IMPERIAL

MATH70042

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)
Summer 2025

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

Algebraic Number Theory

Date: Tuesday, May 27, 2025

Time: Start time 14:00 – End time 16:30 (BST)

Time Allowed: 2.5 hours

This paper has 5 Questions.

Please Answer All Questions in 1 Answer Booklet

This is a closed book examination.

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

Supplementary books may only be used after the relevant main book(s) are full.

Any required additional material(s) will be provided.

Credit will be given for all questions attempted.

Allow margins for marking.

DO NOT OPEN THIS PAPER UNTIL THE INVIGILATOR TELLS YOU TO DO SO

1. (a) Let K be a number field. Give the definition of the ring of integers $\mathcal{O}_K$. (4 marks)

   (b) Let $d < 0$ be a square-free integer. Give the Minkowski constant M_d for $\mathbb{Q}(\sqrt{d})$. (4 marks)

   (c) Let $d = -14$, list all the prime ideals of $\mathcal{O}_{-14}$ of norm at most $M_{-14} < 5$. (6 marks)

   (d) Let
   $$I = (7, \sqrt{-14}) \text{ and } J = (36, 2 + \sqrt{-14})$$
   be ideals of $\mathcal{O}_{-14}$. Determine whether these ideals are principal ideals or prime ideals. Justify your answer. (6 marks)

   (Total: 20 marks)

2. (a) Let K be a number field. State what it means for a prime number $p \in \mathbb{Z}$ to ramify in $\mathcal{O}_K$. (4 marks)

   (b) Let $K = \mathbb{Q}(\sqrt{35})$, which prime numbers $p \in \mathbb{Z}$ ramify in $\mathcal{O}_K$? (4 marks)

   (c) Show that the class group is generated by ideals above 2, 3 and 5 and give the structure of the class group. (6 marks)

   (d) Let p be a prime number such that $p \equiv 1 \mod 28$. Show that p splits in $\mathcal{O}_{35}$ if and only if p is a square modulo 5. (6 marks)

   (Total: 20 marks)

3. (a) Give the definition of an integrally closed domain. (4 marks)

Let K be a number field with ring of integers $\mathcal{O}_K$. Let $R \subseteq \mathcal{O}_K$ be a subring of $\mathcal{O}_K$.

(b) Assume that $\mathrm{Frac}(R) = K$. Show that if $R \subsetneq \mathcal{O}_K$, then R is not an integrally closed domain. (6 marks)

(c) Give an example of K, R and $\mathcal{O}_K$ satisfying the assumptions in part (b). (4 marks)

(d) Let R be a subring of $\mathcal{O}_K$. Prove that every non-zero prime ideal $\mathfrak{p} \subseteq R$ is maximal. [You can use without proving it that R is a free abelian group of finite rank.] (6 marks)

(Total: 20 marks)

4. This question is on the Mordell's equation

$$y^2 = x^3 - 37. \tag{1}$$

In this question, you may use without proof that $\mathrm{Cl}(\mathcal{O}_{-37}) \simeq \mathbb{Z}/2\mathbb{Z}$.

(a) Show that if a prime ideal $\mathfrak{p}$ divides both the ideals $(y + \sqrt{-37})$ and $(y - \sqrt{-37})$ then $\mathfrak{p}$ lies above 2 or above 37. (4 marks)

(b) Deduce from part (a) that $(y + \sqrt{-37})$ and $(y - \sqrt{-37})$ are coprime. (6 marks)

(c) Use part (b) to deduce that there exists $\mathfrak{a} \subseteq \mathcal{O}_{-37}$ such that

$$(y + \sqrt{-37}) = \mathfrak{a}^3.$$

(4 marks)

(d) Using the fact that $\mathrm{Cl}(\mathcal{O}_{-37})$ is cyclic of order 2, show that $\mathfrak{a}$ has to be principal. Deduce that there are no integer solutions to equation (1). (6 marks)

(Total: 20 marks)

