# Algebraic number theory — Exercise sheet 3

https://www.maths.tcd.ie/~mascotn/teaching/2022/MAU34109/index.html

Version: October 22, 2022

Email your answers to mascotn@tcd.ie by Wednesday November 02 noon.

# Exercise 3.1: A cubic field (100 pts)

Let  $f(x) = x^3 - 5x + 5$ , and let  $K = \mathbb{Q}(\alpha)$ , where  $\alpha$  is a root of f(x).

- 1. (15 pts) Determine the degree  $[K : \mathbb{Q}]$  and the ring of integers  $\mathbb{Z}_K$  of K.
- 2. (10 pts) Which primes  $p \in \mathbb{N}$  ramify in K?
- 3. (25 pts) For each  $n \in \mathbb{N}$ ,  $n \leq 7$ , compute explicitly the decomposition of  $n\mathbb{Z}_K$  as a product of prime ideals.
- 4. (15 pts) Prove that the prime(s) above 5 are principal, and find an explicit generator for them.
- 5. (15pts) List all the ideals  $\mathfrak{a}$  of  $\mathbb{Z}_K$  such that  $N(\mathfrak{a}) \leq 7$ .
- 6. (20 pts) Factor the ideals  $(\alpha 2)$  and  $(\alpha + 1)$  into primes.

You may use without proof the result of Exercise 3.2 below (which BTW I really encourage you to solve).

## Solution 3.1:

1. Let  $A(x) = x^3 - 5x + 5$ . This is Eisenstein at p = 5, and therefore irreducible, so A(x) is the minimal polynomial of  $\alpha$  whence  $[K : \mathbb{Q}] = \deg A = 3$ .

We have  $\operatorname{disc}(A) = -4 \cdot (-5)^3 - 27 \cdot 5^2 = 5^2 \cdot (4 \cdot 5 - 27) = -5^2 \cdot 7$ , so the order  $\mathbb{Z}[\alpha]$  is maximal at all p except maybe at p = 5. However, since A(x) is Eisenstein at 5,  $\mathbb{Z}[\alpha]$  is in fact also maximal at 5. As a result,

$$\mathbb{Z}_K = \mathbb{Z}[\alpha].$$

- 2. The primes that ramify are the ones which divide the discriminant, which in this case is disc  $K = -5^2 \cdot 7$  according to the previous question. Therefore, the primes that ramify in K are precisely 5 and 7.
- 3. Since  $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ , we can see how  $p\mathbb{Z}_K$  decomposes by studying how A(x) factors mod p. For this, we can use the fact that since it is of degree 3, it is irreducible iff. it has no root.
  - We have  $1\mathbb{Z}_K = \mathbb{Z}_K$ .

