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 $p = 2$.

Solution 1

1. Let K be a quadratic field. We know that $K = \mathbb{Q}(\sqrt{d})$ for some squarefree $d \in \mathbb{Z}$ which is neither 0 nor 1. Then if $d \not\equiv 1 \pmod 4$, we have $\operatorname{disc} K = 4d$, whereas $\operatorname{disc} K = d$ if $d \equiv 1 \pmod 4$. Besides, the primes that ramify in K are exactly the ones that divide $\operatorname{disc} K$, so for K to be ramified at p only, we need $d = \pm p$ (since d is squarefree) and $d \equiv 1 \pmod 4$. As a result, there is only one such field, namely $\mathbb{Q}(\sqrt{p})$ if $p \equiv 1 \pmod 4$, and $\mathbb{Q}(\sqrt{-p})$ if $p \equiv 3 \pmod 4$.
2. With the same notation, we see that d must be -1, 2 or -2 (since d must be squarefree and different from 1), and conversely all 3 of $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$ work. Besides, these are pairwise non-isomorphic, since (for instance) they have distinct discriminants, namely -4, 8 and -8.

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.

Solution 2

The biggest error is that $\mathfrak{p}$ has no reason to be principal. Besides, u could very well be ± 1, so there is no contradiction. Finally, the fact that the rank of $\mathbb{Z}_K^\times$ is zero implies that

$\mathbb{Z}_K^\times$ is reduced to W_K, but W_K itself is not necessarily reduced to $\{\pm 1\}$ (more precisely, we have $W_K = \{\pm 1, \pm\sqrt{-1}\}$ if $K \simeq \mathbb{Q}(\sqrt{-1})$, $W_K = \{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\}$ if $K \simeq \mathbb{Q}(\sqrt{-3})$, and $W_K = \{\pm 1\}$ else.

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 $u \in W_K$?

Solution 3

1. The primary use of the discriminant is the determination of the ring of integers and of the ramification of the primes. However, this is done in terms of the factorisation of the discriminant, and since we'd rather not factor 930069 by hand, there is not much we can do. There is still something though: since we are dealing with a field of degree 4, the possible signatures are $(r_1, r_2) = (4, 0)$, $(2, 1)$ and $(0, 2)$, and the fact that $\operatorname{disc} f > 0$ and that $\operatorname{disc} K$ differs from it by a square means that $\operatorname{disc} K > 0$, so r_2 is even. As a result, our field K is either totally real or totally imaginary.

2. The non-realness of the roots means that K is totally imaginary, so its signature is in fact $(0, 2)$. The roots of f are the images of α under the embeddings of K into $\mathbb{C}$, so $\operatorname{Tr}_{\mathbb{Q}}^K(\alpha)$ is the sum of these roots, which is approximately -3. But α is an algebraic integer, so its trace is an integer and so $\operatorname{Tr}_{\mathbb{Q}}^K(\alpha) = -3$ exactly. However, we already knew that: the trace of an algebraic number is minus the coefficient of x^{n-1} in its characteristic polynomial (same rule as for matrices). As f is irreducible, it is the characteristic polynomial of α, and so $\operatorname{Tr}_{\mathbb{Q}}^K(\alpha) = -3$.

3. We immediately see that $\mathbb{Z}[\alpha]$ is maximal at every prime except possibly at 3 and 7, and that its index is at most $3 \cdot 7$. Even if 3 did divide the index, $\operatorname{disc} K$ would still be divisible by 3 because 3 shows with odd multiplicity in $\operatorname{disc} f$, so 3 is definitely ramified in K, and so are 19 and 37. The factor 7^2 in $\operatorname{disc} f$ could either come from $\operatorname{disc} K$, in which case 7 ramifies and $\mathbb{Z}[\alpha]$ is maximal at 7, or from the index of $\mathbb{Z}[\alpha]$, in which case 7 does not ramify and $\mathbb{Z}[\alpha]$ is not maximal at 7. The other primes are unramified in K.

