IMPERIAL

MATH70042

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)
May 2024

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

Algebraic Number Theory

Date: Friday, May 24, 2024

Time: 10:00 – 12:30 (BST)

Time Allowed: 2.5 hours

This paper has 5 Questions.

Please Answer All Questions in 1 Answer Booklet

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.

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

1. (a) Give the definition of an *algebraic integer*. (3 marks)

   (b) Prove that $\sqrt[3]{3+\sqrt{2}}$ is an algebraic integer. (4 marks)

   (c) Let K be a number field. Define the *norm* $N_K(\alpha)$ and *trace* $\mathrm{tr}_K(\alpha)$ of an element $\alpha \in K$. (3 marks)

   (d) Give an example of an algebraic integer α with $N_{\mathbf{Q}(\alpha)}(\alpha) = 1$ and $\mathrm{tr}_{\mathbf{Q}(\alpha)}(\alpha) = 2$. Justify your answer. (5 marks)

   (e) Compute the discriminant of $\mathbf{Q}(\sqrt{2})$ directly from the definition. You may use without proof that the integer ring of $\mathbf{Q}(\sqrt{2})$ is $\mathcal{O}_2 = \mathbf{Z}[\sqrt{2}]$. (5 marks)

(Total: 20 marks)

2. In this problem $d \neq 0, 1$ is a squarefree integer.

   (a) Define what it means for a prime p to be *split*, *ramified*, or *inert* in the quadratic field $\mathbf{Q}(\sqrt{d})$. (4 marks)

   (b) Factor $(1+2\sqrt{-5}) \subseteq \mathcal{O}_{-5}$ into prime ideals. Justify your answer. (6 marks)

   (c) For which values of d is $(\sqrt{d}) \subseteq \mathcal{O}_d$ a prime ideal? Prove your answer. (4 marks)

   (d) Suppose that $d < 0$, $d \not\equiv 1 \pmod 4$, and $d \equiv 1 \pmod 3$ so that $(3) = \mathfrak{p}_3\overline{\mathfrak{p}}_3$ splits in $\mathcal{O}_d$. Let r be the order of $[\mathfrak{p}_3]$ in the class group $\mathrm{Cl}(\mathcal{O}_d)$. Prove that $3^r > -d$. (6 marks)

(Total: 20 marks)

3. (a) State the *Minkowski bound* for real and imaginary quadratic fields. (4 marks)

(b) Compute the class group of $\mathcal{O}_{77}$. You may use that $\frac{\sqrt{77}}{2} < 5$. (6 marks)

(c) Compute the class group of $\mathcal{O}_{-42}$. You may use that $\frac{4}{\pi}\sqrt{42} < 9$. (10 marks)

(Total: 20 marks)

4. In this question you will solve the Diophantine equation $y^2 = x^3 - 11$ for $x, y \in \mathbf{Z}$. You may use without proof that $\mathcal{O}_{-11}$ is a principal ideal domain.

(a) Rewrite the equation as $(y+\sqrt{-11})(y-\sqrt{-11}) = x^3$ and show that $y+\sqrt{-11}$ and $y-\sqrt{-11}$ are coprime elements of $\mathcal{O}_{-11}$. (5 marks)

(b) Prove that $y + \sqrt{-11} = \alpha^3$ for some $\alpha \in \mathcal{O}_{-11}$. (5 marks)

(c) Prove that the only solutions to $y^2 = x^3 - 11$ for $x, y \in \mathbf{Z}$ are $(x, y) = (3, \pm 4), (15, \pm 58)$. (10 marks)

(Total: 20 marks)

5. In this problem, K is an imaginary quadratic field. You may use any result from the course or the mastery material as long as you state it precisely.

(a) Define what it means for an extension of number fields L/K to be *unramified*. (3 marks)

(b) Define the *Hilbert class field* of K and state the relation between the Galois group and the class group of K. (3 marks)

(c) Prove that $K = \mathbf{Q}(\sqrt{-1})$ does not have an unramified quadratic extension. (5 marks)

(d) Prove that the Hilbert class field of $K = \mathbf{Q}(\sqrt{-15})$ is $L = \mathbf{Q}(\sqrt{-3}, \sqrt{5})$. You may use that $\frac{2}{\pi}\sqrt{15} < 3$. (9 marks)

(Total: 20 marks)

BSc and MSci EXAMINATIONS (MATHEMATICS)

May 2024

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) Give the definition of an *algebraic integer*.

