Imperial College
London

MATH70042

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)
May 2023

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

Algebraic Number Theory

Date: 16 May 2023

Time: 14:00 – 16:30 (BST)

Time Allowed: 2.5hrs

This paper has 5 Questions.

Please Answer All Questions in 1 Answer Booklet

Candidates should start their answers 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.

Allow margins for marking.

Credit will be given for all questions attempted.

Each question carries equal weight.

DO NOT OPEN THIS PAPER UNTIL THE INVIGILATOR TELLS YOU TO

You can use, without proof, any results from the lectures provided you state them correctly and clearly.

1. (a) Write the matrix:

$$\begin{pmatrix} 88 & 34 \\ 119 & 46 \end{pmatrix}$$

in the form SAT, where $S, T \in GL_2(\mathbb{Z})$ and A is a diagonal matrix with diagonal entries $a_{11}, a_{22} \in \mathbb{Z}$ such that $a_{11} | a_{22}$. (7 marks)

(b) Let R be a Dedekind domain and let $I, J \triangleleft R$ be two non-zero ideals. Show that $I + J = R$ if and only if I, J do not have a common prime factor in their prime factorisation. (5 marks)

(c) Is it true that for every Dedekind domain R which is not a field there is a non-zero proper ideal $I \triangleleft R$ such that the quotient R/I is finite? Justify your answer. (2 marks)

(d) Let R be a Dedekind domain and let $k \subseteq R$ be a subfield. Then R has a structure of a k-linear vector space and every ideal $I \triangleleft R$ is a k-linear subspace. Assume that for every non-zero prime ideal $\mathfrak{p} \triangleleft R$ the quotient $R/\mathfrak{p}$ is a finite dimensional k-linear vector space. Show that for every non-zero ideal $I \triangleleft R$ the quotient R/I is a finite dimensional k-linear vector space, and for every non-zero $I, J \triangleleft R$ we have:

$$\dim_k(R/IJ) = \dim_k(R/I) + \dim_k(R/J).$$

(6 marks)

(Total: 20 marks)

2. Let K be a number field, and let $\mathcal{O}_K$ denote the ring of integers of K.

(a) Give the definition of the norm $N(I)$ of a non-zero ideal $I \triangleleft \mathcal{O}_K$. Give the definition of the norm $N(J)$ of a non-zero fractional ideal J of $\mathcal{O}_K$. (3 marks)

(b) Let $K = \mathbb{Q}(\sqrt{-5})$. Factorise the following ideals in $\mathcal{O}_K$ into a product of prime ideals:

$$(3 + \sqrt{-5}), (49, 21 + 7\sqrt{-5}, 4 + 6\sqrt{-5}), (3 + \sqrt{-5}, 1 + 2\sqrt{-5}).$$

(You are required to give details of your calculation.) (10 marks)

(c) Let $I \triangleleft \mathcal{O}_K$ be such that the greatest common divisor of the norms of all $\alpha \in I$ is a prime number p. Show that I is a prime ideal of norm p. (3 marks)

(d) Let K be a quadratic number field and let p be a prime number ramified in K. Show that the greatest common divisor of the norms of all elements of the unique prime ideal $\mathfrak{p} \triangleleft \mathcal{O}_K$ of norm p is the number p. (4 marks)

(Total: 20 marks)

3. (a) Find every reduced integral quadratic form of discriminant -139. You need to justify your answer. (14 marks)

(b) Compute the class group $Cl(\mathcal{O}_{-139})$. What is the relation with the reduced quadratic forms in part (a)? (3 marks)

(c) Find a non-zero ideal $\mathfrak{a} \lhd \mathcal{O}_{-139}$ whose class has order 3. Justify your answer. (3 marks)

(Total: 20 marks)

4. Let x, y be integer solutions of the Diophantine equation:

$$x^2 + 32 = y^4.$$

Show that $x = \pm 7$ and $y = \pm 3$. (20 marks)

(Total: 20 marks)

5. (a) Let n be a positive integer. Show that n is the sum of two squares of integers if and only if it is the sum of two squares of rational numbers. (5 marks)

Now let $x, y, z \in \mathbb{Q}$ be such that $x^2 + y^2 + z^2 \in \mathbb{Z}$.

