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 **Semester 1, 2022**

MAU34109 Algebraic number theory

Not today **Not here** **Not right now**

Dr. Nicolas Mascot

Instructions to candidates:

This is NOT a real exam! These exercises are just here to help you prepare for the real exam. The use of non-programmable calculators is therefore allowed, the lecturer does not care.

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

Question 1 *Quadratic fields with little ramification*

1. Let $p \in \mathbb{N}$ be an odd prime. Find all quadratic number fields (real and imaginary) which are ramified at p and only at p.

2. Same question for $p = 2$.

Question 2 *Your turn to mark!*

Find all that is wrong in the following paragraph:

Let K be an imaginary quadratic field. By Dirichlet's theorem, the rank of $\mathbb{Z}_K^\times$ is zero, so the only units in K are ± 1. But let us consider a prime $p \in \mathbb{N}$ which ramifies in K, say $p\mathbb{Z}_K = \mathfrak{p}^2$. Write $\mathfrak{p} = (\gamma)$; then we have $(p) = \mathfrak{p}^2 = (\gamma)^2 = (\gamma^2)$, so we get that $u = \gamma^2/p$ is a unit in K, which contradicts Dirichlet's theorem.

Question 3 *A quartic field and some big numbers*

Let $f(x) = x^4 + 3x^3 - 18x^2 - 24x + 129$, which is an irreducible polynomial over $\mathbb{Q}$ (why?), and let $K = \mathbb{Q}(\alpha)$, where α is a root of $f(x)$.

1. If I told you that $\operatorname{disc} f = 930,069$, why would not that be very useful to you? What information can you get from that nonetheless?

2. I now tell you that the roots of f are approximately $-4.1 \pm 0.1i$ and $2.6 \pm 1.0i$. What is the signature of K? Can you compute the trace of α from these approximate values? Why is the result obvious?

3. If I now tell you that $\operatorname{disc} f$ factors as $3^3 \cdot 7^2 \cdot 19 \cdot 37$, what can you say about the ring of integers of K and the primes that ramify in K?

4. In principle (don't actually do it), how could you test whether $\beta = \frac{\alpha^3 - 2\alpha^2 - \alpha + 2}{7}$ is an algebraic integer?

5. If I now tell you that the characteristic polynomial of β is $\chi(\beta) = x^4 + 28x^3 + 207x^2 + 154x + 247$, whose discriminant is $\operatorname{disc} \chi(\beta) = 25,364,993,616$, which conclusions can you draw from that?

6. Given that $\operatorname{disc} \chi(\beta)$ factors as $2^4 \cdot 3^3 \cdot 17^4 \cdot 19 \cdot 37$, what is the index of the order $\mathbb{Z}[\beta]$? What consequence does this have on the expression of a $\mathbb{Z}$-basis of $\mathbb{Z}_K$ in terms of β?

7. Let $\gamma = \frac{\beta^2 - 3\beta - 3}{34}$, and let $\delta = \frac{\beta^3 - 12\beta - 9}{34}$, whose respective characteristic polynomials are $\chi(\gamma) = x^4 - 13x^3 + 42x^2 + 8x + 1$ and $\chi(\delta) = x^4 + 139x^3 + 5163x^2 + 973$. Prove that $\{1, \beta, \gamma, \delta\}$ is a $\mathbb{Z}$-basis of $\mathbb{Z}_K$.

8. Compute explicitly the decomposition of 2, 3, and 7 in K.

9. Determine the rank of $\mathbb{Z}_K^\times$, and bound the size of W_K.

10. Find a non-trivial (that is to say $u \neq \pm 1$) unit u in K.

11. How can you test whether $u \in W_K$?

Question 4 *A cubic field*

Let $f(x) = x^3 - 4x^2 + 2x - 2$, which is an irreducible polynomial over $\mathbb{Q}$ (why?), and let $K = \mathbb{Q}(\alpha)$, where α is a root of f.

1. Given that $\operatorname{disc} f = -300$, what can you say about the ring of integers of K and the primes that ramify in K? What if, on the top of that, you notice that $f(x + 3) = x^3 + 5x^2 + 5x - 5$?