   One last thing: if you pay attention enough (and you should !), you'll notice that f is Eisenstein at 3 (and hence irreducible as claimed). As a result, $\mathbb{Z}[\alpha]$ is maximal at 3,

and 3 is totally ramified in K. Thus either $\mathbb{Z}[\alpha]$ has index 7 and 7 does not ramify, or $\mathbb{Z}[\alpha] = \mathbb{Z}_K$ and 7 does ramify. In the former case, there would exists elements of $\mathbb{Z}_K$ which, when written as polynomials in α, would have a non-trivial denominator, which would be powers of 7 only.

4. I would compute its characteristic polynomial: β is an algebraic integer if and only if this polynomial lies in $\mathbb{Z}[x]$. To do so, I could for example use the formula

$$\chi(\beta) = \prod_{\sigma\colon K\hookrightarrow\mathbb{C}} \big(x - \sigma(\beta)\big) = \prod_{\substack{z\in\mathbb{C}\\ f(z)=0}} \left(x - \frac{z^3 - 2z^2 - z + 2}{7}\right)$$

$$= \operatorname{Res}_y \left(f(y), x - \frac{y^3 - 2y^2 - y + 2}{7}\right).$$

5. Lots of conclusions. First, since $\chi(\beta)$ lies in $\mathbb{Z}[x]$, we see that β is an algebraic integer, so that $\mathbb{Z}_K$ is strictly larger than $\mathbb{Z}[\alpha]$. In view of question 3, this means that $\mathbb{Z}[\alpha]$ has index 7, that 7 does not ramify in K, and that $\operatorname{disc} K = 3^3 \cdot 19 \cdot 37$.

   Besides, $\mathbb{Z}[\alpha, \beta]$ is an order which is strictly larger than $\mathbb{Z}[\alpha]$, its index is strictly smaller (by a factor which is a power of 7 to be precise, since the denominator of β w.r.t. $\mathbb{Z}[\alpha]$ is 7), and since the index of $\mathbb{Z}[\alpha]$ is 7 which is prime, we must have $\mathbb{Z}_K = \mathbb{Z}[\alpha, \beta]$.

   Finally, since $\operatorname{disc} \chi(\beta) \neq 0$, $\chi(\beta)$ is squarefree. It is thus the minimal polynomial of β, so β has degree 4 and is thus another primitive element for K. Since it is also an algebraic integer, $\mathbb{Z}[\beta]$ is an order in K.

6. The formula

$$\operatorname{disc} \mathcal{O} = [\mathbb{Z}_K : \mathcal{O}]^2 \operatorname{disc} K$$

   shows that the index of $\mathbb{Z}[\beta]$ is $2^2 \cdot 17^2$. A consequence of this is that if we were to elements of $\mathbb{Z}_K$ as polynomials in β, we would get non-trivial denominators, which would be made up of powers of 2 and 17.

7. As β is a primitive element for K, the elements 1, β, β^2 and β^3 form a $\mathbb{Q}$-basis of K. Since the elements 1, β, γ, δ are in echelon form with respect to this basis, they also form a $\mathbb{Q}$-basis of K. Let Λ be the lattice they span.

The fact that $\chi(\gamma)$ and $\chi(\delta)$ lie in $\mathbb{Z}[x]$ shows that γ and δ are algebraic integers, so $\Lambda \subseteq \mathbb{Z}_K$. Besides, it is clear that $\Lambda \supsetneq \mathbb{Z}[\beta]$.

The change of basis matrix between the two aforementioned bases of K is

$$\begin{pmatrix} 1 & 0 & \frac{-3}{34} & \frac{-9}{34} \\ 0 & 1 & \frac{-3}{34} & \frac{-12}{34} \\ 0 & 0 & \frac{1}{34} & 0 \\ 0 & 0 & 0 & \frac{1}{34} \end{pmatrix}$$

whose determinant is clearly $1/34^2$. As these bases are $\mathbb{Z}$-bases of $\mathbb{Z}[\beta]$ and of Λ, this means that $[\Lambda : \mathbb{Z}[\beta]] = 34^2 = 2^2 \cdot 17^2 = [\mathbb{Z}_K : \mathbb{Z}[\beta]]$. The containment $\Lambda \subseteq \mathbb{Z}_K$ and the equality of indices then forces $\Lambda = \mathbb{Z}_K$.