(b) Let

$$\widetilde{\Lambda} = \{(u + tx, v + ty, w + tz) \in \mathbb{R}^3 \mid u, v, w, t \in \mathbb{Z}\},$$

and

$$\Lambda = \{(u + tx, v + ty, w + tz) \in \mathbb{R}^3 \mid u, v, w, t \in \mathbb{Z},\ ux + vy + wz \in \mathbb{Z}\}.$$

Show that $\widetilde{\Lambda}$ and Λ are discrete lattices of rank 3 and $[\widetilde{\Lambda} : \Lambda] = [\widetilde{\Lambda} : \mathbb{Z}^3]$.

(4 marks)

(c) Let

$$\Omega = \{(a, b, c) \in \mathbb{R}^3 \mid a^2 + b^2 + c^2 < 2\}.$$

Apply Minkowski's first theorem to Ω and Λ to deduce that there exist $a, b, c \in \mathbb{Q}$ such that $a^2 + b^2 + c^2 = 1$ and $ax + by + cz \in \mathbb{Z}$. (You need to check that the conditions of the theorem apply.) (7 marks)

(d) Show that $x^2 + y^2 + z^2$ is the sum of three squares of integers.

[*Hint: use the following identity; let a, b, c be such that $a^2 + b^2 + c^2 = 1$ and $b^2 + c^2 \neq 0$. Then*

$$x^2 + y^2 + z^2 = (ax + by + cz)^2 + U^2 + V^2,$$

where

$$U = bx - \frac{ab^2 + c^2}{b^2 + c^2}y + \frac{-abc + bc}{b^2 + c^2}z,$$

$$V = cx + \frac{-abc + bc}{b^2 + c^2}y - \frac{ac^2 + b^2}{b^2 + c^2}z.]$$

(4 marks)

(Total: 20 marks)

Module:	MATH96028/MATH97037/MATH97145
Setter:	Pál
Checker:	Skorobogatov
Editor:	Pál
External:	Lotay
Date:	April 5, 2023
Version:	Draft version for checking

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)

May – June 2023

MATH96028/MATH97037/MATH97145 Algebraic Number Theory Solutions

The following information must be completed:

Is the paper suitable for resitting students from previous years:

Category A marks: available for basic, routine material (excluding any mastery question) (40 percent = 32/80 for 4 questions):
1(a) 7 marks; 2(a) 3 marks; 3(a) 14 marks; 4) 8 marks.

Category B marks: Further 25 percent of marks (20/ 80 for 4 questions) for demonstration of a sound knowledge of a good part of the material and the solution of straightforward problems and examples with reasonable accuracy (excluding mastery question):
1(b) 5 marks; 1(c) 2 marks; 2(b) 10 marks; 3(b) 3 marks

Category C marks: the next 15 percent of the marks (= 12/80 for 4 questions) for parts of questions at the high 2:1 or 1st class level (excluding mastery question):
2(d) 4 marks; 3(c) 3 marks; 4) 5 marks.

Category D marks: Most challenging 20 percent (16/80 marks for 4 questions) of the paper (excluding mastery question):
1(d) 6 marks; 2(c) 3 marks; 4) 7 marks.

Signatures are required for the final version:

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

Temporary front page

BSc, MSc and MSci EXAMINATIONS (MATHEMATICS)

May – June 2023

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

Algebraic Number Theory Solutions

Date: ??

Time: ??

Time Allowed: 2 Hours for MATH96 paper; 2.5 Hours for MATH97 papers

This paper has *4 Questions (MATH96 version); 5 Questions (MATH97 versions)*.

Statistical tables will not be provided.

- Credit will be given for all questions attempted.
- Each question carries equal weight.