- Since A(0) ≡ A(1) ≡ 1 mod 2, A(x) has not root mod 2, so it is irreducible mod 2, and so 2 is inert in K, i.e. 2Z<sub>K</sub> = p<sub>2</sub> is a prime of residual degree 3.
- Mod 3, we have  $A(-1) \equiv 0$ , so  $x + 1 \mid A(x) \mod 3$ . After a Euclidean division mod 3, we find that  $A(x) \equiv (x + 1)(x^2 x 1) \mod 3$ , and the quadratic factor has no root in  $\mathbb{Z}/3\mathbb{Z}$ , so this is the full factorisation. Therefore,  $3\mathbb{Z}_K = \mathfrak{p}_3\mathfrak{p}'_3$ , with  $\mathfrak{p}_3 = (3, \alpha + 1)$  and  $\mathfrak{p}'_3 = (3, \alpha^2 \alpha 1)$ , whose respective residual degrees are 1 and 2.
- We have  $4\mathbb{Z}_K = 2\mathbb{Z}_K \cdot 2\mathbb{Z}_K = \mathfrak{p}_2^2$ .
- We have  $A(x) \equiv x^3 \mod 5$ , and so  $5\mathbb{Z}_K = \mathfrak{p}_5^3$ , where  $\mathfrak{p}_5 = (5, \alpha)$ , whose residual degree is 1. In particular, 5 is totally ramified in K, but we already knew that since A(x) is Eisenstein at 5.
- We have  $6\mathbb{Z}_K = 2\mathbb{Z}_K \cdot 3\mathbb{Z}_K = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}'_3$ .
- Finally, we check that A(x) has two roots in  $\mathbb{Z}/7\mathbb{Z}$ , namely  $4 \equiv -3$  and  $5 \equiv -2$ , so  $(x+3)(x+2) \mid f(x) \mod 7$ . A Euclidean division<sup>1</sup> reveals that in fact,  $A(x) \equiv (x+2)^2(x+3) \mod 7$ , and so  $7\mathbb{Z}_K = \mathfrak{p}_7^2\mathfrak{p}_7'$ , where  $\mathfrak{p}_7 = (7, \alpha + 2)$  and  $\mathfrak{p}_7' = (7, \alpha + 3)$  both have residual degree 1.
- 4. The only prime above 5 is  $\mathfrak{p}_5$ . We have  $\alpha \in \mathfrak{p}_5$ , and  $N_{\mathbb{Q}}^K(\alpha) = -5$  (from the constant coefficient of A(x)), so  $|N_{\mathbb{Q}}^K(\alpha)| = N(\mathfrak{p}_5)$ , which proves that  $\mathfrak{p}_5 = \alpha \mathbb{Z}_K$  is the ideal generated by  $\alpha$ .
- 5. The only ideal of norm 1 is  $\mathbb{Z}_K$  itself.
  - An ideal of norm 2 would be a prime (since its norm is prime) lying above 2, but  $N(\mathfrak{p}_2) = 2^3 = 8$ , so no such ideal exists.
  - For the same reason, we find that the only ideal of norm 3 is  $\mathfrak{p}_3$ .
  - An ideal of norm 4 would be a product of ideals above 2, but since  $N(\mathfrak{p}_2) = 8$ , there are no such ideals.
  - An ideal of norm 5 must be a prime above 5, so must be  $\mathfrak{p}_5$ .
  - An ideal of norm 6 must factor as a product of primes above 2 and 3. Among these primes, the product of those lying above 2 must be of norm 2, but  $N(\mathfrak{p}_2) = 8$ , so there is not such ideal.
  - Finally, for the same reasons as above, the only ideals of norm 7 are p<sub>7</sub> and p<sub>7</sub>'.

As a conclusion, the ideals of  $\mathbb{Z}_K$  of norm up to 7 are  $\mathbb{Z}_K$  itself,  $\mathfrak{p}_3$ ,  $\mathfrak{p}_5$ ,  $\mathfrak{p}_7$  and  $\mathfrak{p}'_7$ .

<sup>&</sup>lt;sup>1</sup>Other possibility : since -3 and -2 are the only roots of  $A(x) \mod 7$ , we must have either  $A(x) \equiv (x+2)^2(x+3)$  or  $(x+2)(x+3)^2 \mod 7$ . Expand both and check that only the first one works mod 7. (It was impossible that both would work mod 7, because  $(\mathbb{Z}/7\mathbb{Z})[x]$  is a UFD since  $\mathbb{Z}/7\mathbb{Z}$  is a field, so we could predict that this method would succeed before we even tried.) Yet another possibility: the coefficient of  $x^2$  in A(x) is the negative of the sum of the roots, so the roots sum to 0. As the first two roots are -2 and -3, the third one is 2+3=5=-2.

6. Let  $\mathfrak{a} = (\alpha - 2)$ . We have  $N(\mathfrak{a}) = |N_{\mathbb{Q}}^{K}(\alpha - 2)| = 3$  by Exercise 3.2, so by the previous question we must have  $\mathfrak{a} = \mathfrak{p}_{3}$ .

