MAU34109-1

Coláiste na Tríonóide, Baile Átha Cliath
Trinity College Dublin
Ollscoil Átha Cliath | The University of Dublin

Faculty of Science, Technology, Engineering and Mathematics

School of Mathematics

JS/SS Maths/TP/TJH **Michaelmas 2024-25**

MAU34109 Algebraic number theory

Wednesday 04 December **Dargan theatre** **14:00 – 16:00**

Dr. Nicolas Mascot

Instructions to candidates:

This exam consists of **one** Question.
This Question is devoted to the study of various properties of the number field $K = \mathbb{Q}(\alpha)$ where α is a root of $A(x) = x^3 + 2x^2 - 6x + 2$.
In order to guide you, this Question is divided into several Parts, numbered from 1 to 5.
Parts 3, 4, and 5 are independent from each other (but rely on the results of Parts 1 and 2), and can thus be solved as if they were independent exercises.
In order to solve any question, you are allowed to assume the result of any **previous** question.
The use of non-programmable calculators and of the standard booklet of formulae and tables is allowed.

You may not start this examination until you are instructed to do so by the Invigilator.

Question 1 *A cubic field (100 pts)*

Let $A(x) = x^3 + 2x^2 - 6x + 2 \in \mathbb{Q}[x]$, which assumes the following values:

n	-4	-3	-2	-1	0	1	2
$A(n)$	-6	11	14	9	2	-1	$6.$

Part 1/5 (10 pts)

1a. (2 pts) Prove that all the complex roots of $A(x)$ are actually real.

1b. (2 pts) Prove that $A(x)$ is irreducible over $\mathbb{Q}$.

In what follows, we let $K = \mathbb{Q}(\alpha)$, where α is a root of $A(x)$.

1c. (1 pt) Determine the extension degree $[K : \mathbb{Q}]$.

1d. (5 pts) Let $n \in \mathbb{Z}$. Prove that the norm $N^K_{\mathbb{Q}}(\alpha + n)$ of $\alpha + n$ is

$$N^K_{\mathbb{Q}}(\alpha + n) = -A(-n).$$

Part 2/5 (10 pts)

2a. (8 pts) We admit without proof that the discriminant of $A(x)$ is

$$\operatorname{disc} A = 2^2 \cdot 101,$$

where 101 is prime. Prove that the ring of integers of K is $\mathbb{Z}[\alpha]$.

2b. (2 pts) Which prime numbers $p \in \mathbb{N}$ ramify in K?

Part 3/5 (30 pts)

3a. (8 pts) Determine explicitly the shape of the decomposition of the ideal $p\mathbb{Z}_K$ into prime ideals for $p = 2$, and then for $p = 3$. You must specify the number of factors, their ramification index, their residue degree, and their norm; but you are not required to provide explicit generators for these factors.

3b. (3 pts) State the formula for the Minkowski bound of a number field.

3c. (3 pts) Give an explicit expression (but do not attempt to evaluate it) for the Minkowski bound M_K of K.

You are not required to calculate the value of M_K, so your final answer should look like $\sqrt{\pi}\log 2$ rather than $1.23\cdots$. However you must specify explicitly the value of the invariants of K involved in M_K; e.g. do not write the degree as n without explicitly saying what the value of n is.

3d. (8 pts) We admit without proof that $M_K = 4.47\cdots$. Prove that $\mathbb{Z}_K$ is a PID.

3e. (6 pts) For each of the prime ideals $\mathfrak{p}$ that you found in question 3a., find a generator, that is to say an element $\gamma_\mathfrak{p} \in \mathbb{Z}_K$ such that $\mathfrak{p} = (\gamma_\mathfrak{p})$.

You may express these generators $\gamma_\mathfrak{p}$ as fractions; you are not required to simplify them.

3f. (2 pts) Is $\gamma_\mathfrak{p}$ unique for each $\mathfrak{p}$?

Part 4/5 (35 pts)

The purpose of this Part is to investigate the units of K.

We write U_K for the group of units in K. We say that a unit is nontrivial if it is not ± 1.

4a. (4 pts) What is the rank of U_K?

4b. (3 pts) Which roots of unity does U_K contain?

4c. (2 pts) Use the table of values of $A(x)$ provided at the beginning of the exercise to find a nontrivial unit $v \in U_K$.

4d. (5 pts) Use the decomposition of the prime $p = 2$ in K to find another nontrivial unit $w \in U_K$.

Let $\sigma_1, \sigma_2, \sigma_3$ be the embeddings of K into $\mathbb{R}$. We define the sign map S as

$$\begin{array}{rccl} S: & K^\times & \longrightarrow & \{+,-\}^3 \\ & \beta & \longmapsto & \big(\operatorname{sign}\sigma_1(\beta), \operatorname{sign}\sigma_2(\beta), \operatorname{sign}\sigma_3(\beta)\big). \end{array}$$

For example, $S(\beta) = (-,-,+)$ would mean that $\sigma_1(\beta) < 0$ and $\sigma_2(\beta) < 0$ but $\sigma_3(\beta) > 0$.

4e. (4 pts) Prove that $S(v) = (-,-,+)$ and that $S(w) = (-,+,+)$ (up to re-ordering $\{\sigma_1, \sigma_2, \sigma_3\}$, in case you did not order the embeddings in the same way I did).

Hints: Using the table of values of $A(x)$, for each root $z \in \mathbb{R}$ of $A(x)$, find an integer $n \in \mathbb{Z}$ such that $n < z < n+1$. And use the most convenient expression of w!

4f. (4 pts) Hence or otherwise, prove that there does not exist any unit $\varepsilon \in U_K$ such that v and w both lie in $\{\pm\varepsilon^n \mid n \in \mathbb{Z}\}$.

4g. (5 pts) Explain why the regulator of v and w is defined, and prove that it is nonzero.

4h. (4 pts) Give an explicit expression for the regulator of v and w in terms of the real roots $\alpha_1, \alpha_2, \alpha_3$ of $A(x)$ (but do not attempt to evaluate it).

4i. (4 pts) Explain how you could test whether $\{v, w\}$ is a system of fundamental units of K if you knew the regulator of K. How would the regulator of K be related to the regulator of $\{v, w\}$ if $\{v, w\}$ were not a system of fundamental units?

Part 5/5 (15 pts)

Let $\gamma = \alpha + 5$. The purpose of this final Part is to investigate whether γ is a square in K.

5a. (5 pts) Prove that if there existed $\delta \in K$ such that $\gamma = \delta^2$, then δ would lie in the ring of integers of K.

5b. (10 pts) Deduce that γ is actually not a square in K, i.e. that there does not exist any $\delta \in K$ such that $\gamma = \delta^2$.

Hint: Reduce modulo a prime ideal.

END