2. Prove that $\mathbb{Z}_K$ is a PID.

3. Find a generator for each of the primes above 2, 3 and 5.

4. Use the results of the previous question to discover that $u = 2\alpha^2 - \alpha + 1$ is a unit.

5. We use the unique embedding of K into $\mathbb{R}$ to view K as a subfield of $\mathbb{R}$ from now on. Prove that there exists a unit $\varepsilon \in \mathbb{Z}_K^\times$ such that $\mathbb{Z}_K^\times = \{\pm\varepsilon^n, n \in \mathbb{Z}\}$ and $\varepsilon > 1$.

6. By the technique of exercise 3 from exercise sheet number 5, it can be proved that $\varepsilon \geqslant 4.1$. Given that $u \approx 23.3$, prove that u is a fundamental unit. What is the regulator of K?

   Hint : Reduce u modulo the primes above 3 to prove that u is not a square in $\mathbb{Z}_K$.

Question 5 *An indefinite quadratic form*

In this exercise, we let $K = \mathbb{Q}(\alpha)$, where $\alpha = \sqrt{195}$. The following facts may be useful:

- 195 factors as $3 \cdot 5 \cdot 13$,
- The squares mod the first few primes are as follows:

p	Squares mod p
2	$0, 1$
3	$0, 1$
5	$0, 1, 4$
7	$0, 1, 2, 4$
11	$0, 1, 3, 4, 5, 9$
13	$0, 1, 3, 4, 9, 10, 12$
17	$0, 1, 2, 4, 8, 9, 13, 15, 16.$

1. What are the ring of integers and the discriminant of K?
2. Find explicit generators for the unit group $\mathbb{Z}_K^\times$ of K.
3. Compute the decomposition of the primes $p \leqslant 13$ in K.
4. Factor the ideals $\alpha\mathbb{Z}_K$ and $(15 + \alpha)\mathbb{Z}_K$ into prime ideals.
5. Prove that $\mathbb{Z}_K$ has no element of norm N for any $N \in \{\pm 2, \pm 3, \pm 5\}$.

   Hint: View K as a subfield of $\mathbb{R}$, and multiply an hypothetical such element by a unit so as to make it neither too small nor too big.

6. Deduce that $\mathrm{Cl}(K)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

7. For each of the following values of m, determine the number of ideals of norm m and whether the equation $x^2 - 195y^2 = m$ has solutions with $x, y \in \mathbb{Z}$, and if it does, say how many solutions it has, and give an explicit such solution:

   (a) $m = 7^{34109}$,

   (b) $m = 10$,

   (c) $m = 195$,

   (d) $m = 2 \cdot 3 \cdot 199961$, noting that $N_{\mathbb{Q}}^{K}(1000 + \alpha) = 5 \cdot 199961$ where 199961 is prime.

   Hint: Think in terms of principal ideals.

Question 6 *Another cubic field*

Let $P(x) = x^3 + 6x + 6 \in \mathbb{Z}[x]$, and let $K = \mathbb{Q}(\alpha)$, where α is a root of $P(x)$.
You may find the following table useful:

n	-5	-4	-3	-2	-1	0	1	2	3	4	5
$P(n)$	-149	-82	-39	-14	-1	6	13	26	51	94	161

1. Compute $[K : \mathbb{Q}]$, $\mathbb{Z}_K$, and $\operatorname{disc} K$.

2. Prove that $\mathrm{Cl}(K)$ is generated by $[\mathfrak{p}_2]$, where $\mathfrak{p}_2$ is the prime of K above 2.

3. Find a non-trivial unit u in K, and prove that it generates the group $\mathbb{Z}_K^{\times}/\mathbb{Z}_K^{\times 3}$ of units modulo cubes of units.

   Hint: Reduce u modulo a prime of K to prove that it is not a cube.

4. Prove that if $\mathfrak{p}_2$ were principal, there would exist a unit v such that $2v$ is a cube in K.

5. Determine $\mathrm{Cl}(K)$.

END