3, A

seen ⇓

A complex number $\alpha \in \mathbf{C}$ is an algebraic integer if it is the root of a monic polynomial $f \in \mathbf{Z}[x]$.

(b) Prove that $\sqrt[3]{3+\sqrt{2}}$ is an algebraic integer.

4, A

meth seen ⇓

It is a root of the monic polynomial $(x^3-3)^2-2$.

(c) Let K be a number field. Define the *norm* $N_K(\alpha)$ and *trace* $\mathrm{tr}_K(\alpha)$ of an element $\alpha \in K$.

3, A

seen ⇓

The norm and trace are the determinant and trace of multiplication by α, $\alpha\cdot : K \to K$ viewed as an endomorphism of the $\mathbf{Q}$-vector space K.

(d) Give an example of an algebraic integer α with $N_{\mathbf{Q}(\alpha)}(\alpha) = 1$ and $\mathrm{tr}_{\mathbf{Q}(\alpha)}(\alpha) = 2$. Justify your answer.

3, B

2, C

unseen ⇓

We can take α to be a root of the monic polynomial $f(x) = x^3 - 2x^2 - 1$. This polynomial is irreducible by the rational root test since ± 1 are not roots. Hence f is the minimal monic polynomial of α. Now we can use the formulas for $N_{\mathbf{Q}(\alpha)}(\alpha)$ and $\mathrm{tr}_{\mathbf{Q}(\alpha)}(\alpha)$ in terms of the coefficients of the minimal monic polynomial of α: the norm is $(-1)^3$ times the constant term and the trace is -1 times the coefficient of x^2.

(e) Compute the discriminant of $\mathbf{Q}(\sqrt{2})$ directly from the definition. You may use without proof that the integer ring of $\mathbf{Q}(\sqrt{2})$ is $\mathcal{O}_2 = \mathbf{Z}[\sqrt{2}]$.

5, A

seen ⇓

Since the ring of integers is $\mathbf{Z}[\sqrt{2}]$, $1, \sqrt{2}$ is an integral basis. Then by definition the discriminant of $\mathbf{Q}(\sqrt{2})$ is

$$\mathrm{disc}(1,\sqrt{2}) = \det \begin{pmatrix} \mathrm{tr}(1\cdot 1) & \mathrm{tr}(1\cdot\sqrt{2}) \\ \mathrm{tr}(\sqrt{2}\cdot 1) & \mathrm{tr}(\sqrt{2}\cdot\sqrt{2}) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix} = 8$$

2. In this problem $d \neq 0, 1$ is a squarefree integer.

(a) Define what it means for a prime p to be *split*, *ramified*, or *inert* in the quadratic field $\mathbf{Q}(\sqrt{d})$.

4, A

seen ⇓

A prime p splits if $(p) = \mathfrak{p}_1\mathfrak{p}_2$ for two distinct prime ideals $\mathfrak{p}_1, \mathfrak{p}_2 \subset \mathcal{O}_d$. A prime p ramifies if $(p) = \mathfrak{p}^2$ for a prime ideal $\mathfrak{p}$ of $\mathcal{O}_d$. A prime p is inert if (p) is a prime ideal of $\mathcal{O}_d$.

(b) Factor $(1 + 2\sqrt{-5}) \subseteq \mathcal{O}_{-5}$ into prime ideals. Justify your answer.

4, A

2, B

meth seen ⇓

We compute the norm:

$$\|(1 + 2\sqrt{-5})\| = N(1 + 2\sqrt{-5}) = 21 = 3 \cdot 7$$

Hence $(1+2\sqrt{-5})$ must be the product of an ideal of norm 3 and an ideal of norm 7. We claim that

$$(1 + 2\sqrt{-5}) = (3, 1 + 2\sqrt{-5})(7, 1 + 2\sqrt{-5})$$

is the factorization into prime ideals. Indeed all four products of the generators on the right are multiplies of $1+2\sqrt{-5}$, while $1+2\sqrt{-5} = 7(1+2\sqrt{-5})-2\cdot3(1+2\sqrt{-5})$ is in the product. The ideals on the right cannot have norm 21 because they contain 3 and 7, so they must have norm 3 and 7 and hence are prime.