1. (a) This problem can be solved by the algorithm presented in the lectures. First we do the following row and column operations:

$$\begin{pmatrix} 88 & 34 \\ 119 & 46 \end{pmatrix} \mapsto \begin{pmatrix} 20 & 34 \\ 27 & 46 \end{pmatrix} \mapsto \begin{pmatrix} 20 & 14 \\ 27 & 19 \end{pmatrix} \mapsto \begin{pmatrix} 6 & 14 \\ 8 & 19 \end{pmatrix} \mapsto \begin{pmatrix} 6 & 2 \\ 8 & 3 \end{pmatrix} \mapsto \begin{pmatrix} 0 & 2 \\ -1 & 3 \end{pmatrix} \mapsto$$

$$\begin{pmatrix} 0 & 2 \\ -1 & 0 \end{pmatrix} \mapsto \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

All but the last one are column operations. The corresponding elementary matrices and their product are:

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -3 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 119 & 46 \\ 44 & 17 \end{pmatrix},$$

so the corresponding factorisation is:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 119 & 46 \\ 44 & 17 \end{pmatrix}.$$

A, *similar seen* (7 marks)

(b) First assume that $I + J = R$. If I, J have a common prime factor $\mathfrak{p}$, then $I, J \subseteq \mathfrak{p}$, and hence $I + J \subseteq \mathfrak{p} + \mathfrak{p} = \mathfrak{p}$, a contradiction. Now assume that I, J have no common prime factor, but $I + J \neq R$. Then the ideal $I + J$ is proper, so it is contained in a proper maximal ideal $\mathfrak{p}$, which is prime. Then $I, J \subseteq I + J \subseteq \mathfrak{p}$, which means that $\mathfrak{p}$ is a common factor, a contradiction. **B**, *similar seen* (5 marks)

(c) Set $R = \mathbb{C}[x]$. Then R is a PID, so it is a Dedekind domain. For every proper ideal $I \lhd R$ the quotient R/I is a non-zero vector space over $\mathbb{C}$, so it is infinite. **B**, *similar seen* (2 marks)

(d) Note that the second claim implies the first by induction on the length of the prime factorisation of I. So we only need to show that latter in the special case when J is a prime ideal $\mathfrak{p}$, again by induction on the length of the prime factorisation. Clearly $\dim_k(R/I\mathfrak{p}) = \dim_k(R/I) + \dim_k(I/I\mathfrak{p})$, so it will be enough to show that $I/I\mathfrak{p} \cong R/\mathfrak{p}$ even as $R/\mathfrak{p}$-linear vector spaces. (Recall that $R/\mathfrak{p}$ is a field, and note that it contains k.) If the latter were false, there would be an ideal $\mathfrak{q} \lhd R$ such that $I\mathfrak{p} \subsetneq \mathfrak{q} \subsetneq I$. Then

$$I^{-1}(I\mathfrak{p}) = \mathfrak{p} \subsetneq I^{-1}\mathfrak{q} \subsetneq I^{-1}I = (1),$$

but this is not possible since $\mathfrak{p}$ is a maximal ideal. **D**, *similar seen* (6 marks)

(Total: 20 marks)

2. (a) The norm $N(I)$ is the cardinality of the finite quotient group $\mathcal{O}_K/I$.

Write J as $(\alpha)I$, where $\alpha \in K^*$ and $I \triangleleft \mathcal{O}_K$, and set $N(J) = |N(\alpha)| \cdot N(I)$. This is independent of the choice of α and I. **A**, *seen* (3 marks)

(b) Since $N(3+\sqrt{-5}) = 14 = 2 \cdot 7$, the ideal $(3+\sqrt{-5})$ is a product of a prime of norm 2 and of norm 7. The obvious choice works:

$$(2, 3+\sqrt{-5})(7, 3+\sqrt{-5}) = (14, 2(3+\sqrt{-5}), 7(3+\sqrt{-5}), (3+\sqrt{-5})^2) =$$

$$((3+\sqrt{-5})(3-\sqrt{-5}), 3+\sqrt{-5}) = (3+\sqrt{-5}).$$

B, *similar seen* (4 marks)

