Imperial College
London

MATH97037 MATH97145

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)
May-June 2021

This paper is also taken for the relevant examination for the
Associateship of the Royal College of Science

Algebraic Number Theory

Date: Wednesday, 12 May 2021

Time: 09:00 to 11:30

Time Allowed: 2.5 hours

Upload Time Allowed: 30 minutes

This paper has 5 Questions.

Candidates should start their solutions to each question on a new sheet of paper.

Each sheet of paper should have your CID, Question Number and Page Number on the top.

Only use 1 side of the paper.

Allow margins for marking.

Any required additional material(s) will be provided.

Credit will be given for all questions attempted.

Each question carries equal weight.

SUBMIT YOUR ANSWERS ONE PDF TO THE RELEVANT DROPBOX ON BLACKBOARD INCLUDING A COMPLETED COVERSHEET WITH YOUR CID NUMBER, QUESTION NUMBERS ANSWERED AND PAGE NUMBERS PER QUESTION.

1. Let $A = \mathbb{Z}\left[\frac{1+i\sqrt{31}}{2}\right]$.

(a) Show that $A^\times = \{\pm 1\}$. (4 marks)

(b) Is A a UFD? (6 marks)

(c) For each prime number p in the following list, determine whether or not the ideal $(p) \subset A$ is prime: (4 marks)

$$3, 7, 11, 73.$$

(d) (i) Show that the class group of A is isomorphic to $\mathbb{Z}/3\mathbb{Z}$. (3 marks)

(ii) Let $\alpha, \beta \in A \smallsetminus \{0\}$. Assume that $(\alpha, \beta) = A$ and that there exists $\gamma \in A$ such that $\alpha\beta = \gamma^3$. Is it true that α and β must be cubes in A? (3 marks)

(You may use any result from the course without proof as long as you state it clearly and correctly.)

(Total: 20 marks)

2. Let $K = \mathbb{Q}(\sqrt{15})$. Recall that, for $\alpha = a+b\sqrt{15} \in K$, we defined $\alpha' = a-b\sqrt{15}$ and $N(\alpha) = \alpha\alpha'$. Let $\mathcal{O}_K$ be the ring of integers of K.

(a) (i) Show that $(1, \sqrt{15})$ is a basis of the free abelian group $(\mathcal{O}_K, +)$. (3 marks)

(ii) Compute the discriminant of $\mathcal{O}_K$. (4 marks)

(iii) Which prime numbers are ramified in K? (3 marks)

(b) Find a unit $u \in \mathcal{O}_K^\times$ different from ± 1, and show that $\mathcal{O}_K^\times$ is infinite. (3 marks)

(c) Show that 3 is irreducible in $\mathcal{O}_K$. (4 marks)

(d) Is $\mathcal{O}_K$ a PID? (3 marks)

(You may use any result from the course without proof as long as you state it clearly and correctly.)

(Total: 20 marks)

3. (a) Give an example of an integral domain which is not integrally closed. (6 marks)

(b) Let K be a number field with ring of integers $\mathcal{O}_K$.

(i) Let $I \subset \mathcal{O}_K$ be an ideal. Prove that there is an integer $k \geq 1$ such that I^k is principal. (3 marks)

(ii) Let $\mathfrak{p} \subset \mathcal{O}_K$ be a non-zero prime ideal. Show that the norm of $\mathfrak{p}$ equals p^d for some prime number p and some integer $d \geq 1$. (4 marks)

(iii) Give an example of a number field K and a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ with norm 9. (3 marks)

(c) Show that the equation $X^2 - 7Y^2 = 2$ has infinitely many integral solutions. Then prove that the equation $X^3 - 7Y^3 = 2$ has finitely many integral solutions. (4 marks)

(You may use any result from the course without proof as long as you state it clearly and correctly.)