(c) For which values of d is $(\sqrt{d}) \subseteq \mathcal{O}_d$ a prime ideal? Prove your answer.

4, B

unseen ⇓

It is prime if and only if $d = \pm p$ for a prime number p. To prove this we compute the norm $\|(\sqrt{d})\| = |N(\sqrt{d})| = |d|$. Thus if $d = \pm p$ for p prime, $(\sqrt{d})$ has prime norm and is hence prime. Conversely if $(\sqrt{d})$ is prime, its norm is a prime power, but since d is squarefree $|d|$ must thus be prime.

(d) Suppose that $d < 0$, $d \not\equiv 1 \pmod 4$, and $d \equiv 1 \pmod 3$ so that $(3) = \mathfrak{p}_3\overline{\mathfrak{p}}_3$ splits in $\mathcal{O}_d$. Let r be the order of $[\mathfrak{p}_3]$ in the class group $\mathrm{Cl}(\mathcal{O}_d)$. Prove that $3^r > -d$.

6, D

unseen ⇓

If $[\mathfrak{p}_3]$ has order r in the class group, $\mathfrak{p}_3^r = (\alpha)$ is a principal ideal. Since $d \not\equiv 1 \pmod 4$, $\mathcal{O}_d = \mathbf{Z}[\sqrt{d}]$ and so $\alpha = x + y\sqrt{d}$ with $x, y \in \mathbf{Z}$. Taking norms we obtain $3^r = x^2 - dy^2$. If $y = 0$ then we must have $x = \pm 3^{r/2}$ and we obtain $\mathfrak{p}_3^r = (3)^{r/2} = \mathfrak{p}_3^{r/2}\overline{\mathfrak{p}}_3^{r/2}$ which contradicts unique factorization into prime ideals. Thus we must have $y \neq 0$. If $x = 0$ we would have $3^r = -dy^2$ which implies $d = -1, -3$ neither of which are possible. Hence $x, y \neq 0$ and so $3^r > -d$.

3. (a) State the *Minkowski bound* for real and imaginary quadratic fields.

4, A

seen ⇓

The Minkowski bound says that any ideal class in $\mathrm{Cl}(\mathcal{O}_K)$ contains an ideal I with $\|I\| < C_K$, where $C_K = \frac{\sqrt{D_K}}{2}$ if K is real quadratic and $C_K = \frac{2\sqrt{|D_K|}}{\pi}$ if K is imaginary quadratic, and D_K is the discriminant of K.

(b) Compute the class group of $\mathcal{O}_{77}$. You may use that $\frac{\sqrt{77}}{2} < 5$.

6, B

meth seen ⇓

Since this is real quadratic, and $77 \equiv 1 \pmod 4$ the discriminant is $D_K = 77$ and hence the Minkowski bound is $\frac{\sqrt{77}}{2} < 5$. Hence we need to determine how 2 and 3 factor. 2 is inert because $77 \equiv 5 \pmod 8$. 3 is inert because $77 \equiv 2 \pmod 3$ is not a square. Hence the only ideals with norm less than C_K are (1) and (2) which are principal, so the class group is trivial.

(c) Compute the class group of $\mathcal{O}_{-42}$. You may use that $\frac{4}{\pi}\sqrt{42} < 9$.

5, C

5, D

meth seen ⇓

Since this is imaginary quadratic and $42 \not\equiv 1 \pmod 4$, the discriminant is $D_K = -4 \cdot 42$ and the Minkowski bound is $\frac{4}{\pi}\sqrt{42} < 9$. We need to factor $2, 3, 5, 7$. 2,3, and 7 divide 42 and hence ramify, while $-42 \equiv 3 \pmod 5$ is not a square so 5 is inert.