Note that we get for free the fact that Λ is stable under multiplication, which was by no means obvious.

8. Since $\mathbb{Z}[\alpha]$ is maximal at 2, we may compute the decomposition of 2 by factoring f mod 2. Clearly, neither 0 nor 1 is a root of $f \bmod 2$, so f is either irreducible or the product of 2 irreducible factors of degree 2. The only polynomials of degree 2 over $\mathbb{F}_2$ are x^2, x^2+1, x^2+x and x^2+x+1, and clearly only the last one is irreducible. Therefore, if $f \bmod 2$ were reducible, it would be $(x^2+x+1)^2$, but this is impossible. There are two ways to see why: we can use the fact that we are in characteristic 2 to compute that $(x^2+x+1)^2 = x^{2^2} + x^2 + 1^2 \not\equiv f \bmod 2$, or we can say that if f were not squarefree mod 2, then its discriminant would be 0 mod 2, which we know is not the case. Either way, we deduce that f remains irreducible mod 2, so that 2 is inert in K. In symbols, $2\mathbb{Z}_K = \mathfrak{p}_2$ is a prime of norm 2^4.

We have already seen that 3 is totally ramified in K. To be more precise, as $\mathbb{Z}[\alpha]$ is maximal at 3 it is legitimate to factor $f \bmod 3$; we find $f \equiv x^4 \bmod 3$, whence $3\mathbb{Z}_K = \mathfrak{p}_3^4$, where $\mathfrak{p}_3 = (3, \alpha)$ is a prime of norm 3^1.

Finally, we may **not** determine the decomposition of 7 by factoring $f \bmod 7$, because the order $\mathbb{Z}[\alpha]$ is not maximal at 7. However, since $7^2 \nmid \operatorname{disc} \chi(\beta)$, the order $\mathbb{Z}[\beta]$ is maximal at 7, so we are saved. We have $\chi(\beta) \equiv x^4 - 3x^2 + 2 \equiv (x^2-1)(x^2-2) \equiv$

$(x-1)(x+1)(x-3)(x+3) \bmod 7$, so

$$7\mathbb{Z}_K = (7, \beta-1)(7, \beta+1)(7, \beta-3)(7, \beta+3)$$

is totally split.

9. Since the signature of K is $(0, 2)$, the rank of $\mathbb{Z}_K^\times$ is $0 + 2 - 1 = 1$ by Dirichlet.

   Suppose we have an n-th root of 1, say ζ_n, in K for some $n \in \mathbb{N}$, and let $p \mid n$ be a prime. Then $\zeta_n^{n/p}$ is a primitive p-th root of 1, so K contains a copy of the p-th cyclotomic field, whose degree is $p-1$, and which is ramified at p except if $p = 2$. Therefore the degree of K would be a multiple of $(p-1)$ and, p would ramify in K if $p \neq 2$. This excludes all the possibilities, except $p = 2$ or 3, so $n = 2^a 3^b$ for some integers a and b. But K also contains $\mathbb{Q}(\zeta_n)$, which has degree $\varphi(n) = \varphi(2^a 3^b) = \varphi(2^a)\varphi(3^b)$ (by multiplicativity of φ), and which must thus divide $[K : \mathbb{Q}] = 4$. Using the formulas $\varphi(2^a) = 2^{a-1}$, $\varphi(3^b) = 2 \cdot 3^{b-1}$ that are valid for $a, b > 0$, we see easily that the only possibilities for n are 1, 2, 3, and 6. Since W_K is cyclic and contains ± 1, we conclude that $\#W_K = 2$ or 6.