5. (a) Calculate the fundamental unit in $K = \mathbb{Q}(\sqrt{82})$. (4 marks)

(b) Show that the class group of $\mathcal{O}_{82}$ is generated by the primes above 2 and 3. (4 marks)

(c) In this question you may use without proof that $2\mathcal{O}_{82} = \mathfrak{p}_2^2$ and $\mathfrak{p}_3\bar{\mathfrak{p}}_3$, with $\mathfrak{p}_2 = (2, \sqrt{82})$ and $\mathfrak{p}_3 = (3, 1 + \sqrt{82})$. Show that $\mathfrak{p}_2\mathfrak{p}_3^2$ is principal.
[Hint: what is the norm of $10 + \sqrt{82}$?] (6 marks)

(d) Show that $\mathfrak{p}_2$ is not principal and deduce that the class group of $\mathcal{O}_{82}$ is cyclic of order 4. (6 marks)

(Total: 20 marks)

BSc and MSci EXAMINATIONS (MATHEMATICS)

May 2025

This paper is also taken for the relevant examination for the Associateship.

M60042

Algebraic Number Theory (Solutions)

Setter's signature	Checker's signature	Editor's signature
.....	.....	.....

1. (a) $\mathcal{O}_K = \{\alpha \in K \mid m_\alpha(T) \in \mathbb{Z}[T]\}$ where m_α is the minimal polynomial of α. seen ⇓

   (b) $M_d = \frac{2}{\pi}\sqrt{\mid D_K \mid}$. 4, A

   (c) $M_{-14} = \frac{2}{\pi} \cdot \sqrt{4 \cdot 14} \simeq 4,764$. We are interested in prime ideals $\mathfrak{p}$ with norm ≤ 4. We want to understand prime ideals above $2, 3$. seen ⇓

   - For $p = 2$, we have $2\mathcal{O}_K = \mathfrak{p}_2^2$, with $\mathfrak{p}_2 = (2, \sqrt{-14})$ and $N_K(2, \sqrt{-14}) = 2$. 4, A
   - For $p = 3$, we have $3\mathcal{O}_K = \mathfrak{p}_3 \cdot \bar{\mathfrak{p}}_3$ with $\mathfrak{p}_3 = (3, 1 + \sqrt{-14})$, with $N_K(\mathfrak{p}_3) = N_K(\bar{\mathfrak{p}}_3) = 3$. sim. seen ⇓

   Hence the prime ideals of norm $\leq M_{-14}$ are $\mathfrak{p}_2$, $\mathfrak{p}_3$ and $\bar{\mathfrak{p}}_3$. 6, A

   (d) Assume $(7, \sqrt{-14}) = (\alpha)$, then $N(\alpha) \mid \gcd(N(7), N(\sqrt{-14})) = 7$, but it is easy to see that there are no elements of norm 7, hence α has to be a unit. However, $(7, \sqrt{-14})$ is prime (the quotient is $\mathbb{Z}/7\mathbb{Z}$). Note that $36 = 2(2 - \sqrt{-14})(2 + \sqrt{-14})$, hence $(36, 2 + \sqrt{-14}) = (2 + \sqrt{-14})$. However, sim. seen ⇓

$$\frac{\mathbb{Z}[T]}{(T^2 + 14, T + 2)} \simeq \frac{\mathbb{Z}}{18\mathbb{Z}}$$

   which is not a domain, hence the ideal is not prime. 6, B

2. (a) A prime number p ramifies in $\mathcal{O}_K$ if in the decomposition

seen ⇓

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$$

with $\mathfrak{p}_i$ distinct prime ideals, at least one $e_i > 1$.