Hence the class group is generated by $[\mathfrak{p}_p] = (p, \sqrt{-42})$ for $p = 2, 3, 7$ and these all have order 2 in the class group. Moreover $(\sqrt{-42}) = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_7$ and so $[\mathfrak{p}_7] = [\mathfrak{p}_2][\mathfrak{p}_3]$. We claim that $\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_2\mathfrak{p}_3$ are all not principal. Indeed $x^2 + 42y^2 = 2, 3, 6$ has no solutions. Thus $\mathrm{Cl}(\mathcal{O}_{-42}) \simeq (\mathbf{Z}/2\mathbf{Z})^2$ with generators $[\mathfrak{p}_2], [\mathfrak{p}_3]$.

4. In this question you will solve the Diophantine equation $y^2 = x^3 - 11$ for $x, y \in \mathbf{Z}$. You may use without proof that $\mathcal{O}_{-11}$ is a principal ideal domain.

(a) Rewrite the equation as $(y + \sqrt{-11})(y - \sqrt{-11}) = x^3$ and show that $y + \sqrt{-11}$ and $y - \sqrt{-11}$ are coprime elements of $\mathcal{O}_{-11}$.

5, B

meth seen ⇓

If a prime $\pi \in \mathcal{O}_{-11}$ divides $y + \sqrt{-11}$ and $y - \sqrt{-11}$ then it also divides

$$y + \sqrt{-11} - (y - \sqrt{-11}) = 2\sqrt{-11}$$

Hence either $2 \mid x$ or $11 \mid x$. If $2 \mid x$ then the equation mod 8 becomes $y^2 \equiv 5 \pmod 8$ which has no solutions. If $11 \mid x$ then also $11 \mid y$ but then $11^2 \mid y^2 - x^3 = -11$. Thus we must have $x + y\sqrt{-11}$ and $x - y\sqrt{-11}$ coprime.

(b) Prove that $y + \sqrt{-11} = \alpha^3$ for some $\alpha \in \mathcal{O}_{-11}$.

5, A

meth seen ⇓

We use that $\mathcal{O}_{-11}$ is a PID and hence a UFD. Since $y+\sqrt{-11}$ and $y-\sqrt{-11}$ have no common factors and their product is a cube, we conclude by unique factorizations that each are a cube up to a unit. But the only units are ± 1 and hence

$$y + \sqrt{-11} = \pm\alpha^3 = (\pm\alpha)^3.$$

(c) Prove that the only solutions to $y^2 = x^3 - 11$ for $x, y \in \mathbf{Z}$ are $(x, y) = (3, \pm 4), (15, \pm 58)$.

5, C

5, D

meth seen ⇓

We write $\alpha = \frac{a+b\sqrt{-11}}{2}$ for $a, b \in \mathbf{Z}$ and $a \equiv b \pmod 2$. We have

$$y + \sqrt{-11} = \left(\frac{a + b\sqrt{-11}}{2}\right)^3 = \frac{a^3 - 33ab^2 + (3a^2b - 11b^3)\sqrt{-11}}{8}$$

Equating the coefficients of $\sqrt{-11}$ we obtain the new Diophantine equation:

$$8 = b(3a^2 - 11b^2)$$

If a, b are odd, we must have $b = \pm 1$ and hence $3a^2 - 11 = \pm 8$ which yields the solutions $a = \pm 1, b = -1$. If a, b are even then $3a^2 - 11b^2$ is a multiple of 4 so we must have $b = \pm 2$ and hence $3a^2 - 11 \cdot 4 = \pm 4$ which yields the solutions $a = \pm 4, b = 2$.

Returning to the original equation we have

$$x = \frac{a^2 + 11b^2}{4}, y = \frac{a^3 - 33ab^2}{8}$$

giving the solutions $(x, y) = (3, \pm 4), (15, \pm 58)$.

5. In this problem, K is an imaginary quadratic field. You may use any result from the course or the mastery material as long as you state it precisely.