(Total: 20 marks)

4. The aim of this exercise is to find the integral solutions of the equation $Y^2 - 2 = X^3$. You can freely use without proof the fact that the class number of $\mathbb{Z}[i\sqrt{6}]$ is 2. Take $(x, y) \in \mathbb{Z}^2$ such that $y^2 - 2 = x^3$.

(a) (i) Show that x, y are odd. (3 marks)

(ii) Prove that 3 does not divide y. (3 marks)

(b) Set $x = z - 1$. Show that

$$y^2 + 6z^2 = (z + 1)^3$$

and that y, z are coprime. (4 marks)

(c) Prove that $(y + i\sqrt{6}z, y - i\sqrt{6}z) = \mathbb{Z}[i\sqrt{6}]$. (2 marks)

(d) (i) Show that there exist $a, b \in \mathbb{Z}$ such that $y + i\sqrt{6}z = (a + i\sqrt{6}b)^3$. (2 marks)

(ii) Deduce that $z + 1 = a^2 + 6b^2$ and (3 marks)

$$a^2(3b - 1) = 6b^3 + 6b^2 - 1.$$

(iii) Prove that $-1 \equiv 0 \pmod{(3b - 1)}$. Deduce that $b = 0$, hence $x = -1$ and $y = \pm 1$. (3 marks)

(You may use any result from the course without proof as long as you state it clearly and correctly.)

(Total: 20 marks)

5. Let $k > 0$ be a squarefree integer congruent to 2 or 3 modulo 4. Let $K = \mathbb{Q}(\sqrt{k})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{k}]$ and let $\Delta(\mathcal{O}_K)$ be the discriminant of $\mathcal{O}_K$. Recall that for $\alpha = a + b\sqrt{k} \in K$ we defined $\alpha' = a - b\sqrt{k}$. Let

$$\begin{aligned} \iota : \mathcal{O}_K &\hookrightarrow \mathbb{R}^2 \\ \alpha &\mapsto (\alpha, \alpha'). \end{aligned}$$

The aim of this exercise is to use geometry of numbers to show that $\mathcal{O}_K^\times$ is infinite.

(a) (i) Prove that for every integer $M \geq 0$ the ring $\mathcal{O}_K$ contains finitely many ideals of norm at most M. (2 marks)

(ii) Deduce that, if there exists a real number $C > 0$ such that $\mathcal{O}_K$ contains infinitely many elements α satisfying $|N(\alpha)| \leq C$, then $\mathcal{O}_K^\times$ is infinite. (3 marks)

(b) Show that $\iota(\mathcal{O}_K)$ is a lattice in $\mathbb{R}^2$ and compute its covolume. (4 marks)

(c) If $a < b$ are real numbers, we set $(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$.

(i) Let $C > 0$ and $\delta > 0$ be real numbers. Prove that the set

$$R_{\delta,C} = (-\delta, \delta) \times \left(-\frac{C}{\delta}, \frac{C}{\delta}\right) \subset \mathbb{R}^2$$

is a convex body with a centre at the origin. Show that, if $C > \sqrt{\Delta(\mathcal{O}_K)}$, then $\mathrm{vol}(R_{\delta,C}) > 4\mathrm{covol}(\iota(\mathcal{O}_K))$. (3 marks)

(ii) Fix $C > \sqrt{\Delta(\mathcal{O}_K)}$. Show that for every $\delta > 0$ there is a non-zero element $\alpha \in \mathcal{O}_K$ such that $\iota(\alpha) \in \iota(\mathcal{O}_K) \cap R_{\delta,C}$. Prove that $|N(\alpha)| \leq C$. (4 marks)

(iii) Deduce that, for C as in the previous point, there are infinitely many elements $\alpha \in \mathcal{O}_K$ such that $|N(\alpha)| \leq C$. (4 marks)

(You may use any result from the course and mastery material without proof as long as you state it clearly and correctly.)

