Durham University

EXAMINATION PAPER

Examination Session:	Year:	Exam Code:
May	2019	MATH4211-WE01

Title:
Number Theory IV

Time Allowed:	3 hours	
Additional Material provided:	None	
Materials Permitted:	None	
Calculators Permitted:	Yes	Models Permitted: Casio fx-83 GTPLUS or Casio fx-85 GTPLUS.
Visiting Students may use dictionaries: No		

Instructions to Candidates:	Credit will be given for: the best **TWO** answers from Section A, the best **THREE** answers from Section B, **AND** the answer to the question in Section C. Questions in Section B and C carry **TWICE** as many marks as those in Section A.

Revision:	

ED01/2019

SECTION A

1. Let p be an odd prime and $\zeta = e^{2\pi i/p}$ a p-th root of unity.

   (a) Show that the minimal polynomial of ζ over $\mathbb{Q}$ is equal to

   $$\Phi(x) = x^{p-1} + x^{p-2} + \ldots + 1.$$

   (b) Write R for the ring of integers of $\mathbb{Q}(\zeta)$. Show that for all $j = 1, 2, \ldots, p-1$ we have

   $$\frac{1-\zeta^j}{1-\zeta} \in R^\times.$$

2. Given that the ring $\mathbb{Z}[i]$ is a Euclidean Domain, find the number of solutions (a, b) with $a, b \in \mathbb{Z}$ of the equation

   $$a^2 + b^2 = 2^3 \times 3^4 \times 37^7.$$

   Carefully justify every step of your answer.

3. Let $R = \mathbb{Z}[\sqrt{-5}]$.

   (a) Let $\mathfrak{p} \subset R$ be a non-zero prime ideal in R. Show that there exists a unique prime $p \in \mathbb{Z}$ such that $\mathfrak{p} \supseteq (p)_R$.

   (b) Find the inverse of the ideal $I = (3, 2-\sqrt{-5})_R$.

   (c) With notation as above, is I a prime ideal? Justify your answer.

4. (a) Find the fundamental unit in $\mathbb{Z}[\sqrt{11}]$.

   (b) Let $d \in \mathbb{Z}$ with $d > 1$. Prove that if $x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ is a unit such that $x + y\sqrt{d} > 1$, then $x > 0$ and $y > 0$.

   (c) Give formulae for the solutions $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ to $x^2 - 11y^2 = 5$. (You may use that $\mathbb{Z}[\sqrt{11}]$ is a UFD.)

5. Let $K = \mathbb{Q}(\sqrt{-23})$ and $R = \mathcal{O}_K$. Let $I_1 = (2, \frac{1+\sqrt{-23}}{2})_R$ and $I_2 = (3, \frac{1+\sqrt{-23}}{2})_R$.

   (a) Compute the norm of the ideal I_1.

   (b) Show that $[I_1] = [I_2]^{-1}$ in the class group of R.

   (c) Show that $[I_1] \neq [I_2]$ in the class group of R.

6. (a) Let K be a number field of degree $n = [K : \mathbb{Q}]$ and Δ_K its discriminant. Show that

   $$|\Delta_K| \geqslant \left(\frac{\pi}{4}\right)^n \frac{n^{2n}}{(n!)^2}.$$

   (b) Let $K = \mathbb{Q}(\sqrt{d})$, where d is a square-free integer. Show that the class number h_K is 1 when $2 \leq d \leq 5$.

SECTION B

7. (a) Show that the ring $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean Domain.

   (b) Let R be the ring of integers of a number field K. A function $\phi : R \setminus \{0\} \to \mathbb{N}$ is called a *Dedekind-Hasse* function if for any non-zero elements $a, b \in R$ either $a \in (b)_R$ or there is a non-zero $x \in (a, b)_R$ such that $\phi(x) < \phi(b)$.

      (i) Show that an R for which a Dedekind-Hasse function exists is a Principal Ideal Domain.

      (ii) Assume now that R is a Principal Ideal Domain and hence also a Unique Factorization Domain. Define a function $\phi : R \setminus \{0\} \to \mathbb{N}$ by setting $\phi(u) = 1$ if $u \in R^\times$ and $\phi(r) = 2^n$ if $r = p_1 p_2 \cdots p_n$ where $p_i \in R$ are irreducible. Show that ϕ is a Dedekind-Hasse function.