   Remark: In fact, it can be proved that in fact $\#W_K = 6$, but this is difficult.

10. We spot that γ is a unit, since $\gamma \in \mathbb{Z}_K$ (because $\chi(\gamma) \in \mathbb{Z}[x]$) and since the constant term of $\chi(\gamma)$ is 1 (and this constant term is the norm up to sign).

11. By the first question, $\gamma \in W_K$ implies $\gamma^6 = 1$. More economically, since clearly $\gamma \neq \pm 1$, we could simply rule out that it is a root of 1 of order 3 or 6 by checking that γ is not a root of the cyclotomic polynomials $\Phi_3(x) = x^2 + x + 1$ and $\Phi_6(x) = x^2 - x + 1$.

    Remark: One finds that $\gamma \notin W_K$. In fact, γ turns out to be a fundamental unit for K, but proving this requires a computer.

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 $\mathbb{Z}_K$.

Solution 4

1. We have $\operatorname{disc} f = -300 = -2^2 \cdot 3 \cdot 5^2$, so the order $\mathbb{Z}[\alpha]$ is p-maximal at every prime $p \neq 2, 5$. Besides, f is Eisenstein at 2, so $\mathbb{Z}[\alpha]$ is actually also maximal at $p = 2$, and 2 is totally ramified in K; incidentally this also proves that f is irreducible as claimed. We thus have only two possibilities: either $\mathbb{Z}[\alpha]$ is also maximal at $p = 5$, in which case $\mathbb{Z}_K = \mathbb{Z}[\alpha]$, so that $\operatorname{disc} K = -2^2 \cdot 3 \cdot 5^2$ and so K ramifies precisely at 2, 3 and 5, or $\mathbb{Z}[\alpha]$ is not maximal at $p = 5$, in which case $\mathbb{Z}[\alpha]$ has index exactly 5 (and not a larger power of 5 since $5^4 \nmid \operatorname{disc} f$), and so $\operatorname{disc} K = -2^2 \cdot 3$ so K is ramified precisely at 2 and 3, but not at 5.

   However, the fact that $\alpha - 3$ is a root of $f(x+3)$ which is Eisenstein at 5 proves that the order $\mathbb{Z}[\alpha - 3]$ is maximal at 5 and that 5 is totally ramified in K. But clearly $\mathbb{Z}[\alpha - 3] = \mathbb{Z}[\alpha]$, so $\mathbb{Z}[\alpha]$ is in fact maximal at 5 and so $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ and K is ramified precisely at 2, 3 and 5. On the top of that, we have shown that 2 and 5 are actually *totally* ramified. We do not know yet whether 3 is totally ramified.

2. Let (r_1, r_2) be the signature of K. As $\operatorname{disc} K = -300 < 0$, we know that r_2 is odd, and so the relation $r_1 + 2r_2 = [K : \mathbb{Q}] = 3$ forces $r_1 = r_2 = 1$. As a result, the Minkowski bound for K is $M = \frac{3!}{3^3}\frac{4}{\pi}\sqrt{300} \approx 4.9$, so the class group of K is generated by the primes above 2 and 3.

   We already know that 2 is totally ramified, say $2\mathbb{Z}_K = \mathfrak{p}_2^3$, whence the relation $[\mathfrak{p}_2]^3 = 1$ in the class group. To compute the decomposition of 3, we factor f mod 3 (this is legitimate because the order $\mathbb{Z}[\alpha]$ attached to f, being maximal at every p, is in particular maximal at 3). We thus compute that

$$f \equiv x^3 - x^2 - x + 1 \bmod 3 \equiv (x-1)(x^2-1) \equiv (x-1)^2(x+1) \bmod 3,$$

   whence the decomposition $3\mathbb{Z}_K = \mathfrak{p}_3^2\mathfrak{p}_3'$, where $\mathfrak{p}_3 = (3, \alpha - 1)$ and $\mathfrak{p}_3' = (3, \alpha + 1)$. We also get the relation $[\mathfrak{p}_3]^2[\mathfrak{p}_3'] = 1$ in the class group.