(Total: 20 marks)

1. Let $A = \mathbb{Z}\left[\frac{1+i\sqrt{31}}{2}\right]$.

   (a) Show that $A^\times = \{\pm 1\}$. (4 marks)

   (b) Is A a UFD? (6 marks)

   (c) For each prime number p in the following list, determine whether or not the ideal $(p) \subset A$ is prime: (4 marks)

$$3, 7, 11, 73.$$

   (d) (i) Show that the class group of A is isomorphic to $\mathbb{Z}/3\mathbb{Z}$. (3 marks)

   (ii) Let $\alpha, \beta \in A \smallsetminus \{0\}$. Assume that $(\alpha, \beta) = A$ and that there exists $\gamma \in A$ such that $\alpha\beta = \gamma^3$. Is it true that α and β must be cubes in A? (3 marks)

(Total: 20 marks)

(a) (**A, 4 marks, routine**) an element $\alpha = a + b\frac{1+i\sqrt{31}}{2} \in A$ is a unit if and only if it has norm one. We have $N(\alpha) = (a + \frac{b}{2})^2 + \frac{31}{4}b^2$. As $\frac{31}{4} > 1$ the equality $N(\alpha) = 1$ forces $b = 0$ and $a = \pm 1$, hence $A^\times = \{\pm 1\}$.

(b) (**A, 6 marks, seen many similar**) The ring A is not a UFD. To show this, observe that we have $2^3 = \frac{1+i\sqrt{31}}{2}\frac{1-i\sqrt{31}}{2}$. The number 2 is irreducible in A: indeed assuming the contrary we can write $2 = \alpha\beta$ with $\alpha, \beta \in A \smallsetminus A^\times$. We deduce that $4 = N(\alpha)N(\beta)$ hence $N(\alpha) = N(\beta) = 2$. Writing $\alpha = a + b\frac{1+i\sqrt{31}}{2}$ we find that $(a + \frac{b}{2})^2 + \frac{31}{4}b^2 = 2$; however this equation has no integral solution.

Now $2 \in A$ is irreducible, and it divides the product $\frac{1+i\sqrt{31}}{2}\frac{1-i\sqrt{31}}{2}$. However 2 does not divide any of the factors, hence 2 is not a prime element in A. Since we know that in a UFD every irreducible element is prime, we deduce that A is not a UFD.

(c) (**B, 4 marks, seen similar**) The ring A is the quadratic ring of discriminant -31. We have proved in the lectures that, for an odd prime p different from 31, the ideal $(p) \subset A$ is prime if and only if $\left(\frac{-31}{p}\right) = -1$. As $-31 \equiv 2 \pmod 3$ we deduce that $(3) \subset A$ is a prime ideal. On the other hand $-31 \equiv 4 \pmod 7$ hence $(7) \subset A$ is not a prime ideal. As $-31 \equiv 2 \pmod{11}$ and 2 is not a quadratic residue modulo 11 we deduce that $(11) \subset A$ is a prime ideal. Finally, we have shown in the lectures that the factorisation of an ideal (p) as above only depends on p modulo 31. Since $73 \equiv 11 \pmod{31}$ the ideal $(73) \subset A$ is also prime.

(d) (i) (**C, 3 marks, not seen**) It suffices to show that $Cl(A)$ has three elements. We know that $Cl(A)$ is in bijection with the set of positive definite reduced binary integral quadratic forms $[a, b, c]$ of discriminant -31. Those satisfy $|b| \leq a \leq c$, $b \geq 0$ if any of the two inequalities is an equality and $a \leq \sqrt{\frac{31}{3}}$. Hence we must have $1 \leq a \leq 3$ and b odd. For $a = 1$ we find $b = 1$ and $c = 8$. For $a = 2$ we find $b = \pm 1$ and $c = 4$. A reduced form $[a, b, c]$ with $a = 3$ would give rise, as seen in the lectures, to an ideal of norm 3. But we have seen above that $(3) \subset A$ is a prime ideal, hence no ideal of norm 3 exists in A. So $Cl(A)$ has cardinality 3.