Note that

$$(7, 3+\sqrt{-5})^2 = (49, 21+7\sqrt{-5}, 4+6\sqrt{-5}),$$

so this is the prime factorisation of the ideal $(49, 21+7\sqrt{-5}, 4+6\sqrt{-5})$. **B**, *similar seen*

(3 marks)

Finally

$$(3+\sqrt{-5}, 1+2\sqrt{-5}) = (3+\sqrt{-5}, -5).$$

The norms $N(3+\sqrt{-5}) = 14$ and $N(-5) = 25$ are divisible by the norm of the ideal $(3+\sqrt{-5}, 1+2\sqrt{-5})$. However they are also relatively prime, so the norm of $(3+\sqrt{-5}, 1+2\sqrt{-5})$ is 1. Therefore the prime factorisation of this ideal is the empty product. **B**, *similar seen*

(3 marks)

(c) The norm $N(I)$ divides the norm of all $\alpha \in I$, and hence it divides p. The ideal I is not zero, otherwise the only norm possible for $\alpha \in I$ would be zero, and for the same reason $1 \notin I$, since the norm of the latter is 1. So I is proper, and hence its norm is exactly p. Since ideals of prime norm are prime, the ideal I is a prime ideal. **D**, *similar seen* (3 marks)

(d) Let d be a square-free integer such that $K = \mathbb{Q}(\sqrt{d})$. Note that every $\alpha \in \mathcal{O}_K$ whose norm is divisible by p is in $\mathfrak{p}$ as $\mathfrak{p}$ is the unique prime above p. If $p|d$ then $p, \sqrt{d} \in \mathfrak{p}$ by the above and $(N(p), N(\sqrt{d})) = (p^2, -d) = p$ as d is square-free. Now assume that p does not divide d. Since it divides the discriminant, we get that $p = 2$ and $d \equiv 3 \mod 4$. Then $2, 1+\sqrt{d} \in \mathfrak{p}$ and $(N(2), N(1+\sqrt{d})) = (4, 1-d) = 2$ as $1-d \equiv 2 \mod 4$. **C**, *similar seen* (4 marks)

(Total: 20 marks)

3. (a) We know that every reduced form of discriminant -139 (a prime) is of the form $aX^2+bXY+cY^2=[a,b,c]$ for some $a,b,c\in\mathbb{Z}$ such that $-139=b^2-4ac$, $|b|\leq a\leq c$, moreover $b\geq 0$ if any of the two equalities occurs, and finally $a\leq\sqrt{\frac{139}{3}}<7$. So $1\leq a\leq 6$ and b must be odd. Now we compute: **A**, *similar seen* (4 marks)

$a=1$ In this case $b=1$ and $c=140/4=35$, hence we find the form $[1,1,35]$. **A**, *similar seen* (1 mark)

$a=2$ In this case $b=\pm 1$. We get the equation $-8c=-140$ which has no integral solution. No forms in this case. **A**, *similar seen* (1 mark)

$a=3$ In this case $b=\pm 1,3$. In the first case we get the equation $-12c=-140$ which has no integral solution. In the second case we get the equation $-12c=-148$, which has no integral solution. No forms in this case. **A**, *similar seen* (2 marks)

$a=4$ In this case we have $b=\pm 1,\pm 3$. These lead to the equations $-16c=-140$ and $-16c=-148$, respectively, which have no integral solutions. No forms in this case. **A**, *similar seen* (2 marks)

$a=5$ In this case we have $b=\pm 1,\pm 3$ or $b=5$. These lead to the equations $-20c=-140$, $-20c=-148$ and $-20c=-164$, respectively, of which only the first has a solution. Hence we find the forms $[5,\pm 1,7]$. **A**, *similar seen* (2 marks)

$a=6$ In this case we have $b=\pm 1,\pm 3$ or $b=\pm 5$. These lead to the equations $-24c=-140$, $-24c=-148$, and $-24c=-164$, which have no solutions. No forms in this case.

