Coláiste na Tríonóide, Baile Átha Cliath
Trinity College Dublin
Ollscoil Átha Cliath | The University of Dublin

Faculty of Science, Technology, Engineering and Mathematics

School of Mathematics

JS/SS Maths/TP/TJH **Michaelmas 2024-25**

MAU34109 Algebraic number theory

DATE PLACE TIME

Dr. Nicolas Mascot

Instructions to candidates:

This exam consists of **two** independent exercises. You must attempt **both** exercises.
In each exercise, in order to solve any question, you are allowed to assume the result of any **previous** question.
The use of non-programmable calculators and of the standard booklet of formulae and tables is allowed.

You may not start this examination until you are instructed to do so by the Invigilator.

Question 1 *A quadratic field (60 pts)*

Let $K = \mathbb{Q}(\sqrt{10})$.

1. (2 pts) What are the degree and the signature of K?

2. (3 pts) What are the ring of integers and the discriminant of K?

3. (10 pts) Find explicit generators for the unit group $\mathbb{Z}_K^\times$ of K. In particular, show that $u = 3 + \sqrt{10}$ is a fundamental unit.

4. Suppose $\mathfrak{a}$ is an ideal of $\mathbb{Z}_K$ of norm $N(\mathfrak{a}) = 2$. We want to show that $\mathfrak{a}$ cannot be principal. In this question, we thus suppose by contradiction that $\mathfrak{a}$ is principal, and we let $\alpha = x + y\sqrt{10} \in \mathbb{Z}_K$ be a generator of $\mathfrak{a}$.

   (a) (3 pts) Explain why we may assume without loss of generality that $\frac{1}{3} < |\alpha| < 3$. In what follows, we make this assumption.

   (b) (4 pts) What are the possible values of $(x+y\sqrt{10})(x-y\sqrt{10})$, where $\alpha = x+y\sqrt{10}$ still?

   (c) (4 pts) Conclude that $\mathfrak{a}$ cannot be principal.

5. (6 pts) Determine the decomposition of the prime numbers 2 and 3 in K.

6. (10 pts) Prove that the class group of K is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

7. (8 pts) For each of the primes $\mathfrak{p}$ above 2 and 3 found in question 5., determine the order $n_\mathfrak{p}$ of $[\mathfrak{p}]$ in the class group of K, and find an explicit generator (in terms of $\sqrt{10}$) of $\mathfrak{p}^{n_\mathfrak{p}}$.

8. (10 pts) Let $n \geqslant 0$ be an integer. Determine the number of pairs of integers $(x, y) \in \mathbb{Z}^2$ that satisfy $x^2 - 10y^2 = 2^n$ in terms of n.

Solution 1

1. As $10 > 0$ is not a square in $\mathbb{Q}$ (or because $x^2 - 10$ is Eisenstein at 2 and 5), $[K : \mathbb{Q}] = 2$, signature $(2, 0)$.

2. As $10 \in \mathbb{Z}$ is squarefree and not $\equiv 1 \bmod 4$, we have $\mathbb{Z}_K = \mathbb{Z}[\sqrt{10}]$, whence $\operatorname{disc} K = \operatorname{disc}(x^2 - 10) = 40$.

3. Since K may be embedded into $\mathbb{R}$, its only roots of 1 are ± 1. Furthermore, by Dirichlet, $\mathbb{Z}_K^\times$ has rank $2+0-1 = 1$. So $\mathbb{Z}_K^\times$ is spanned by -1 and a fundamental unit u. In order to find u, we look for elements of $\mathbb{Z}_K$ of norm ± 1. The generic element of $\mathbb{Z}_K$ is $x + y\sqrt{10}$ with $x, y \in \mathbb{Z}$, and its norm is $x^2 - 10y^2$. By a theorem seen in class, fundamental units thus correspond to the simplest nontrivial solutions of $x^2 - 10y^2 = \pm 1$. Already for $y = 1$, we find the solution $x = 3$, so we can take $u = 3 + \sqrt{10}$.

4. (Process seen in class)

   (a) We have $\mathfrak{a} = (\alpha) = (v\alpha)$ for any $v \in \mathbb{Z}_K^\times$. Multiplying α by $v = u^n$ for a suitable $n \in \mathbb{Z}$, we may thus assume that

   $$\frac{1}{\sqrt{u}} \leqslant |\alpha| \leqslant \sqrt{u}.$$

   But plainly $\sqrt{u} = \sqrt{3 + \sqrt{10}} < \sqrt{3+4} < \sqrt{9} = 3$.

   (b) Since we assume $\mathfrak{a} = (\alpha)$, we know that $|(x + y\sqrt{10})(x - y\sqrt{10})| = |N_{\mathbb{Q}}^K(\alpha)| = N(\mathfrak{a}) = 2$, whence $(x + y\alpha)(x - y\alpha) = \pm 2$.