(ii) (**D, 3 marks, unseen**) The assertion is not true. Take $\alpha = \frac{1+i\sqrt{31}}{2}, \beta = \frac{1-i\sqrt{31}}{2}$. Then (α, β) contains $\alpha + \beta = 1$, hence $(\alpha, \beta) = A$. We also have $\alpha\beta = \gamma^3$ for $\gamma = 2 \in A$. On the other hand, we claim that α is not a cube in A. Indeed the norm of α is 8, and we have shown in point (b) that A contains no element of norm 2.

2. Let $K = \mathbb{Q}(\sqrt{15})$. Recall that, for $\alpha = a+b\sqrt{15} \in K$, we defined $\alpha' = a-b\sqrt{15}$ and $N(\alpha) = \alpha\alpha'$. Let $\mathcal{O}_K$ be the ring of integers of K.

(a) (i) Show that $(1, \sqrt{15})$ is a basis of the free abelian group $(\mathcal{O}_K, +)$. (3 marks)

(ii) Compute the discriminant of $\mathcal{O}_K$. (4 marks)

(iii) Which prime numbers are ramified in K? (3 marks)

(b) Find a unit $u \in \mathcal{O}_K^\times$ different from ± 1, and show that $\mathcal{O}_K^\times$ is infinite. (3 marks)

(c) Show that 3 is irreducible in $\mathcal{O}_K$. (4 marks)

(d) Is $\mathcal{O}_K$ a PID? (3 marks)

(Total: 20 marks)

(a) (i) (**A, 3 marks, routine**) The number 15 is squarefree and congruent to 3 modulo 4, hence the ring of integers of $\mathbb{Q}(\sqrt{15})$ is $\mathbb{Z}[\sqrt{15}] = \{a + b\sqrt{15}, a, b \in \mathbb{Z}\}$. Therefore $(1, \sqrt{15})$ is a basis of $(\mathbb{Z}[\sqrt{15}], +)$.

(ii) (**A, 4 marks, basic example**) The discriminant of $\mathcal{O}_K$ can be computed as the determinant of the trace form with respect to the basis $(1, \sqrt{15})$ found above. Hence it is the determinant of the matrix $\begin{pmatrix} 2 & 0 \\ 0 & 30 \end{pmatrix}$, which equals 60.

(iii) (**B, 3 marks, seen similar**) We have seen that a prime p ramifies in K if and only if it divides the discriminant of $\mathcal{O}_K$, which is 60 by the previous point. Hence $2, 3, 5$ are the only primes which ramify in K.

(b) (**B, 3 marks, seen similar**) The element $u = 4 + \sqrt{15}$ is a unit with inverse $4 - \sqrt{15}$. For every integer $n > 1$ we have $u^n > u^{n-1}$, hence u generates an infinite subgroup of $\mathcal{O}_K^\times$.

(c) (**D, 4 marks, unseen**) Assume by contradiction that we can write $3 = \alpha\beta$ with $\alpha, \beta \in \mathcal{O}_K \setminus \mathcal{O}_K^\times$. Then the norm of α is ± 3. Writing $\alpha = a+b\sqrt{15}$ with $a, b \in \mathbb{Z}$ we find $a^2 - 15b^2 = \pm 3$. Reducing modulo 5 we obtain a contradiction, as ± 3 are not quadratic residues modulo 5.

(d) (**C, 3 marks, not seen**) We will show that $\mathcal{O}_K$ is not a UFD; this implies that it is not a PID, since every PID is a UFD. We have $3 \cdot 5 = 15 = \sqrt{15} \cdot \sqrt{15}$. We have shown that 3 is irreducible; however it does not divide $\sqrt{15}$, hence it is not prime in $\mathbb{Z}[\sqrt{15}]$. It follows that $\mathbb{Z}[\sqrt{15}]$ is not a UFD.