Let  $\mathfrak{b} = (\alpha + 1)$ . This time  $N(\mathfrak{b}) = |N_{\mathbb{Q}}^{K}(\alpha + 1)| = 9$ , so either  $\mathfrak{b} = \mathfrak{p}_{3}^{2}$  or  $\mathfrak{b} = \mathfrak{p}_{3}^{\prime}$ . However, we know that  $\alpha + 1 \in \mathfrak{p}_{3}$ , so  $\mathfrak{p}_{3} | \mathfrak{b}$ . Therefore the only possibility is that  $\mathfrak{b} = \mathfrak{p}_{3}^{2}$ .

Remark: we could have tried to prove that  $\alpha + 1 \notin \mathfrak{p}'_3$ , but this is more difficult.

7. By the previous question, we have  $(\alpha + 1) = \mathfrak{p}_3^2 = (\alpha - 2)^2 = ((\alpha - 2)^2)$ , so  $u = \frac{\alpha + 1}{(\alpha - 2)^2}$  is a unit in  $\mathbb{Z}_K$ . It is clearly not  $\pm 1$  (in fact we can compute that  $u = 2\alpha^2 + 3\alpha - 6$ ).

Other possibility: By questions 3 and 4, we have  $(5) = \mathfrak{p}_5^3 = (\alpha)^3 = (\alpha^3)$ , so  $v = \alpha^3/5 = \frac{5\alpha-5}{5} = \alpha - 1$  is a unit, which is clearly not  $\pm 1$ .

Remark (to be read after the chapter on units): Since disc K < 0, K has signature (1,1), so  $\mathbb{Z}_{K}^{\times}$  has rank 1 by Dirichlet's theorem, so u and v cannot be independent. In fact, one may check that  $u = -v^{-2}$ , and it can be proved that v is a fundamental unit.

This was the only mandatory exercise, that you must submit before the deadline. The following exercises are not mandatory; they are not worth any points, and you do not have to submit them. However, I highly recommend that you try to solve them for practice (they may even give you inspiration to help you solve Exercise 1), and you are welcome to email me if you have questions about them. The solutions will be made available with the solution to the mandatory exercise.

#### Exercise 3.2: A useful formula

Let  $A(x) \in \mathbb{Q}[x]$  be monic and irreducible, and consider the number field  $K = \mathbb{Q}(\alpha)$ where  $A(\alpha) = 0$ . Prove that for all  $n \in \mathbb{Z}$ ,

$$N_{\mathbb{O}}^{K}(\alpha+n) = (-1)^{\deg A} A(-n).$$

## Solution 3.2:

Since A(x) is monic and irreducible, it is the minimal polynomial of  $\alpha$ .

Let  $\alpha_1, \dots, \alpha_d \in \mathbb{C}$  be the complex roots of A(x), so that  $A(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ ,  $d = \deg A = [K : \mathbb{Q}]$ , and the complex embeddings of K are given by  $\alpha \mapsto \alpha_i$ . Then these complex embeddings take  $\alpha + n \in K$  to  $\alpha_i + n \in \mathbb{C}$ , whence

$$N_{\mathbb{Q}}^{K}(\alpha+n) = (\alpha_{1}+n)\cdots(\alpha_{d}+n) = (-1)^{d}(-n-\alpha_{1})\cdots(-n-\alpha_{d}) = (-1)^{d}A(-n).$$

Other approach: Let  $M_{\alpha}$  be the  $d \times d$  matrix of the multiplication-by- $\alpha$  map (with respect to some Q-basis of K, e.g. the power basis attached to  $\alpha$ ). The characteristic polynomial of  $M_{\alpha}$  is  $\det(xI_d - M_{\alpha}) = \chi_{\alpha}(x)$  by definition, where  $I_d$  is the identity matrix. But since  $\alpha$  is a primitive element for K, we have that  $\chi_{\alpha}(x) =$ A(x). Furthermore, the matrix of multiplication by n is  $nI_d$  (with respect to our chosen  $\mathbb{Q}$ -basis of K, and indeed with respect to any  $\mathbb{Q}$ -basis of K), so the matrix of multiplication by  $\alpha + n$  is  $M_{\alpha} + nI_d$ . Therefore

$$N_{\mathbb{Q}}^{K}(\alpha+n) = \det(M_{\alpha}+nI_{d}) = (-1)^{d} \det(-nI_{d}-M_{\alpha}) = (-1)^{d} \chi_{\alpha}(-n) = (-1)^{d} A(-n).$$