(a) Define what it means for an extension of number fields L/K to be *unramified*. [3, M]

L/K is unramified if for every prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$, $\mathfrak{p}\mathcal{O}_L$ factors into a product of distinct primes. (Note that we don't need to say anything about infinite primes because K is imaginary quadratic.) [seen ⇓]

(b) Define the *Hilbert class field* of K and state the relation between the Galois group and the class group of K. [3, M]

The Hilbert class field of K is the maximal unramified extension of K with abelian Galois group. Its Galois group over K is isomorphic to the Class group of K. [seen ⇓]

(c) Prove that $K = \mathbf{Q}(\sqrt{-1})$ does not have an unramified quadratic extension. [5, M]

A quadratic extension L/K would be Galois with Galois group $\mathbf{Z}/2\mathbf{Z}$ and hence abelian. If it is further unramified it would be contained in the Hilbert class field of K. But because the class group of K is trivial, the Hilbert class field of K must be K itself, and so K has no non trivial unramified abelian extensions. [meth seen ⇓]

(d) Prove that the Hilbert class field of $K = \mathbf{Q}(\sqrt{-15})$ is $L = \mathbf{Q}(\sqrt{-3}, \sqrt{5})$. You may use that $\frac{2}{\pi}\sqrt{15} < 3$. [9, M]

We first claim that $\mathbf{Q}(\sqrt{-3}, \sqrt{5})$ is an unramified extension of $\mathbf{Q}(\sqrt{-15})$. We can write $L = K(\sqrt{5}) = K(\frac{1+\sqrt{5}}{2})$ and the minimal polynomial of $\frac{1+\sqrt{5}}{2}$ is $x^2 - x - 1$ which is separable mod p for $p \neq 5$. Hence any prime of $\mathcal{O}_K$ except possibly for $\mathfrak{p}_5 = (5, \sqrt{-15})$ is unramified. But we can also write $L = K(\sqrt{-3}) = K(\frac{1+\sqrt{-3}}{2})$ and the minimal polynomial of $\frac{1+\sqrt{-3}}{2}$ is $x^2 - x + 1$ which is separable mod p for $p \neq 3$. Hence any prime of $\mathcal{O}_K$ except possibly for $\mathfrak{p}_3 = (3, \sqrt{-15})$ is unramified. Combined we conclude that no prime ramifies. [meth seen ⇓]

Now to prove that L is the Hilbert class field, it suffices to compute $\mathrm{Cl}(\mathcal{O}_{-15})$ and see that it has order 2. The Minkowski bound is $C_K = \frac{2}{\pi}\sqrt{15} < 3$. Since $-15 \equiv 1 \pmod 8$ we have $(2) = \mathfrak{p}_2\overline{\mathfrak{p}}_2$ splits. But we note that $N(\frac{1+\sqrt{-15}}{2}) = 4$ while $\frac{1+\sqrt{-15}}{2}$ is not a multiple of 2. It follows that $(\frac{1+\sqrt{-15}}{2}) = \mathfrak{p}_2^2$ or $\overline{\mathfrak{p}}_2^2$. Hence $\mathrm{Cl}(\mathcal{O}_{-15}) = \{1, [\mathfrak{p}_2]\}$ has order 2.

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

MATH60042 Algebraic Number Theory

Question	Marker's comment
1	This question overall went very well. nbsp;In part b some of you tried to show the polynomial you found is irreducible, when this is totally unnecessary! nbsp;Part d was the hardest, where you have to realize that you can't use a quadratic algebraic integer because x^2-2x+1 is reducible.
2	Parts a and b went very well. nbsp;For part c many of you had the good ideal to compute the norm of (sqrt(d)), but some of you incorrectly stated that a nonzero ideal is prime if and only if its norm is prime (it could also be a prime power.) nbsp;Part d was the hardest but I was happy to see many correct solutions.
3	For part a, many of you just gave the Minkowski constant without actually stating the theorem. nbsp;Part b went very well. nbsp;Part c was the hardest. nbsp;Many of you failed to try to justify why 1, [p_2], [p_3], [p_7] were the only elements of the class group, rather than just generators.
4	Part a went well. nbsp;In part b many of you forgot to mention units in your solution. nbsp;In part c some of you forgot that O_{-11} is not Z[\sqrt{-11}] and thus missed one of the solutions.

MATH70042 Algebraic Number Theory

Question	Marker's comment
5	Questions an and b are just about definitions and overall went fairly well. nbsp;Question c turned out to be harder than I had intended. nbsp;Question d was also hard, but I was happy to see that many of you reduced it to proving that K in L is unramified, which is probably the tricky part.