3. (a) Give an example of an integral domain which is not integrally closed. (6 marks)

(b) Let K be a number field with ring of integers $\mathcal{O}_K$.

(i) Let $I \subset \mathcal{O}_K$ be an ideal. Prove that there is an integer $k \geq 1$ such that I^k is principal. (3 marks)

(ii) Let $\mathfrak{p} \subset \mathcal{O}_K$ be a non-zero prime ideal. Show that the norm of $\mathfrak{p}$ equals p^d for some prime number p and some integer $d \geq 1$. (4 marks)

(iii) Give an example of a number field K and a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ with norm 9. (3 marks)

(c) Show that the equation $X^2 - 7Y^2 = 2$ has infinitely many integral solutions. Then prove that the equation $X^3 - 7Y^3 = 2$ has finitely many integral solutions. (4 marks)

(Total: 20 marks)

(a) (**A, 6 marks, seen**) The integral domain $A = \mathbb{Z}[i\sqrt{3}]$ is not integrally closed: the element $\zeta_3 = \frac{-1+i\sqrt{3}}{2}$ belongs to the fraction field of A and it is integral over A. However $\zeta_3 \notin A$.

(b) (i) (**C, 3 marks, not seen**) If $I = (0)$ then I is principal. If $I \neq (0)$ we consider its image in $Cl(\mathcal{O}_K) = I(\mathcal{O}_K)/P(\mathcal{O}_K)$. We know that $Cl(\mathcal{O}_K)$ is a finite group, hence, letting h be its cardinality, the ideal I^h must map to the identity element in $Cl(\mathcal{O}_K)$. Therefore I^h is principal.

(ii) (**B, 4 marks, seen similar**) The quotient $\mathcal{O}_K/\mathfrak{p}$ is a finite integral domain, hence a finite field. So its cardinality, which is the norm of $\mathfrak{p}$, is a power of a prime.

(iii) (**B, 3 marks, basic example**) Take $K = \mathbb{Q}(i\sqrt{31})$; then $\mathcal{O}_K$ is the ring A considered in Exercise 1. We have shown that $(3) \subset A$ is prime, and its norm is $3^2 = 9$.

(c) (**D, 4 marks, not seen**) One integral solution of the equation $X^2 - 7Y^2 = 2$ is $(3, 1)$. Furthermore, for every $u \in \mathbb{Z}[\sqrt{7}]^\times$ with norm one, writing $\alpha = (3 + \sqrt{7})u = a + b\sqrt{7}$ with $a, b \in \mathbb{Z}$ we have $N(\alpha) = a^2 - 7b^2 = 2$. There are infinitely many units with norm one in the real quadratic ring $\mathbb{Z}[\sqrt{7}]$, hence there are infinitely many integral solutions of the equation $X^2 - 7Y^2 = 2$.

The fact that the equation $X^3 - 7Y^3 = 2$ has finitely many integral solutions is a special case of Thue's theorem. One could also more simply observe that there is no integral solution of this equation, because 2 is not a cube modulo 7.

4. The aim of this exercise is to find the integral solutions of the equation $Y^2 - 2 = X^3$. You can freely use without proof the fact that the class number of $\mathbb{Z}[i\sqrt{6}]$ is 2. Take $(x, y) \in \mathbb{Z}^2$ such that $y^2 - 2 = x^3$.