   (c) We infer that $|x - y\sqrt{10}| = 2/|x + y\sqrt{10}| < 6$, whence $|2y\sqrt{10}| = |(x + y\sqrt{10}) - (x - y\sqrt{10})| < 3 + 6 = 9$. Thus $|y| < 9/2\sqrt{10} < 3/2$. However, the equation $x^2 - 10y^2 = \pm 2$ has no integer solutions with $|y| < 3/2$, contradiction.

5. Since $\mathbb{Z}_K = \mathbb{Z}[\sqrt{10}]$, we can obtain the decomposition of any prime number p in K by factoring mod p the minimal polynomial $x^2 - 10$ of $\sqrt{10}$.

   For $p = 2$, we find $x^2 - 10 \equiv x^2$, whence

   $$2\mathbb{Z}_K = \mathfrak{p}_2^2, \quad \mathfrak{p}_2 = (2, \sqrt{10}).$$

   For $p = 3$, we have $x^2 - 10 \equiv (x-1)(x+1)$, so

   $$3\mathbb{Z}_K = \mathfrak{p}_3\mathfrak{q}_3, \quad \mathfrak{p}_3 = (3, \sqrt{10} - 1), \mathfrak{q}_3 = (3, \sqrt{10} + 1).$$

6. The Minkowski bound is
$$M_K = \frac{2!}{2^2}\left(\frac{4}{\pi}\right)^0 \sqrt{4}0 = \sqrt{10} < 5,$$
so $\operatorname{Cl} K$ is generated by the classes of the primes above 2 and 3. We determined these primes in the previous question; more specifically, we have already found that $[\mathfrak{p}_2]^2 = [\mathfrak{p}_3][\mathfrak{q}_3] = 1$.

   Next, we spot that $N_{\mathbb{Q}}^K(2+\sqrt{10}) = 2^2 - 10 = -6$, so $(2+\sqrt{10})$ is an ideal of norm 6, which must be either $\mathfrak{p}_2\mathfrak{p}_3$ or $\mathfrak{p}_2\mathfrak{q}_3$. This shows that $\operatorname{Cl} K$ is generated by $[\mathfrak{p}_2]$, and is thus a quotient of $\mathbb{Z}/2\mathbb{Z}$.

   Finally, question 5. tells us that $\mathfrak{p}_2$ cannot be principal, so we conclude that $\operatorname{Cl} K \simeq \mathbb{Z}/2\mathbb{Z}$.

7. The relations found in the previous question show that $[\mathfrak{p}_2] = [\mathfrak{p}_3] = [\mathfrak{q}_3]$; thus all have order 2 in $\operatorname{Cl} K$.

   We already know that $\mathfrak{p}_2^2 = (2)$.

   Next, we observe that $(2+\sqrt{10}) = \mathfrak{p}_2\mathfrak{p}_3$ as $\mathfrak{p}_3 \ni 2+\sqrt{10}$, whence
$$\mathfrak{p}_3^2 = \mathfrak{p}_2^2\mathfrak{p}_3^2/\mathfrak{p}_2^2 = (2+\sqrt{10})^2/(2) = \left(\frac{(2+\sqrt{10})^2}{2}\right) = (7+2\sqrt{10}).$$
   Finally, we have
$$\mathfrak{q}_3^2 = (\mathfrak{p}_3\mathfrak{q}_3)^2/\mathfrak{p}_3^2 = \left(\frac{3^2}{7+2\sqrt{10}}\right) = (7-2\sqrt{10}).$$
   Alternatively, we can spot that $1 \pm \sqrt{10}$ have norm -3^2.

8. Suppose $(x,y) \in \mathbb{Z}^2$ satisfies $x^2 - 10y^2 = 2^n$, and let $\beta = x + y\sqrt{10}$. Then $\beta \in \mathbb{Z}_K$ has norm 2^n, so (β) is a principal ideal of norm 2^n, which can only be $\mathfrak{p}_2^n$. If n is odd, this contradicts the fact that $[\mathfrak{p}_2]$ has order 2, so there are no solutions. On the contrary, if n is even, then $\mathfrak{p}_2^n$ is indeed principal. Let $\gamma \in \mathbb{Z}_K$ generate it, then $N_Q^K(\gamma) = \pm 2^n$. As u has norm -1, replacing γ with $u\gamma$, we may assume that γ has norm 2^n, whence a solution to $x^2 - 10y^2 = 2^n$. (Or we could simply take $x = 2^{n/2}$.) But then $u^{2k}\gamma$ also has norm 2^n for all $k \in \mathbb{Z}$, so there are infinitely many solutions to $x^2 - 10y^2 = 2^n$.