   Now that we have generators, we need to find relations between these generators. For this, we look for elements of small norm : if the norm of an element only involves powers of 2 and 3, then the principal ideal generated by this element will have the same norm (up to sign), and so its factorisation will only involve $\mathfrak{p}_2$, $\mathfrak{p}_3$ and $\mathfrak{p}_3'$, whence a relation between $[\mathfrak{p}_2]$, $[\mathfrak{p}_3]$ and $[\mathfrak{p}_3']$. We have

$$N(n-\alpha) = \prod_{\sigma\colon K \hookrightarrow \mathbb{C}} \sigma(n-\alpha) = \prod_{\sigma\colon K \hookrightarrow \mathbb{C}} \big(n - \sigma(\alpha)\big) = f(n)$$

   for all $n \in \mathbb{Q}$ where the products range over the embeddings of K into $\mathbb{C}$, so we can use this formula to compute the norm of elements of the form $n - \alpha$.

   For example, we have $N(\alpha) = -f(0) = 2$, whence $(\alpha) = \mathfrak{q}_2$ where $\mathfrak{q}_2$ is some prime of inertial degree 1 above 2, which can only be $\mathfrak{p}_2$. Thus $[\mathfrak{p}_2] = 1$.

   Similarly, we have $N(1-\alpha) = f(1) = -3$, so $(1-\alpha) = \mathfrak{q}_3$ for some prime $\mathfrak{q}_3$ of degree 1 above 3. Thanks to the criterion

$$\mathfrak{p} \mid (\beta) \iff (\beta) \subseteq \mathfrak{p} \iff \beta \in \mathfrak{p}$$

   valid for all prime $\mathfrak{p}$ and element $\beta \in \mathbb{Z}_K$, we see that $(1-\alpha) = \mathfrak{p}_3$.

   Therefore $[\mathfrak{p}_3] = 1$ and so $[\mathfrak{p}_3'] = 1$, so the class group is trivial and $\mathbb{Z}_K$ is a PID.

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

   We have already proved that $\mathfrak{p}_2 = (\alpha)$ and that $\mathfrak{p}_3 = (\alpha - 1)$. Besides, we know that $(5) = \mathfrak{p}_5^3$ is totally ramified, and since $\alpha - 3$ is a root of $f(x+3) = x^3 + 5x^2 + 5x - 5$, we have $N(\alpha - 3) = 5$ whence $\mathfrak{p}_5 = (\alpha - 3)$.

   It remains to find a generator for $\mathfrak{p}_3'$. For this, we can use the relation $(3) = \mathfrak{p}_3^2\mathfrak{p}_3' = (\alpha-1)^2\mathfrak{p}_3'$ to deduce that $\mathfrak{p}_3' = (\beta)$ where $\beta = \frac{3}{(\alpha-1)^2}$. Note that we get for free that β is an algebraic integer, and that its norm is ± 3.

   There is (at least) one other easy way to find a generator for $\mathfrak{p}_3'$: we have $N(2-\alpha) = f(2) = -6$, so the ideal $(2-\alpha)$ factors as $\mathfrak{q}_2\mathfrak{q}_3$, a,d as in the previous question we see that $\mathfrak{q}_2 = \mathfrak{p}_2$ and that $\mathfrak{q}_3 = \mathfrak{p}_3'$. Thus $\mathfrak{p}_3' = (2-\alpha)/(\alpha) = (\beta')$, where $\beta' = \frac{2-\alpha}{\alpha} = \frac{2}{\alpha} - 1 = \alpha^2 - 4\alpha + 1$ in view of the relation $f(\alpha)/\alpha = 0$.

4. The key to discovering units is finding more than one generator for the same principal ideal.

   For instance, we have just seen that $\mathfrak{p}_3' = (\beta) = (\beta')$, so β'/β is a unit. Unfortunately, it turns out that

   $$\frac{\beta'}{\beta} = (\alpha^2 - 4\alpha + 1)\frac{(\alpha-1)^2}{3} = -1,$$

   so this unit is not a very interesting one...

