EXAMINATION PAPER

Examination Session:	Year:	Exam Code:
May/June	2021	MATH41620-WE01

Title: Number Theory

Time (for guidance only):	3 hours	
Additional Material provided:		
Materials Permitted:		
Calculators Permitted:	Yes	Models Permitted: There is no restriction on the model of calculator which may be used.

Instructions to Candidates:	Credit will be given for your answers to all questions. All questions carry the same marks. Please start each question on a new page. Please write your CIS username at the top of each page. To receive credit, your answers must show your working and explain your reasoning.

Revision:	

ED01/2021

Q1 Let p be a prime integer. In the following we make the convention that for a p-adic expansion $\sum_{n=m}^{\infty} a_n p^n \in \mathbb{Q}_p$ with $m \in \mathbb{Z}$, we select $a_n \in \{0, 1 \ldots, p-1\}$.

1.1 Assume that $a \in \mathbb{Q}_p$ has p-adic expansion $\sum_{n=-m}^{\infty} c_n p^n$ for some $m \in \mathbb{N}$. Give the p-adic expansion of $-a$ in terms of the c_n's. Justify your answer.

1.2 (i) Let $0 \neq a = p^k \sum_{n=0}^{\infty} a_n p^n \in \mathbb{Q}_p$, with $k \in \mathbb{Z}$, and write $a^{-1} = p^{-k} \sum_{n=0}^{\infty} b_n p^n$. Show that for any $m \in \mathbb{N}$, the numbers $b_0, b_1, \ldots, b_m$ can be determined by $a_0, a_1, \ldots, a_m$.

(ii) Show that $\frac{1}{7} \in \mathbb{Z}_5$. Further, if we write $\frac{1}{7} = \sum_{n=0}^{\infty} a_n 5^n$ then determine $a_0, a_1, a_2, a_3 \in \{0, 1, 2, 3, 4\}$. Show your working.

1.3 Assume that $a \in \mathbb{Q}_p$ is of the form $a = p^{2n-1} b$ with $b \in \mathbb{Z}_p^\times$ for some $n \in \mathbb{N}$. Is $\sqrt{a} \in \mathbb{Q}_p$? Justify your answer.

1.4 (i) Let $a \in \mathbb{Z}_p$ and write $b := a^{p-1}$. Show that $a \in \mathbb{Z}_p^\times$ if and only if $\sqrt[n]{b} \in \mathbb{Z}_p$ for infinitely many $n \in \mathbb{N}$.

(ii) Show that the only field automorphism of $\mathbb{Q}_p$ is the identity.

Q2 **2.1** Let $f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_1 x + a_0 \in \mathbb{Z}[x]$. Let p be a prime factor of a_0 and write $r \in \mathbb{N}$ such that p^r divides a_0 and p^{r+1} does not. Assume further that all a_i for $i = 1, \ldots, n-1$ are divisible by p^r and that the polynomial $f(x)$ is irreducible over $\mathbb{Q}$. Denote by R the ring of integers of $\mathbb{Q}(\alpha)$, where $\alpha \in \mathbb{C}$ such that $f(\alpha) = 0$. Show that:

(i) There is an ideal I in R such that $(p^r)_R = I^n$.

(ii) If r and n are relatively prime then there exists an ideal J in R such that $(p)_R = J^n$.

2.2 Let K be a number field and write $\mathcal{O}_K$ for its ring of integers.

(i) Let I be a non-zero proper ideal in $\mathcal{O}_K$. Show that there exists an element $\gamma \in K$ such that $\gamma \notin \mathcal{O}_K$ and $(\gamma)_R I \subset \mathcal{O}_K$.

(ii) Let F be a finite extension of K and write $\mathcal{O}_F$ for the ring of integers of F. Let I be a proper ideal of $\mathcal{O}_K$, and consider the set

$$\mathfrak{I} := \left\{ \sum_{i=1}^{n} a_i r_i \;\middle|\; n \in \mathbb{N}, a_i \in I, r_i \in \mathcal{O}_F \right\}.$$

A. Show that $\mathfrak{I}$ is an ideal in $\mathcal{O}_F$.

B. Show that $\mathfrak{I} \neq \mathcal{O}_F$.

C. Show that we may select F such that $\mathfrak{I}$ is a principal ideal in $\mathcal{O}_F$.

Q3 **3.1** Let $i \in \mathbb{C}$ with $i^2 = -1$. Is the ring $\mathbb{Z}[2i] := \{a + 2bi \mid a, b \in \mathbb{Z}\}$ a UFD? Justify your answer.