EXAM CONTINUES OVERLEAF

Question 2 *Controlled ramification (40 pts)*

In this exercise, by "quadratic field", we mean a field extension of $\mathbb{Q}$ of degree 2.

Let $D = \{d \in \mathbb{Z} \mid d \text{ is squarefree}, d \neq 0, d \neq 1\} \subset \mathbb{Z}$. We admit without proof the fact that the map $d \mapsto \mathbb{Q}(\sqrt{d})$ is a bijection between D and isomorphism classes of quadratic fields.

1. (4 pts) Let $d \in D$, and let $K = \mathbb{Q}(\sqrt{d})$. State the formula expressing $\operatorname{disc} K$ in terms of d. (You may have to distinguish between several cases.)

2. Find a quadratic field that is ramified at ℓ and unramified at all the other primes (you just need to find one, not all of them), when

   (a) (3 pts) $\ell = 17$,

   (b) (3 pts) $\ell = 19$.

   Hint: Remember that d is allowed to be negative.

3. (10 pts) Let $\ell \neq 2$ be an odd prime. Prove that there exists a quadratic field K_ℓ which is ramified at ℓ and unramified at all the other primes (so, in particular, K_ℓ must be unramified at 2), and that this field is unique up to isomorphism. Express K_ℓ in terms of ℓ.

4. (10 pts) Up to isomorphism, how many quadratic fields are ramified at 2, but unramified at all the other primes? List them.

5. (10 pts) We define the *absolute discriminant* of a number field K as the absolute value $|\operatorname{disc} K|$ of its discriminant. What is the smallest possible absolute discriminant of a quadratic field? How many quadratic fields (up to isomorphism) reach this minimum?

Solution 2

1. As seen in class, since d is squarefree, the ring of integers of K is $\mathbb{Z}[\sqrt{d}]$ if $d \not\equiv 1 \bmod 4$, and is $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ if $d \equiv 1 \bmod 4$. In the former case, $\operatorname{disc} K = 4d$; in the latter, $\operatorname{disc} K = d$.

2. Recall that the primes that ramify are exactly those that divide the discriminant.

   (a) For $\ell = 17$, we can try $d = 17$. As this is $1 \bmod 4$, the discriminant of $\mathbb{Q}(\sqrt{17})$ is 17, so only 17 ramifies, as desired.

   (b) This doesn't work for $\ell = 19$; indeed, the discriminant of $\mathbb{Q}(\sqrt{19})$ is $4 \cdot 19$ as $19 \not\equiv 1 \bmod 4$, so 2 also ramifies.

   However, following the hint, we can try $d = -19$ instead, and indeed $\mathbb{Q}(\sqrt{-19})$ has discriminant -19, so only 19 ramifies.

3. We know that $K \simeq \mathbb{Q}(\sqrt{d})$ for some $d \in D$. If $d \not\equiv 1 \bmod 4$, then $\operatorname{disc} K = 4d$, so 2 ramifies, and we do not want that; therefore we must have $d \equiv 1 \bmod 4$. Then $\operatorname{disc} K = d$, so we need $|d|$ to be a power of ℓ. As d must also be squarefree, we must have $d = \pm\ell$. Only one of these is $\equiv 1 \bmod 4$, so K exists and is unique up to isomorphism, and is given by

$$K = \mathbb{Q}(\sqrt{\pm\ell})$$

   where the sign is chosen so that $\pm\ell \equiv 1 \bmod 4$.

4. Let $d \in D$, and let again $K = \mathbb{Q}(\sqrt{d})$. Then $\operatorname{disc} K = d$ or $4d$, so we don't want d to be divisible by any odd prime, so $d \in \{\pm 1, \pm 2\}$. As d cannot be 1, we are left with $d \in \{-1, 2, -2\}$, which yield discriminants -4, 8, and -8 respectively. These all admit only 2 as a prime factor, so we conclude that there are exactly 3 such quadratic fields, namely $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{2})$, and $\mathbb{Q}(\sqrt{-2})$.

5. In the previous question, we have already spotted that $\mathbb{Q}(\sqrt{-1})$ has absolute discriminant 4, which is already quite low. Let us see if we can do better.

   Let $K = \mathbb{Q}(\sqrt{d})$ for some $d \in D$. Its absolute discriminant is either $|d|$ or $|4d|$, so it is at least $|d|$. Thus, if we want to beat $\mathbb{Q}(\sqrt{-1})$, our only hope is to restrict ourselves to $|d| < 4$. Bearing in mind that d is not allowed to be 0 or 1, we see that our list of candidates is $d = -3, -2, -1, 2, 3$. We have already examined most of those in the previous question, so we easily determine that the corresponding absolute discriminants are $3, 8, 4, 8, 6$. This shows that the lowest possible absolute discriminant is actually 3, and is achieved for $K = \mathbb{Q}(\sqrt{-3})$ only.

END