   Let's try again : we have $(2) = \mathfrak{p}_2^3 = (\alpha)^3 = (\alpha^3)$, so $u = \alpha^3/2 = 2\alpha^2 - \alpha + 1$ is a unit.

   We could also have used the fact that $(5) = (\alpha-3)^3$ to discover the unit $v = \frac{(\alpha-3)^3}{5} = -\alpha^2 + 5\alpha - 5$.

5. According to Dirichlet's theorem, the rank of $\mathbb{Z}_K^\times$ is $r_1 + r_2 - 1 = 1$. Besides, as K can be embedded into $\mathbb{R}$, the only roots of unity it contains are ± 1, so $\mathbb{Z}_K^\times = \{\pm\varepsilon^n, n \in \mathbb{Z}\}$ for some fundamental unit ε. Possibly after replacing ε with $\pm\varepsilon^{\pm 1}$ which is also a fundamental unit, we may assume that $\varepsilon > 1$.

   Remark: Note that since $\mathbb{Z}_k^\times$ has rank 1, there must be a relation between our units u and v; indeed it turns out that $v = 1/u$.

6. We have $u = \pm\varepsilon^n$ for some $n \in \mathbb{Z}$. As $u > 1$, we must in fact have $u = \varepsilon^n$ for some $n > 0$. Besides, since $\varepsilon > 4.1$, we have $n \leqslant 2$. As a result, we either have $u = \varepsilon$ or $u = \varepsilon^2$; in the first case, u is a fundamental unit, in the second case it isn't.

   In order to prove that u is fundamental, we are going to prove that u is not a square in K. As u is a unit, its norm is ± 1, so we could conclude immediately if its norm were -1; unfortunately $N(u) = +1$, so we must find something else.

   The key is to compute the reduction of u modulo some primes $\mathfrak{p}$: if we get a non-square in the finite field $\mathbb{Z}_K/\mathfrak{p}$, this will prove that u is not a square. Now, every element of $\mathbb{F}_2$ is a square, so let us not consider $\mathfrak{p} = \mathfrak{p}_2$. Let us try $\mathfrak{p} = \mathfrak{p}_3$ instead : we have $\alpha - 1 \in \mathfrak{p}_3$, so $\alpha \equiv 1 \bmod \mathfrak{p}_3$ and so $u = 2\alpha^2 - \alpha + 1 \equiv 2 \bmod \mathfrak{p}_3$, which is not a square in $\mathbb{Z}_K/\mathfrak{p}_3$, bingo ! You may check that, on the other hand, $\mathfrak{p} = \mathfrak{p}_3'$ and $\mathfrak{p}_5$ were inconclusive.

   As a consequence, the regulator of K is $\log \varepsilon = \log u$. (This turns out to be pretty close to π, but this is purely coincidental.)

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.

Solution 5

1. Since 195 is squarefree and not 1 mod 4, we have $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ and $\operatorname{disc} K = 4 \times 195 = 2^2 \cdot 3 \cdot 5 \cdot 13$.

2. K is a real quadratic field, so we have $\mathbb{Z}_K^\times = \{\pm\varepsilon^n,\ n \in \mathbb{Z}\} = \langle -1, \varepsilon \rangle$ for some fundamental unit $\varepsilon \in \mathbb{Z}_K^\times$. Letting $\varepsilon = x + y\alpha$, we have $x, y \in \mathbb{Z}$ since $\mathbb{Z}_K = \mathbb{Z}[\alpha]$, and we may take x and y to be the smallest such that $x^2 - 195y^2 = \pm 1$. Noting that $14^2 = 195 + 1$, we deduce that we can take $\varepsilon = 14 + \alpha$.