4, A

(b) $35 \equiv 3 \mod 4$, hence $D_K = 4 \cdot 35 = 4 \cdot 5 \cdot 7$ and we know that p ramifies if and only if it divides the discriminant, hence $p = 2, 5, 7$ are the primes that ramify in $\mathcal{O}_K$.

meth seen ⇓

4, A

(c) $M_K = \sqrt{35} < 6$. For $p = 2$, we get $2\mathcal{O}_K = \mathfrak{p}_2^2$, with $\mathfrak{p}_2 = (2, 1 + \sqrt{35})$, while $3\mathcal{O}_K$ is prime. Also $p = 5$ ramifies, i.e. $(5) = \mathfrak{p}_5^2$, with $\mathfrak{p}_5 = (5, \sqrt{35})$. However, we observe that

meth seen ⇓

$$5 + \sqrt{35} = 5(1 + \sqrt{35}) - 4\sqrt{35} \in \mathfrak{p}_2 \cdot \mathfrak{p}_5$$

Hence, for norm reasons, $(5 + \sqrt{35}) = \mathfrak{p}_2 \cdot \mathfrak{p}_5$. Since the Minkowski bound is < 6 primes of norm ≤ 5 describe the class group. The only non-trivial prime ideal in the class group of $\mathcal{O}_K$ is $\mathfrak{p}_2$, which is such that $\mathfrak{p}_2^2$ is principal. Finally, $\sqrt{2}$ is not principal, otherwise, there would exists an element $a + b\sqrt{35}$ of norm 2. Namaely, there exists $a, b \in \mathbb{Z}$ such that $a^2 - 35b^2 = \pm 2$. However,

$$a^2 \equiv 2 \mod 5$$

has no solutions and

$$a^2 \equiv -2 \mod 7$$

has no solutions.

6, A

(d) We know that an odd prime p splits in a quadratic field if and only if $\left(\frac{d}{p}\right) = 1$. In this case, we have

meth seen ⇓

$$\left(\frac{35}{p}\right) = \left(\frac{7}{p}\right)\left(\frac{5}{p}\right).$$

By quadratic reciprocity

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$$

and

$$\left(\frac{7}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{7}\right).$$

Finally, since $p \equiv 1 \mod 28$, we have that $(-1)^{(p-1)/2}\left(\frac{p}{7}\right) = 1$ and hence

$$\left(\frac{35}{p}\right) = 1 \quad \Leftrightarrow \quad \left(\frac{p}{5}\right) = 1.$$

6, B

3. (a) Let R be a domain, then R is integrally closed if for every element $x \in \mathrm{Frac}(R)$ such that there exists $p(T) \in R[T]$ monic with $p(x) = 0$, $x \in R$.

seen ⇓

4, A

(b) Let $\alpha \in \mathcal{O}_K \setminus R$, then by definition of $\mathcal{O}_K$, the minimal polynomial m_α of α is a monic polynomial with integer coefficients such that $m_\alpha(\alpha) = 0$. Hence α is an element of K which is a root of a monic polynomial with coefficients in R and does not belong to R.

sim. seen ⇓

6, C

(c) Take $K = \mathbb{Q}(\sqrt{5})$ and $R = \mathbb{Z}[\sqrt{5}]$. Then $\mathrm{Frac}(R) = \mathbb{Q}(\sqrt{5})$ and $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

unseen ⇓

4, D

sim. seen ⇓

(d) Let $\mathfrak{p}$ be a non-zero prime ideal of R, then we want to show that $R/\mathfrak{p}$ is finite. In fact, since finite domains are fields, this is enough to prove that every non-zero prime ideal is maximal. Let $\alpha \in \mathfrak{p}$ be a non-zero element, and $m_\alpha(T) = T^r + \cdots + a_0 \in \mathbb{Z}[T]$ be its minimal polynomial. Then

$$m_\alpha(\alpha) = 0 \Rightarrow a_0 = -\alpha(\alpha^{n-1} + \cdots + a_1) \in \mathfrak{p} \cap \mathbb{Z}.$$

Hence,

$$\#(R/\mathfrak{p}) \leq \#(R/a_0).$$

Finally, since $R \subseteq \mathcal{O}_K$ and $\mathcal{O}_K$ is a free abelian group of rank n, by the weak form of the structure theorem R is free of rank $q \leq n$. Therefore,

$$\#(R/a_0) = \#(\mathbb{Z}^q/a_0) \simeq \#(\mathbb{Z}/a_0\mathbb{Z})^q < \infty.$$