So the reduced forms are $[1,1,35]$ and $[5,\pm 1,7]$. **A**, *similar seen* (2 marks)

(b) By a fundamental theorem the class number of $\mathcal{O}_{-139}$, which is the order of $Cl(\mathcal{O}_{-139})$, is equal to the cardinality of reduced forms of discriminant -139. Therefore the class number of $\mathcal{O}_{-139}$ is 3. Since this order is a square-free number, the class group is isomorphic to the cyclic group $\mathbb{Z}/3\mathbb{Z}$. **B**, *similar seen* (3 marks)

(c) Every non-principal ideal has order 3 in the class group. One such ideal is $(5,1+\sqrt{-139})$, since its norm is 5:

$$(5,1+\sqrt{-139})(5,1-\sqrt{-139})=(25,5(1+\sqrt{-139}),140)=(5),$$

but there is no element of norm 5 (the equation $x^2+139y^2=5$ or 20 has no solution). **C**, *similar seen* (3 marks)

(Total: 20 marks)

4. First assume that y is even. Then $x^2 \equiv y^4 \equiv 0 \mod 16$, so $4|x$. Write $x = 4r$ and $y = 2s$. Then $r^2 + 2 = s^4$. Since $r^2 \equiv 0, 1 \mod 4$, we get that $s^4 \equiv 2, 3 \mod 4$, but since s^4 is a square this is not possible. Therefore y is odd. **A**, *similar seen* (5 marks)

We factor the equation in $\mathbb{Z}[\sqrt{-2}]$, which is a PID, as follows: $(x+4\sqrt{-2})(x-4\sqrt{-2}) = y^4$. Let d be a common divisor of $x + 4\sqrt{-2}$ and $x - 4\sqrt{-2}$. Then $d|8\sqrt{-2}$ and $d|y^4$. So the norm of d divides the greatest common divisor of 128 and y^8. But y is odd, so the former is 1, and we get that $x + 4\sqrt{-2}$ and $x + 4\sqrt{-2}$ are relatively prime. **C**, *similar seen* (5 marks)

Since $\mathbb{Z}[\sqrt{-2}]$ is a PID we may apply the separation of powers trick to get that $x + 4\sqrt{-2} = u(a + \sqrt{-2}b)^4$ for some $u \in \mathbb{Z}[\sqrt{-2}]^*$ and $a, b \in \mathbb{Z}$. Since $\mathbb{Z}[\sqrt{-2}]^* = \{\pm 1\}$, we get, by looking at the imaginary part, the following equations:

$$4 = \pm(4a^3b - 8ab^3), \text{ and hence } 1 = \pm ab(a^2 - 2b^2).$$

D, *similar seen* (5 marks)

Since a, b divide 1, both a, b must be one of ± 1. By looking at the real part we get that only

$$x = \pm(a^4 - 12a^2b^2 + 4b^4) = \pm(1 - 12 + 4) = \mp 7$$

is possible, and hence $y = \pm 3$. These are actually solutions. **A,C**, *similar seen* (5 marks)

(Total: 20 marks)

5. (a) The first condition trivially implies the second, so let's prove the converse. Assume that $n = x^2 + y^2$ with $x, y \in \mathbb{Q}$. Write $x = x_1/d, y = y_1/d$ with $x_1, y_1, d \in \mathbb{Z}$ and $d \neq 0$. Then $x_1^2 + y_1^2 = n \cdot d^2$. Since the RHS is a sum of two squares of integers, every prime congruent to 3 mod 4 divides it to an even power. Therefore the same holds for n, too, and hence the latter is a sum of two squares of integers, since this property characterises the sum of two squares. *unseen*

(5 marks)