3. The primes 2, 3, 5, and 13 divide $\operatorname{disc} K$, so they ramify. As K has degree only 2, the only possibilities are $2\mathbb{Z}_K = \mathfrak{p}_2^2$, $3\mathbb{Z}_K = \mathfrak{p}_3^2$, $5\mathbb{Z}_K = \mathfrak{p}_5^2$, $13\mathbb{Z}_K = \mathfrak{p}_{13}^2$, where $\mathfrak{p}_p$ is a prime of norm p.

   We also note that 195 is not a square mod 7 nor mod 11 thanks to the table of squares, so 7 and 11 are both inert in K.

4. We note that $N_{\mathbb{Q}}^K(x + y\alpha) = x^2 - 195y^2$ (e.g. by complex embeddings).

   In particular, α has norm -195, so $\alpha\mathbb{Z}_K$ has norm $195 = 3 \cdot 5 \cdot 13$. Since $\mathfrak{p}_p$ is the only prime above p for all $p \in \{2, 3, 5, 13\}$, we necessarily have $\alpha\mathbb{Z}_K = \mathfrak{p}_3\mathfrak{p}_5\mathfrak{p}_{13}$.

   Similarly, since $(15 + \alpha)\mathbb{Z}_K$ has norm $15^2 - 195 = 30 = 2 \cdot 3 \cdot 5$, we must have $(15 + \alpha)\mathbb{Z}_K = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5$.

5. Let us suppose by contradiction that β be such an element. Since $\mathbb{Z}_K = \mathbb{Z}[\alpha]$, we must have $\beta = x + y\alpha$ for some $x, y \in \mathbb{Z}$, such that $x^2 - 195y^2 = N$. In particular, $x - y\alpha = N/\beta$.

   We note that $N_{\mathbb{Q}}^K(-1) = +1$ and that $N_{\mathbb{Q}}^K(\varepsilon) = 14^2 - 195 = +1$, so every unit in K has norm $+1$ since $\mathbb{Z}_K^\times$ is generated by -1 and ε. Thus $u\beta$ also has norm N for all $u \in \mathbb{Z}_K^\times$, and after replacing β by $u\beta$ with a well-chosen u, we may assume that $1/\sqrt{\varepsilon} \leq \beta \leq \sqrt{\varepsilon}$, where the inequalities should be understood through the obvious embedding of K into $\mathbb{R}$.

   We then deduce that

$$|2y\alpha| = |\beta - N/\beta| \leq (|N| + 1)\sqrt{\varepsilon},$$

   whence $|y| \leq (|N| + 1)\sqrt{\varepsilon}/(2\alpha)$.

   For $|N| = 2$ or 3, this gives $|y| < 1$, whence $y = 0$ since $y \in \mathbb{Z}$; but this is absurd as we then get $x^2 = N$. For $N = \pm 5$, we could also have $y = \pm 1$, but there is still no $x \in \mathbb{Z}$ such that $x^2 - 195y^2 = N$. Therefore, such a β cannot exist.

6. The degree of K is 2 and its signature is $(2, 0)$, so the Minkowski bound is

$$M_K = \frac{2!}{2^2}(4/\pi)^0\sqrt{195} = \sqrt{195} < 16,$$

which means that $\mathrm{Cl}(K)$ is generated by the primes that we have already encountered. Actually, since 7 and 11 are inert, $\mathrm{Cl}(K)$ is generated by $[\mathfrak{p}_2]$, $[\mathfrak{p}_3]$, $[\mathfrak{p}_5]$, and $[\mathfrak{p}_{13}]$.

Next, we have the relations $[\mathfrak{p}_2]^2 = [\mathfrak{p}_3]^2 = [\mathfrak{p}_5]^2 = [\mathfrak{p}_{13}]^2 = 1$ from question 3., so these generators each have order at most 2. Also, by question 4. we have $[\mathfrak{p}_3][\mathfrak{p}_5][\mathfrak{p}_{13}] = 1$, so $\mathrm{Cl}(K)$ is generated by $[\mathfrak{p}_2]$, $[\mathfrak{p}_3]$, $[\mathfrak{p}_5]$, and $[\mathfrak{p}_2][\mathfrak{p}_3][\mathfrak{p}_5] = 1$, so $\mathrm{Cl}(K)$ is generated by $[\mathfrak{p}_2]$ and $[\mathfrak{p}_3]$, and is thus a quotient of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

