) Explain how the approximate values of the roots of $F(x)$ may be used to confirm that your calculations for $\mathrm{Tr}_{\mathbb{Q}}^{K}(\beta)$ and $N_{\mathbb{Q}}^{K}(\beta)$ are correct, at least approximately.
8. (10 pts) Prove that there exist rational numbers $a, b, c \in \mathbb{Q}$ such that $1/\beta = a + b\alpha + c\alpha^2$. Are a, b, c unique? Justify your answer.
9. (20 pts) Sketch two different methods that you could use to determine a, b, c as in the previous question (but do not actually determine them).

This was the only mandatory exercise, that you must submit before the deadline. The following exercises are not mandatory; they are not worth any points, and you do not have to submit them. However, I highly recommend that you try to solve them for practice (especially the warm-up exercise just below), and you are welcome to email me if you have questions about them. The solutions will be made available with the solution to the mandatory exercise.

Exercise 1.2: Warm up: review of methods

Let $K = \mathbb{Q}(\sqrt{3})$, and let $\alpha = a + b\sqrt{3}$ $(a, b \in \mathbb{Q})$ be an element of K. Express the trace, norm, and characteristic polynomial of α (with respect to the extension $K/\mathbb{Q}$) in terms of a and b

1. by writing down the matrix of the multiplication-by-α map with respect to the $\mathbb{Q}$-basis of K of your choice,

2. by considering complex embeddings (*Hint:* $K = \mathbb{Q}(\alpha)$ *where* $\alpha^2 = 3$).

Remark: This exercise is meant as a warm up for the next exercises, so as to remind you that some computations can be done in different ways. In the other exercises, remember that depending on the situation, some methods require less efforts than others!

Exercise 1.3: A biquadratic extension

1. Let $K = \mathbb{Q}(\sqrt{2})$. Prove that $\sqrt{5} \notin K$.

2. Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{5})$. Determine $[L : \mathbb{Q}]$, and find a $\mathbb{Q}$-basis of L.

3. What is the signature of L?

4. Let $\alpha = \sqrt{2} + \sqrt{5} \in L$. Write down the matrix of

$$\begin{aligned} \mu_\alpha : L &\longrightarrow L \\ x &\longmapsto \alpha x \end{aligned}$$

   with respect to the $\mathbb{Q}$-basis of L that you found in question 2.

5. Deduce the value of $\operatorname{Tr}^L_{\mathbb{Q}}(\alpha)$.

6. Determine the norm $N^L_{\mathbb{Q}}(\alpha)$ of α.

   Note: It is possible to do this without computing a big determinant.

7. The characteristic polynomial $\chi^L_{\mathbb{Q}}(\alpha)$ of α turns out to be $x^4 - 14x^2 + 9$ (we admit this without proof). Is it squarefree? What does this tell us about α?

8. Compute the characteristic polynomial $\chi^L_K(\alpha)$ of α with respect to the extension L/K.

Exercise 1.4: Computations in $\mathbb{Q}(\sqrt[3]{2})$

1. Prove that $x^3 - 2$ is irreducible over $\mathbb{Q}$.

2. Let $K = \mathbb{Q}(\sqrt[3]{2})$, and let $\alpha = \frac{\sqrt[3]{2}+1}{\sqrt[3]{2}-1} \in K$. Find $a, b, c \in \mathbb{Q}$ such that $\alpha = a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2$.

3. Are these rational numbers a, b, c unique ?

4. What is the degree of K over $\mathbb{Q}$?
5. Prove that $\sqrt{2} \notin K$.

   Hint: Think in terms of degrees.
6. Prove that $K = \mathbb{Q}(\alpha)$.
7. Compute the trace, norm, and characteristic polynomial of α.
8. What is the minimal polynomial of α over $\mathbb{Q}$?

Exercise 1.5: Resultant practice

1. Let $\gamma = \sqrt{3} - \sqrt[3]{2}$. Express a non-zero polynomial in $\mathbb{Q}[x]$ vanishing at γ as a resultant, and then express this resultant as a determinant.

   You are not required to compute this determinant explicitly. All this questions asks is to express this polynomial as a resultant, and then as a determinant, but you are not required to compute this polynomial explicitly.
2. Let $K = \mathbb{Q}(\alpha)$ be a number field, let $A(x) \in \mathbb{Q}[x]$ be the minimal polynomial of α, and let $\beta = B(\alpha) \in K$, where $B(x) \in \mathbb{Q}[x]$ is some polynomial. Express the characteristic polynomial $\chi_{\mathbb{Q}}^{K}(\beta)$ of β in terms of a resultant involving A and B.

   Hint: Think in terms of complex embeddings.

Exercise 1.6: (Non)-repeated values of complex embeddings

Let K be a number field of degree $n = [K : \mathbb{Q}]$, fix $\alpha \in K$, and let $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$.

Prove that α is a primitive element for $K/\mathbb{Q}$ if and only if the values $\{\sigma(\alpha), \sigma \in \operatorname{Hom}(K, \mathbb{C})\}$ are all distinct.

More generally (without assuming that α is a primitive element), relate the values $\{\sigma(\alpha), \sigma \in \operatorname{Hom}(K, \mathbb{C})\}$ to the roots of the characteristic polynomial and of the minimal polynomial of α. How many times is each value $\sigma(\alpha)$ repeated in $\{\sigma(\alpha), \sigma \in \operatorname{Hom}(K, \mathbb{C})\}$?