6, D

4. (a) If $\mathfrak{p} \mid (y+\sqrt{-37})$ and $\mathfrak{p} \mid (y-\sqrt{-37})$, then $2\sqrt{-37} \in \mathfrak{p}$, hence either $2 \in \mathfrak{p}$ or $\sqrt{-37} \in \mathfrak{p}$. Both 2 and 37 ramify in $\mathcal{O}_{-37}$, hence $2 \in \mathfrak{p}$, implies that $\mathfrak{p} = \mathfrak{p}_2$ is the only prime ideal above 2 and $\sqrt{-37} \in \mathfrak{p}$, implies $\mathfrak{p} = \mathfrak{p}_{37}$, the only prime ideal above 37. meth seen ⇓ 4, B

(b) - $\mathfrak{p} = \mathfrak{p}_2$, in this case, we get that $(y-\sqrt{-37})(y+\sqrt{-37}) \in \mathfrak{p}_2^2 = (2)\mathcal{O}_K$, hence $y^2 + 37 \equiv 0 \mod 2$, which implies that $x^3 \equiv 0 \mod 2$, hence $x \equiv 0 \mod 2$ and therefore $y^2 \equiv -37 \mod 8$, which is not possible. meth seen ⇓

- $\mathfrak{p} = \mathfrak{p}_7$, in this case, we get that $(y-\sqrt{-37})(y+\sqrt{-37}) \in \mathfrak{p}_{37}^2 = (37)\mathcal{O}_K$, hence $y^2 \equiv 0 \mod 37$, which implies that $37^2 \mid y$, hence since $x^3 - y^2 = 37$ also $37 \mid x$, which implies that $37^2 \mid x^3 - y^2 = 37$, which is not possible. 6, C

(c) It follows from unique factorisation into prime ideals in Dedekind rings and the fact that the two ideals $(y+\sqrt{-37})$ and $(y-\sqrt{-37})$ are coprimes. 4, B

(d) Since the ideal class of $\mathfrak{a}$ has order dividing 3 and $\mathrm{Cl}(\mathcal{O}_K)$ has order 2, $\mathfrak{a}$ has to have order 1, namely is principal. We can therefore write $\mathfrak{a} = (a+\sqrt{-37}b)$ for some $a, b \in \mathbb{Z}$. In particular, the equation meth seen ⇓

$$(y+\sqrt{-37}) = ((a+b\sqrt{-37})^3)$$

implies that $y+\sqrt{-37} = \pm(a+b\sqrt{-37})^3$[1], hence without loss of generality there exists $a, b \in \mathbb{Z}$ such that

$$y+\sqrt{-37} = (a+b\sqrt{-37})^3 = (a^3+3ab^2(-37)) + (3a^2b - 37b^3)\sqrt{-37}.$$

In particular, we get $1 = b(3a^2 - 37b^2)$, which implies that $b = \pm 1$ and $3a^2 - 37 = \pm 1$, which implies that $3a^2 = 38$ or $3a^2 = -36$ and both these equations have no solutions. 6, D

[1]Here we are using that $\mathbb{Z}[\sqrt{-37}]^\times = \{\pm 1\}$.

5. (a) By what we have seen in class we just need to find solutions to $a^2 - 82b^2 = \pm 1$ with the smallest value of b. Note that for $b = 1$, the equation $a^2 - 88b^2 = -1$ has $a = 9$ as a solution. Hence

meth seen ⇓

$$\epsilon = 9 + \sqrt{82}$$

is the fundamental unit.

4, M

(b) We have that the Minkowski constant C_K is < 10. Hence we just need to check that we do not need prime above 5 and 7.

meth seen ⇓

- for $p = 5$, we have
$$T^2 - 82 \equiv T^2 - 2 \mod 5$$
which is irreducible, hence 5 is inert.
- for $p = 7$ we have
$$T^2 - 82 \equiv T^2 - 5 \mod 7$$
which is also irreducible, hence 7 is inert as well.