(a) (i) Show that x, y are odd. (3 marks)

(ii) Prove that 3 does not divide y. (3 marks)

(b) Set $x = z - 1$. Show that

$$y^2 + 6z^2 = (z + 1)^3$$

and that y, z are coprime. (4 marks)

(c) Prove that $(y + i\sqrt{6}z, y - i\sqrt{6}z) = \mathbb{Z}[i\sqrt{6}]$. (2 marks)

(d) (i) Show that there exist $a, b \in \mathbb{Z}$ such that $y + i\sqrt{6}z = (a + i\sqrt{6}b)^3$. (2 marks)

(ii) Deduce that $z + 1 = a^2 + 6b^2$ and (3 marks)

$$a^2(3b - 1) = 6b^3 + 6b^2 - 1.$$

(iii) Prove that $-1 \equiv 0 \pmod{(3b-1)}$. Deduce that $b = 0$, hence $x = -1$ and $y = \pm 1$. (3 marks)

(Total: 20 marks)

(a) (i) (**A, 3 marks, seen many similar**) If x is even and $y^2 - 2 = x^3$ then $y^2 \equiv 2 \pmod 8$, which is not possible. Hence x is odd and $y^2 = x^3 + 2$ is odd; therefore y is odd.

(ii) (**B, 3 marks, similar to above**) If $3 \mid y$ then $x^3 \equiv 7 \pmod 9$. However the only cubes modulo 9 are $0, \pm 1$.

(b) (**A, 4 marks, straightforward**) We have

$$y^2 - 2 = z^3 - 3z^2 + 3z - 1 \Rightarrow y^2 + 6z^2 = z^3 + 3z^2 + 3z + 1 = (z + 1)^3.$$

A prime p dividing y, z also divides $(z + 1)^3$ hence $z + 1$. Therefore y, z have no common prime factor.

(c) (**D, 2 marks, unseen**) Let $I = (y + i\sqrt{6}z, y - i\sqrt{6}z)$; we need to show that $1 \in I$. The ideal I contains $2y, 24z^2$ and $(y + i\sqrt{6}z)(y - i\sqrt{6}z) = y^2 + 6z^2$. Hence it suffices to show that the greatest common divisor d (in $\mathbb{Z}$) of $2y, 24z^2, y^2 + 6z^2$ is one. As $y^2 + 6z^2$ is odd so is d; hence $d \mid \gcd(y, 3z^2)$. As y, z are coprime and $3 \nmid y$ we deduce that $d = 1$.

(d) (i) (**A, 2 marks, seen many similar**) The product $(y + i\sqrt{6}z)(y - i\sqrt{6}z)$ is a cube, and the ideals $(y + i\sqrt{6}z), (y - i\sqrt{6}z)$ have no common factor by the previous point. It follows that $(y + i\sqrt{6}z) = \mathfrak{a}^3$ for some ideal $\mathfrak{a} \subset \mathbb{Z}[i\sqrt{6}]$. As the class number of $\mathbb{Z}[i\sqrt{6}]$ is 2 and the cube of $\mathfrak{a}$ is principal, the ideal $\mathfrak{a}$ must be principal. Therefore we have $y + i\sqrt{6}z = \pm\alpha^3 = (\pm\alpha)^3$ for some $\alpha \in \mathbb{Z}[i\sqrt{6}]$. Writing $\pm\alpha = a + i\sqrt{6}b$ with $a, b \in \mathbb{Z}$ we get $y + i\sqrt{6}z = (a + i\sqrt{6}b)^3$.

(ii) (**D, 3 marks, not seen**) Taking the norm on both sides of the equality in the previous point we find $(z + 1)^3 = y^2 + 6z^2 = (a^2 + 6b^2)^3$, hence $z + 1 = a^2 + 6b^2$. On the other hand we have

$$y + i\sqrt{6}z = a^3 - 18ab^2 + i\sqrt{6}(3a^2b - 6b^3) \Rightarrow z = 3a^2b - 6b^3.$$

Hence we obtain

$$a^2 + 6b^2 - 1 = 3a^2b - 6b^3 \Rightarrow a^2(3b - 1) = 6b^3 + 6b^2 - 1.$$

(iii) (**C, 3 marks, not seen**) The equality in the previous point implies that

$$54b^3 + 54b^2 - 9 \equiv 0 \pmod{(3b-1)};$$

Now $54b^3 \equiv 2 \pmod{(3b-1)}$ and $54b^2 \equiv 6 \pmod{(3b-1)}$. Hence we find $2 + 6 - 9 \equiv 0 \pmod{(3b-1)}$.

