Durham University

EXAMINATION PAPER

Examination Session:	Year:	Exam Code:
May/June	2025	MATH41620-WE01

Title:
Number Theory V

Time:	3 hours	
Additional Material provided:		
Materials Permitted:		
Calculators Permitted:	Yes	Models Permitted: Casio FX83 series or FX85 series.

Instructions to Candidates:	Answer all questions. Section A is worth 30%, Section B is worth 60%, and Section C is worth 10%. Within Sections A and B, all questions carry equal marks. Write your answer in the white-covered answer booklet with barcodes. Begin your answer to each question on a new page.

Revision:	

ED01/2025

SECTION A

Q1 (a) Let R be an integral domain. Define what it means for R to be a Euclidean Domain.

(b) Let R be a Euclidean Domain with Euclidean function ϕ. Show that if $a, b \in R \setminus \{0\}$ and b is a non-unit, then $\phi(ab) > \phi(a)$. *(Hint: divide a by ab with remainder.)*

Q2 (a) Show that $\sqrt{-2} + \sqrt{-22}$ is not a root of any monic quadratic polynomial with coefficients in $\mathbb{Q}$.

(b) Is $\frac{1+\sqrt{11}}{3\sqrt{-2}}$ an algebraic integer? Justify your answer.

Q3 (a) Find the fundamental unit in $\mathbb{Z}[\frac{1+\sqrt{13}}{2}]$.

(b) Find all the solutions of the equation

$$x^2 - 13y^2 = 1,$$

where $x, y \in \mathbb{Z}$.

SECTION B

Q4 Let $K = \mathbb{Q}(\sqrt{5})$ and $A = \mathbb{Z}[\sqrt{5}]$.

(a) Prove that $\mathfrak{p} = (2, 1 + \sqrt{5})_A$ is a maximal ideal of A.

(b) Prove that $\mathfrak{p}^2 = 2\mathfrak{p}$.

(c) Prove that there is no ideal I of A such that $I\mathfrak{p} = (2)_A$. *(Note that $A \neq \mathcal{O}_K$, so prime ideals may not have inverses, unique factorisation into prime ideals may fail, the ideal norm is not necessarily multiplicative and Kummer–Dedekind does not apply to A.)*

Q5 Let $\alpha \in \mathbb{C}$ be a root of a polynomial

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \qquad a_i \in \mathbb{Z},\ n \geq 2,$$

such that there exists a prime number p dividing a_i for $0 \leq i \leq n-1$ but p^2 does not divide a_0. Let $K = \mathbb{Q}(\alpha)$.

(a) Show that $\alpha^n/p \in \mathcal{O}_K$ and that p^2 does not divide $N_K(\alpha)$.

(b) Suppose that p divides $|\mathcal{O}_K/\mathbb{Z}[\alpha]|$. Show that there is an element $\xi \in \mathcal{O}_K$ such that $\xi \notin \mathbb{Z}[\alpha]$ and such that

$$p\xi = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}, \qquad b_i \in \mathbb{Z},$$

where not all of the b_i are divisible by p. *(Hint: Use Cauchy's theorem that a finite group whose order is divisible by p has an element of order p.)*

(c) Let ξ be as in the previous part and let $j \geq 0$ be the least index such that b_j is not divisible by p. Show that

$$(b_j\alpha^{n-1})/p \in \mathcal{O}_K.$$

(Hint: You may want to start by considering the case $j = 0$.)

(d) Consider the norm $N_K((b_j\alpha^{n-1})/p)$ to prove that p does not divide $|\mathcal{O}_K/\mathbb{Z}[\alpha]|$.

Q6 You are given that the polynomial $f(x) = x^3 - x^2 - 2x - 8$ is irreducible over $\mathbb{Q}$. Let $\theta \in \mathbb{C}$ be a root of $f(x)$ and $K = \mathbb{Q}(\theta)$.

(a) Compute $\Delta_K(1, \theta, \theta^2)$.

(b) You are given that $\beta = (\theta^2 + \theta)/2 \in \mathcal{O}_K$. Compute $\Delta_K(1, \theta, \beta)$ by relating it to $\Delta_K(1, \theta, \theta^2)$. Use a result from the lectures applied to the full lattice $S = \mathbb{Z}[1, \theta, \beta] \subseteq \mathcal{O}_K$ to deduce that $\mathbb{Z}[1, \theta, \beta] = \mathcal{O}_K$.

Q7 (a) Show that $\mathbb{Q}(\sqrt{6})$ has class number 1. You may use the Minkowski bound, given by $B_K = \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{|\Delta_K|}$.

(b) Let $K = \mathbb{Q}(\sqrt{-65})$ and $R = \mathcal{O}_K$. Let $\mathfrak{p}$ be a prime ideal of R that divides $(3)_R$. Show that $[\mathfrak{p}]$ has order 4 in the class group $Cl(R)$. *(Hint: consider the element $4 + \sqrt{-65}$.)*

SECTION C

Q8 (a) Determine the p-adic expansion of $\frac{-1}{1-p}$, for an arbitrary prime number p.

(b) Determine the 5-adic expansion of $\frac{2}{3}$.

(c) Show that a p-adic integer

$$a = a_0 + a_1 p + a_2 p^2 + \cdots$$

is a unit in $\mathbb{Z}_p$ (i.e., has a multiplicative inverse that is also a p-adic integer) if and only if $a_0 \neq 0$.