4, M

(c) Note that $N_K(10 + \sqrt{82}) = 10^2 - 82 = 18 = 2 \cdot 3^2$. Hence, if we denote by I the ideal generated by $10 + \sqrt{82}$, then $I = \mathfrak{p}_2 \cdot J$ with J ideal lying above 3. Assume that both $\mathfrak{p}_3$ and $\bar{\mathfrak{p}}_3$ appear in the factorisation in prime ideals of J, then $3 \in I$, which would imply that $N(I) \mid N(3) = 9$. Finally, $10 + \sqrt{82} = 9 + (1 + \sqrt{82}) \in \mathfrak{p}_3$.

unseen ⇓

6, M

(d) From the previous point we know that $[\mathfrak{p}_2] = [\mathfrak{p}_3]^2$, hence the class group is generated by $\mathfrak{p}_3$. We are left to show that $\mathfrak{p}_2$ is not principal. Assume $\mathfrak{p}_2 = (\alpha) = (a + \sqrt{82}b)$, then $2\mathcal{O}_K = (a + b\sqrt{82})^2\mathcal{O}_K$, namely there exists $u \in \mathbb{Z}[\sqrt{82}]^\times$ such that

meth seen ⇓

$$2 = u \cdot (a + b\sqrt{82})^2.$$

Note that by point $1.$ we know that $u = (9 + \sqrt{82})^k$ for some $k \in \mathbb{Z}$. Now, since $N_K(u) = N_K(9 + \sqrt{82})^k = (-1)^k$, and $N_K(2), N_K((a + b\sqrt{82})^2) = N_K(a + b\sqrt{82})^2 \geq 0$, we get that k has to be even. In particular

$$2 = (u_0(a + b\sqrt{82}))^2$$

which implies that $\sqrt{2} \in \mathbb{Z}[\sqrt{82}]$, that gives the desired contradiction.

6, M

Review of mark distribution:
Total A marks: 32 of 32 marks
Total B marks: 20 of 20 marks
Total C marks: 12 of 12 marks
Total D marks: 16 of 16 marks
Total marks: 100 of 80 marks
Total Mastery marks: 20 of 20 marks

MATH70042 Algebraic Number Theory Markers Comments

Question 1	Overall, Question 1 was done well. In part (a), a common mistake was to give a tautological definition of the ring of integers, stating that it is the ring consisting of algebraic integers without explaining what algebraic integers are. Parts (b) and (c) were answered well by the majority. Part (d) was more challenging. Even though similar arguments were discussed in class, only about half of the students realised that 36=2(2+\sqrt{-14})(2−\sqrt{-14}), an observation that was necessary to analyse the ideal J.
Question 2	Question 2 was done well overall. In part (a), some students gave the definition of totally ramified instead of ramified primes, which caused them to lose some points. Parts (b) and (c) were done well. In part (d), the most challenging part, a common mistake was failing to mention—or to use correctly—quadratic reciprocity, which was one of the main ingredients needed to answer the question.
Question 3	I expected Question 3 to be more challenging; instead, I was pleased to find that students performed well overall. Parts (a), (b), and (c) were on average answered well. Part (d) was more difficult, and not many students provided the correct argument. There were different possible strategies, but all required recalling the approach we discussed in class for proving that, in the ring of integers of a number field, every non-zero prime ideal is maximal.
Question 4	Question 4 was the best-answered question overall. Students generally had the correct strategy in mind; the few mistakes were mostly computational.
Question 5	Question 5 was probably the hardest one. Most students were able to answer parts (a) and (b) correctly. In part (c), there was a typo (which was pointed out by a student during the exam, and all students were informed). Part (c) remained difficult—even with the hint, not many students managed to carry out the computations efficiently or include all the necessary details to reach a conclusion. Part (d) was also tricky, as it required keeping track of units other than ±1.