3.2 Let d be a square-free integer with $d \equiv 1 \pmod 4$. Write $K = \mathbb{Q}(\sqrt{d})$, and denote by R the ring of integers of K. For p an odd prime, show that if $(p)_{\mathbb{Z}}$ is not inert in K, then there exists an integer b with $0 \leq b \leq p-1$ such that p divides $N_{K/\mathbb{Q}}(b + \frac{1+\sqrt{d}}{2})$.

3.3 Let $K = \mathbb{Q}(\sqrt{-65})$, and write R for its ring of integers. Factorise the ideal $(75 - 15\sqrt{-65}, -195 - 15\sqrt{-65})_R$ into a product of prime ideals in R.

Q4 Let $K = \mathbb{Q}(\sqrt{7}, \sqrt{10})$ and fix any $\alpha \in \mathcal{O}_K$ such that $K = \mathbb{Q}(\alpha)$. Let $f(x) \in \mathbb{Z}[x]$ be the irreducible monic polynomial for which $f(\alpha) = 0$. Throughout this question, given a polynomial $g(x) \in \mathbb{Z}[x]$ let $\overline{g}(x)$ denote the reduction of this polynomial modulo 3. Namely, $\overline{g}(x) \in (\mathbb{Z}/3)[x]$.

4.1 Compute $N_K(\sqrt{7})$ and $\mathrm{Tr}_K(\sqrt{7})$.

4.2 Show that $g(\alpha)$ is divisible by 3 in $\mathbb{Z}[\alpha]$ if and only if $\overline{f}(x) \mid \overline{g}(x)$ in $(\mathbb{Z}/3)[x]$. You may use here that the ring $\mathbb{Z}[\alpha]$ is isomorphic to the ring $\mathbb{Z}[x]/(f(x))_{\mathbb{Z}[x]}$ via the evaluation at α map.

4.3 Let

$$\alpha_1 = (1 + \sqrt{7})(1 + \sqrt{10})$$
$$\alpha_2 = (1 + \sqrt{7})(1 - \sqrt{10})$$
$$\alpha_3 = (1 - \sqrt{7})(1 + \sqrt{10})$$
$$\alpha_4 = (1 - \sqrt{7})(1 - \sqrt{10}),$$

be in $\mathcal{O}_K$. Prove that $3 \mid \alpha_i\alpha_j$ for any $i \neq j$, but 3 does not divide any power of α_i^n for any $i = 1, 2, 3, 4$ and any $n \geq 1$.
(Hint: $\alpha_1, ..., \alpha_4$ are related to each other in a special way. Can you spot this relation and use it to compute traces?)

4.4 Let $\alpha_1, ..., \alpha_4$ be as defined above in Question 4.3. Suppose $\alpha_i \in \mathbb{Z}[\alpha]$ for each $i = 1, ..., 4$, then we must have $\alpha_i = f_i(\alpha)$ for some polynomials $f_i(x) \in \mathbb{Z}[x]$. Show that $\overline{f}(x) \mid \overline{f_i}(x)\overline{f_j}(x)$ for $i \neq j$ but $\overline{f}(x)$ does not divide $\overline{f_i}(x)^n$ in $(\mathbb{Z}/3)[x]$, for any $i = 1, 2, 3, 4$ and any $n \geq 1$.

4.5 Conclude that $\overline{f}(x)$ has at least four distinct monic irreducible factors in $(\mathbb{Z}/3)[x]$ and use it to prove that $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$ for any $\alpha \in \mathcal{O}_K$. Give careful reasoning.
(Hint: Recall that $(\mathbb{Z}/3)[x]$ is a UFD.)

Q5 **5.1** Compute the group structure of the class group of $K = \mathbb{Q}(\sqrt{-33})$. Give careful reasoning.

5.2 Let $K = \mathbb{Q}(\alpha)$ and $R = \mathcal{O}_K = \mathbb{Z}[\alpha]$, where $\alpha^3 = \alpha + 1$. Factorise the ideal $(345)_R$, as a product of prime ideals in R.

5.3 Let p be a prime such that $p \equiv 3 \bmod 4$. Assume further that the class group of the field $K = \mathbb{Q}(\sqrt{p})$ is of odd order. Use this information to prove that there are infinitely many integers $a, b \in \mathbb{Z}$ satisfying

$$a^2 - pb^2 = (-1)^{(p+1)/4}2.$$