If this quotient were strict, then at least one of $\mathfrak{p}_2$, $\mathfrak{p}_3$, and $\mathfrak{p}_2\mathfrak{p}_3$ would be principal. But the first two cannot be principal, since there is no element of norm ± 2 nor ± 3 in $\mathbb{Z}_K$ by the previous question; also, if $\mathfrak{p}_2\mathfrak{p}_3$ were principal, then so would be $\mathfrak{p}_5$ by the relation $[\mathfrak{p}_2][\mathfrak{p}_3][\mathfrak{p}_5] = 1$, and again this is impossible since $\mathbb{Z}_K$ has no element of norm ± 5.

7. We make the following remark: a solution to $x^2 - 195y^2 = m$ corresponds to an element γ of $\mathbb{Z}_K$ or norm m, which must generate a principal ideal $\mathfrak{a} = \gamma\mathbb{Z}_K$ of norm $|m|$.

   (a) For $m = 7^{34109}$, there is no solution, since there is no ideal of norm 7^{34109} in $\mathbb{Z}_K$ (because the only prime above 7 is $7\mathbb{Z}_K$, which has norm 2, whereas 34109 is odd.)

   (b) If we had a solution for $m = 10$, then $\mathfrak{a}$ would have norm 10, and hence factor as $\mathfrak{p}_2\mathfrak{p}_5$ since these are the only primes above 2 and 5. But $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5 = (15 + \alpha)$ is principal, so if $\mathfrak{a}$ were principal, then so would be $\mathfrak{p}_3$, which contradicts 5. as seen in 6. This contradiction shows that there is no solution for $m = 10$.

   (c) For $m = 195$, $\mathfrak{a}$ must factor as $\mathfrak{p}_3\mathfrak{p}_5\mathfrak{p}_{13}$. This ideal is principal, indeed it is generated by α according to question 4. So γ must be associate to α, say $\gamma = u\alpha$ for some unit u. But all units have norm $+1$, so this contradicts the fact that γ has norm $+195$. So again there is no solution.

   (d) Since $N_{\mathbb{Q}}^K(1000 + \alpha) = 5 \cdot 199961$ with 199961 prime and since $\mathfrak{p}_5$ is the only prime above 5, the ideal $(1000 + \alpha)\mathbb{Z}_K$ must factor as $\mathfrak{p}_5\mathfrak{q}$ for some prime ideal $\mathfrak{q}$ of norm 199961. In particular, 199961 cannot be inert in K; and sinced it is not ramified either, it must split, say as $\mathfrak{q}\mathfrak{q}'$; whence exactly two ideals of norm m, namely $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{q}$ and $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{q}'$.

Furthermore, $(15+\alpha)(1000+\alpha)\mathbb{Z}_K$ factors as $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5^2\mathfrak{q} = 5\mathfrak{p}_2\mathfrak{p}_3\mathfrak{q}$, and is principal by construction. Therefore, $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{q}$ is also principal, and generated by $\gamma = (15+\alpha)(1000+\alpha)/5$. By multiplicativity of the norm, γ has norm $N_{\mathbb{Q}}^K(1000+\alpha)N_{\mathbb{Q}}^K(15+\alpha)/N_{\mathbb{Q}}^K(5) = 5\cdot 199961\cdot 2\cdot 3\cdot 5/5^2 = m$, so we get a solution! Explicitly, $\gamma = 3039+203\alpha$, so we have found the solution $x=3039$, $y=203$. Besides, $u\gamma$ also has norm m for every unit u (since u always has norm $+1$); since $\mathbb{Z}_K^\times$ is infinite, we actually have infinitely many solutions.

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 $\mathrm{Cl}(K)$.

Solution 6

See example 6.4.1 in the lecture notes.

END