      (iii) Assume again that R is a Principal Ideal Domain. Show that the function $\phi(r) := |N_{K/\mathbb{Q}}(r)|$ (the absolute value of the norm) is a Dedekind-Hasse function.
      (Hint: Here you may want to use the fact that an $r \in R$ is a unit if and only if $N_{K/\mathbb{Q}}(r) = \pm 1$.)

8. Let $K = \mathbb{Q}(\sqrt{d})$ for some square-free integer d with $d \neq 0, 1$, and write R for the ring of integers of K.

   (a) (i) Show that the norm of ideals of R is multiplicative, that is $N(IJ) = N(I)N(J)$ for non-zero ideals $I, J \subseteq R$.

      (ii) Let $p \in \mathbb{Z}$ be an odd prime and assume that $d \equiv m^2 \not\equiv 0 \pmod{p}$ for some integer m. Show that $(p)_R = \mathfrak{p}\widetilde{\mathfrak{p}}$ with $\mathfrak{p} \neq \widetilde{\mathfrak{p}}$, where $\mathfrak{p} = (p, m - \sqrt{d})_R$.

   (b) In the notation above we take $d = -29$.

      (i) Find the number of ideals in R of norm equal to 33, and of norm equal to 275. Justify your answer.

      (ii) Are there any non-principal ideals of norm 33? If yes, then give such an ideal by listing a set of generators for it.

9. (a) Let $K = \mathbb{Q}(\theta)$ where $\theta \in \mathbb{C}$ is such that $\theta^3 - \theta - 2 = 0$. Compute the discriminant of $\mathbb{Z}[\theta]$ and prove that $\mathbb{Z}[\theta] = \mathcal{O}_K$.

   (b) Let p be an odd prime, $\zeta = e^{2\pi i/p}$ a p-th root of unity, and $K = \mathbb{Q}(\zeta)$. Compute the discriminant Δ_K.

10. Let $K = \mathbb{Q}(\sqrt{-17})$ and $R = \mathcal{O}_K$.

   (a) Decompose the ideals $(2)_R$, $(3)_R$ and $(5)_R$ into products of prime ideals.

   (b) Find all the ideals in R of norm at most 5.

   (c) Show that the class number h_K is at most 5.

   (d) Determine the class number h_K.

SECTION C

11. Let $p \in \mathbb{Z}$ be a prime and for a non-zero $a \in \mathbb{Z}$ define $ord_p(a)$ as the highest power of p dividing a, and set $ord_p\left(\frac{a}{b}\right) := ord_p(a) - ord_p(b)$ where a, b are non-zero integers. We set $|x|_p := p^{-ord_p(x)}$ if $x \in \mathbb{Q}^\times$, and $|x|_p = 0$ otherwise.

   (i) Show that $|x+y|_p \leq \max(|x|_p, |y|_p)$ for $x, y \in \mathbb{Q}$.

   (ii) Show that for a non-zero $x \in \mathbb{Q}$ we have that
   $$\prod_p |x|_p = |x|^{-1},$$
   where the product is over all primes p and $|x|$ denotes the usual absolute value on $\mathbb{Q}$.

   (iii) Let $x \in \mathbb{Q}$ with $|x|_p \leq 1$ for some fixed prime p. Show that for every $i \in \mathbb{N}$ there exists an integer $a \in \{0, 1, 2, \ldots, p^i - 1\}$ such that $|a - x|_p \leq p^{-i}$.

   (iv) Let $\{c_i\}$ be any sequence in $\mathbb{Q}_p$ (the field of p-adic numbers) for some fixed prime p and assume that $|c_i|_p \to 0$ as $i \to \infty$. Show that the series $\sum_{i=0}^{\infty} c_i$ converges in $\mathbb{Q}_p$.

   (v) Let $p \in \mathbb{Z}$ be a prime and suppose that n is a non-zero integer not divisible by p. Show that for any $\alpha \in \mathbb{Z}_p$ (the ring of p-adic integers) with $|\alpha - 1|_p < 1$ there exists a $\beta \in \mathbb{Q}_p$ such that $\beta^n = \alpha$.