This implies that $3b - 1$ equals either 1 or -1. As b is an integer we find $b = 0$, hence $a^2 = 1$ and $z = 0$. Therefore we find $x = -1$ and $y = \pm 1$.

5. Let $k > 0$ be a squarefree integer congruent to 2 or 3 modulo 4. Let $K = \mathbb{Q}(\sqrt{k})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{k}]$ and let $\Delta(\mathcal{O}_K)$ be the discriminant of $\mathcal{O}_K$. Recall that for $\alpha = a + b\sqrt{k} \in K$ we defined $\alpha' = a - b\sqrt{k}$. Let

$$\begin{aligned} \iota : \mathcal{O}_K &\hookrightarrow \mathbb{R}^2 \\ \alpha &\mapsto (\alpha, \alpha'). \end{aligned}$$

The aim of this exercise is to use geometry of numbers to show that $\mathcal{O}_K^\times$ is infinite.

(a) (i) Prove that for every integer $M \geq 0$ the ring $\mathcal{O}_K$ contains finitely many ideals of norm at most M. (2 marks)

(ii) Deduce that, if there exists a real number $C > 0$ such that $\mathcal{O}_K$ contains infinitely many elements α satisfying $|N(\alpha)| \leq C$, then $\mathcal{O}_K^\times$ is infinite. (3 marks)

(b) Show that $\iota(\mathcal{O}_K)$ is a lattice in $\mathbb{R}^2$ and compute its covolume. (4 marks)

(c) If $a < b$ are real numbers, we set $(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$.

(i) Let $C > 0$ and $\delta > 0$ be real numbers. Prove that the set

$$R_{\delta,C} = (-\delta, \delta) \times \left(-\frac{C}{\delta}, \frac{C}{\delta}\right) \subset \mathbb{R}^2$$

is a convex body with a centre at the origin. Show that, if $C > \sqrt{\Delta(\mathcal{O}_K)}$, then $\mathrm{vol}(R_{\delta,C}) > 4\mathrm{covol}(\iota(\mathcal{O}_K))$. (3 marks)

(ii) Fix $C > \sqrt{\Delta(\mathcal{O}_K)}$. Show that for every $\delta > 0$ there is a non-zero element $\alpha \in \mathcal{O}_K$ such that $\iota(\alpha) \in \iota(\mathcal{O}_K) \cap R_{\delta,C}$. Prove that $|N(\alpha)| \leq C$. (4 marks)

(iii) Deduce that, for C as in the previous point, there are infinitely many elements $\alpha \in \mathcal{O}_K$ such that $|N(\alpha)| \leq C$. (4 marks)

(Total: 20 marks)

(a) (i) (**2 marks, seen similar**) It suffices to show that for every integer $n \geq 1$ there are finitely many ideals of norm n in $\mathcal{O}_K$. Every non-zero ideal contains its norm, so ideals of norm n form a subset of the set of ideals of the quotient $\mathcal{O}_K/(n)$, which is finite. Hence the result follows.

(ii) (**3 marks, seen similar**) Take $C > 0$ such that $\mathcal{O}_K$ contains infinitely many elements of norm at most C in absolute value. By the previous point infinitely many of these elements must generate the same ideal, hence they differ by multiplication by a unit. It follows that $\mathcal{O}_K^\times$ is infinite.

