Durham University

EXAMINATION PAPER

Examination Session:	Year:	Exam Code:
May	2017	MATH3031-WE01

Title: Number Theory III

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 **FOUR** answers from Section A and the best **THREE** answers from Section B. Questions in Section B carry **TWICE** as many marks as those in Section A.

Revision:	

ED01/2017

University of Durham Copyright

SECTION A

1. (i) Prove that there are no integral solutions to the Diophantine equation

$$15x^2 - 7y^2 = 1.$$

(ii) Let $R = \mathbb{Z}[\sqrt{d}]$, where $d < -1$ is an odd integer.

(a) Prove that 2 is an irreducible element in R.

(b) Using the previous part or otherwise, prove that R is not a UFD.
[*Hint: You may consider the element* $1 - d$].

2. (a) What is the full ring of integers $\mathcal{O}_{-11}$ in $K = \mathbb{Q}(\sqrt{-11})$?

(b) Put $\alpha = -5 + \sqrt{-11}$ and $\beta = 7 + \sqrt{-11}$. By considering β/α, or otherwise, find $\gamma \in \mathcal{O}_{-11}$ such that

$$N_{K/\mathbb{Q}}(\beta - \gamma\alpha) < N_{K/\mathbb{Q}}(\alpha)\,.$$

(c) Let $R = \mathbb{Z}[\sqrt{-11}]$ and put $J = (3, 1+\sqrt{-11})_R$. Show that $J^2 = (9, a+\sqrt{-11})_R$ for some integer a.

3. (i) Let $K = \mathbb{Q}(\sqrt{3})$. Let $\mathcal{O}_3$ be the number ring of K. Then prove that $\alpha \in \mathcal{O}_3$ is a unit if and only if $|N_{K/\mathbb{Q}}(\alpha)| = 1$.

(ii) Let $K = \mathbb{Q}(\alpha)$, where α is a root of the polynomial $x^3 + 14x + 7$. Find the degree $[K : \mathbb{Q}]$ and calculate the trace $Tr_{K/\mathbb{Q}}(\beta)$ for $\beta = \alpha^2 - \alpha - 1$.

4. (i) (a) Give the ring of integers $\mathcal{O}_{69}$ of $\mathbb{Q}(\sqrt{69})$ and find its fundamental unit.

(b) Give all solutions in integers x, y , if any, of $x^2 - 69y^2 = 4$.

(ii) Let $R = \mathbb{Z}[\sqrt{-74}]$. Factorise the ideal $(13 - \sqrt{-74})_R$ as a product of prime ideals. Determine which, if any, of these are principal ideals and show that R has an ideal class of order 5.

5. (i) Let $R = \mathbb{Z}[\sqrt{-31}]$. Calculate the norm $N(I)$ of the ideal in R given by

$$I = (2 - \sqrt{-31}, 3 + 2\sqrt{-31})_R$$

and exhibit a fractional ideal F such that $I\,F = R$.

(ii) Determine how many solutions there are to the equation

$$x^2 + 2y^2 = 11^{11}$$

such that x is not divisible by 11.
[You may use that $\mathbb{Z}[\sqrt{-2}]$ is a UFD, but you should emphasise at which point you are invoking this.]

6. Let $R = \mathcal{O}_{-23}$.
Consider the ideals $I_1 = (3, -2 + \sqrt{-23})_R$ and $I_2 = (8, 1 + \sqrt{-23})_R$ in R.

(a) Do I_1 and I_2 lie in the same ideal class?

(b) Is either one of I_1 or I_2 principal?

University of Durham Copyright

SECTION B

7. (i) Let $m \neq n$ be two square-free integers, i.e. they are products of distinct primes. Prove that $\mathbb{Q}(\sqrt{m}) \neq \mathbb{Q}(\sqrt{n})$.

   (ii) Given any integer n, let $\omega_n = \exp(2\pi i/n)$ denote a primitive n-th root of unity. The fields $\mathbb{Q}(\omega_n) = \mathbb{Q}[\omega_n]$ are called *cyclotomic* extensions of $\mathbb{Q}$.

   (a) For any positive integer n, prove that $\omega_{2n}^2 = \omega_n$ and $-\omega_{2n}^{n+1} = \omega_{2n}$.

   (b) Using the above relations, or otherwise, prove that $\mathbb{Q}[\omega_n] = \mathbb{Q}[\omega_{2n}]$, where n is a positive odd integer.

   (iii) Give an example of a quadratic extension of $\mathbb{Q}$ which is also a cyclotomic extension.

8. (i) Show that $\mathbb{Z}[\sqrt{-11}]$ contains elements of norm 53 and 103, respectively. How many integer solutions are there to

$$x^2 + 11y^2 = 2^2 \cdot 53^5 \cdot 103^7 \ ?$$

   How many integer solutions with x, y positive are there?
   [You may assume that $\mathbb{Z}[(1+\sqrt{-11})/2]$ is a UFD and that the only units in this ring are ± 1.]

   (ii) In this part, you may use that $\mathbb{Z}[i]$ is a UFD.

   (a) Factorise 2 as a product of primes in $\mathbb{Z}[i]$.

   (b) Prove that the equation

$$(x + 16i)(x - 16i) = y^3,$$

   would necessarily imply that $x + 16i$ is a cube in $\mathbb{Z}[i]$.

   (b) Prove that the Diophantine equation

$$x^2 + 256 = y^3$$

   has at most finitely many solutions where x and y are integers.
   [Carefully justify your method.]

9. Determine the ideal class group of $K = \mathbb{Q}(\sqrt{-39})$.
   [You may assume that every ideal class contains an ideal of norm no more than B_K, where, in the usual notation, $B_K = \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{|\Delta_K|}$.]

10. Let $K = \mathbb{Q}(\theta)$ where θ is a root of $f(x) = x^3 - 3x - 3$.

   (a) Find the norm and trace of $\theta^2 + 1$.

   (b) Find the discriminant $\Delta_K(\mathbb{Z}[\theta])$ and show that $\mathcal{O}_K = \mathbb{Z}[\theta]$.

   (c) Show that the class number of K is 1.
   [You may use the formula from Question 9.]

University of Durham Copyright