(b) Let d be the smallest positive integer such that $x = x_1/d, y = y_1/d, z = z_1/d$ with $x_1, y_1, z_1 \in \mathbb{Z}$; then $\gcd(x_1, y_1, z_1, d) = 1$. Clearly $\widetilde{\Lambda} \supseteq \Lambda$ are subgroups of $\mathbb{R}^3$, and

$$\widetilde{\Lambda} = \{(u + tx, v + ty, w + tz) \in \mathbb{R}^3 \mid u, v, w \in \mathbb{Z}, t = 0, 1, \ldots, d - 1\},$$

so $[\widetilde{\Lambda} : \mathbb{Z}^3] = d$. In particular $\widetilde{\Lambda}$ is a discrete lattice. Moreover $ux + vy + wz \in \mathbb{Z}$ if and only if $ux_1 + vy_1 + wz_1 \equiv 0 \mod d$, so $[\widetilde{\Lambda} : \Lambda] = d$. As a finite index subgroup of a discrete lattice, the latter is also a discrete lattice. *similar seen* (4 marks)

(c) Since $\mathrm{covol}(\mathbb{Z}^3) = 1$, we get that $\mathrm{covol}(\Lambda) = 1$ from part (b). Clearly Ω is a convex, symmetric open subset such that

$$\mathrm{vol}(\Omega) = \frac{4\pi}{3}(\sqrt{2})^3 > 8 = 8 \cdot \mathrm{covol}(\Lambda).$$

Therefore by Minkowski's first theorem there exists an $(a, b, c) \in \Lambda$ such that

$$(a, b, c) = (u + tx, v + ty, w + tz), \quad 0 < a^2 + b^2 + c^2 < 2.$$

Since

$$a^2 + b^2 + c^2 = u^2 + v^2 + w^2 + 2t(ux + vy + wz) + t^2(x^2 + y^2 + z^2) \in \mathbb{Z},$$

we must have

$$a^2 + b^2 + c^2 = 1,$$

and

$$ax + by + cz = ux + vy + wx + t(x^2 + y^2 + z^2) \in \mathbb{Z}.$$

similar seen (7 marks)

(d) Let $a, b, c \in \mathbb{Q}$ be as in part (c). We may assume that $b^2 + c^2 \neq 0$ without the loss of generality by rearranging the order of x, y, z, if it is necessary. Let U, V be as in the hint. Then $U^2 + V^2$ is an integer by the identity which is also a sum of two squares of rational numbers. Therefore it is a sum of two squares of integers by part (a). The claim now follows from the identity. *unseen*
(4 marks)

(Total: 20 marks)

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.		
ExamModuleCode	**QuestionNumber**	**Comments for Students**
MATH60042/70042	1	Part (a) could be done via a routine computation, which many students did well. However often the solution did not contain the matrices S,T, although the problem explicitly asked for it. It could also be done by noticing that the determinant of the matrix is 2, while the second column is divisible by 2, which implies a trivial decomposition. Parts (b), (c), (d) were more challenging, checking the understanding of the theory of Dedekind rings, but the proofs were all seen in one form or another. In particular (d) was just a variant of the proof of the multiplicativity of norms of ideals in rings of integers of number fields.
MATH60042/70042	2	Part (a) was bookwork, part (b) was routine computation with ideals, which most students did well. Parts (c), (d) required arguments, but these were standard, like divisibility implies divisibility of norms, ideals of prime norm are prime, etc.
MATH60042/70042	3	Most students did this problem well, including the computation of reduced forms, the relation with the class group and providing an ideal which is a generator.
MATH60042/70042	4	I was the most happy marking this problem; many students carried out the routine argument correctly adapted to this new situation, while a lot of other students used a different, completely elementary and beautiful approach by moving x^2 to the other side, factorising the right hand side and just using the arithmetic properties of integers.
MATH70042	5	This mastery question turned out to be more challenging than I expected, although it was largely routine, except part (a). The latter is a consequence of the two squares theorem, but not many candidates realised this.