(b) (**4 marks, seen similar**) We have $\iota(\mathcal{O}_K) = \{(a+b\sqrt{k}, a-b\sqrt{k}), a, b \in \mathbb{Z}\} \subset \mathbb{R}^2$. The linear map f sending $(x, y) \in \mathbb{R}^2$ to $\left(\frac{x+y}{2}, \frac{x-y}{2\sqrt{k}}\right)$ sends $\iota(\mathcal{O}_K)$ to $\mathbb{Z}^2$. The absolute value of the determinant of f is $\frac{1}{2\sqrt{k}}$; hence $\iota(\mathcal{O}_K)$ is a lattice with covolume $2\sqrt{k} = \sqrt{\Delta(\mathcal{O}_K)}$.

(c) (i) (**3 marks, seen similar**) The set $R_{\delta,C}$ is an open rectangle symmetric with respect to the origin, hence it is a convex body with a centre at the origin. Its area is $\mathrm{vol}(R_{\delta,C}) = (2\delta)(2C/\delta) = 4C$. Hence if $C > \sqrt{\Delta(\mathcal{O}_K)}$ then $\mathrm{vol}(R_{\delta,C}) > 4\mathrm{covol}(\iota(\mathcal{O}_K))$.

(ii) (**4 marks, not seen**) The existence of α with the stated properties follows from Minkowski's first theorem, which can be applied in view of the previous point. We have $|N(\alpha)| = |\alpha\alpha'|$; as $\iota(\alpha) = (\alpha, \alpha')$ and $\iota(\alpha) \in R_{\delta,C}$ we have $|\alpha| < \delta$ and $|\alpha'| < \frac{C}{\delta}$, hence $|N(\alpha)| \leq C$.

(iii) (**4 marks, not seen**) Take $\delta = 1$ and pick $\alpha_1 \in \mathcal{O}_K$ with the properties stated in the previous point. Now take $\delta = |\alpha_1|$ (notice that $|\alpha_1| > 0$) and pick an element $\alpha_2 \in \mathcal{O}_K$ as in the previous point; observe that α_2 is different from α_1. Repeating the argument we obtain a sequence of distinct non-zero elements $(\alpha_k)_{k\geq 1}$ with $|N(\alpha_k)| \leq C$.

If your module is taught across multiple year levels, you might have received this form for each level of the module. You are only required to fill this out once for each question.

Please record below, some brief but non-trivial comments for students about how well (or otherwise) the questions were answered. For example, you may wish to comment on common errors and misconceptions, or areas where students have done well. These comments should note any errors in and corrections to the paper. These comments will be made available to students via the MathsCentral Blackboard site and should not contain any information which identifies individual candidates. Any comments which should be kept confidential should be included as confidential comments for the Exam Board and Externals. If you would like to add formulas, please include a sperate pdf file with your email.

ExamModuleCode	QuestionNumber	Comments for Students
MATH96028 MATH97037 MATH97145	1	Quadratic reciprocity was used correctly in (c) by almost everyone. The last point asked if the ring A satisfies a property called SP(3) in the lectures. We have proved in the course that if 3 does not divide the class number of A, then SP(3) holds, but we did not prove the converse in general. To show that A does not satisfy SP(3), a counterexample has to be provided.
MATH96028 MATH97037 MATH97145	2	Points (a) and (b) were almost always well done. In (c), if one wants to verify directly that 3 is irreducible, one should remember that non-trivial factors of 3 could have a priori norm equal either to 3 or to -3
MATH96028 MATH97037 MATH97145	3	Well done except for (b)(ii), where incorrect arguments were sometimes used. A possible way to argue is explained in the solution sheet.
MATH96028 MATH97037 MATH97145	4	In point (d)(i), one needs to use property SP(3). As emphasised during the course, one should explain why units can be absorbed in the cube. This was often forgotten, but it is crucial: we have seen in the lectures that if one attempts to solve the equation Y^2-2=X^3 working with the natural real quadratic ring one runs into troubles precisely because of units.
MATH96028 MATH97037 MATH97145	5	The main point was to apply Minkowski's theorem in (c)(ii); this was mostly done correctly. The last point was often not attempted; it required the idea to apply (c)(ii) repeatedly, for smaller and smaller delta.