## Exercise 3.3: Ideals of fixed norm

- 1. How many ideals of norm 900 are there in the ring of integers of  $\mathbb{Q}(\sqrt{7})$ ? Hint: Compute the decomposition in  $\mathbb{Q}(\sqrt{7})$  of the primes  $p \in \mathbb{N}$  that divide 900.
- 2. How many ideals of norm 80 are there in the ring of integers of  $\mathbb{Q}(\zeta)$ , where  $\zeta$  is a primitive 60th root of unity?

## Solution 3.3:

1. The key to this exercise is to remember that the norm of ideals is multiplicative, and that the norm of a prime  $\mathfrak{p}$  of residual degree f above  $p \in \mathbb{N}$  is  $p^f$ . Thus for instance if  $\mathfrak{a}$  is an ideal of norm  $200 = 2^3 5^2$ , and if  $\mathfrak{a}$  factors as

$$\mathfrak{a} = \prod_i \mathfrak{p}_i^{e_i},$$

then the factor  $5^2$  in 200 comes exclusively from the primes  $\mathfrak{p}_i$  that lie above 5, and similarly for  $2^3$ . Also, all the  $\mathfrak{p}_i$  lie either above 2, or above 5, since they would contribute another prime to the norm of  $\mathfrak{a}$  else. So if we regroup the  $\mathfrak{p}_i$  according to the rational prime  $p \in \mathbb{N}$  they lie above, say

$$\mathfrak{a} = \left(\prod_{\mathfrak{p}_i|2} \mathfrak{p}_i^{e_i}
ight) \left(\prod_{\mathfrak{p}_i|5} \mathfrak{p}_i^{e_i}
ight)$$

where  $\mathfrak{p} \mid p$  means that the prime ideal  $\mathfrak{p}$  lies above the prime number p, then we have  $N\left(\prod_{\mathfrak{p}_i|2}\mathfrak{p}_i^{e_i}\right) = 2^3$  and  $N\left(\prod_{\mathfrak{p}_i|5}\mathfrak{p}_i^{e_i}\right) = 5^2$ . And then, the kind of primes  $\mathfrak{p}_i$  and exponents  $e_i$  that we can use to achieve these equalities depends on how 2 and 5 decompose.

So, back to the question of the exercise, let  $K = \mathbb{Q}(\sqrt{7})$ . In order to find the ideals of norm  $900 = 2^2 3^2 5^2$  in K, we first take a look at how 2, 3 and 5 decompose in K.

As  $7 \equiv 3 \mod 4$ , we find that 2 ramifies in K, say

$$2\mathbb{Z}_K = \mathfrak{p}_2^2$$

where  $\mathbf{p}_2$  has residual degree 1 and hence norm  $2^1 = 2$ . So the factor  $2^2 \mid 900$ , which can only come from primes above 2, must actually come from  $\mathbf{p}_2^2$ , since there is no other choice.

Next, since  $7 \equiv 1 \mod 3$  is a square mod 3, we find that 3 splits in K, say

$$3\mathbb{Z}_K = \mathfrak{p}_3\mathfrak{p}_3'$$

This time the situation is more interesting: to make the factor  $3^3 \mid 900$ , we need either two primes of degree 1 above 3, or one prime of degree 2 above 3; but both  $\mathfrak{p}_3$  and  $\mathfrak{p}'_3$  have degree 1, so the only choices we have are to take  $\mathfrak{p}_3$  twice, or  $\mathfrak{p}'_3$  twice, or both  $\mathfrak{p}_3$  and  $\mathfrak{p}'_3$  once each.

Finally, since 7 is not a square mod 5 (as can been seen by computing  $x^2 \mod 5$  for x from 1 to 5), we find that 5 is inert in K, so that the only prime above 5 is  $\mathfrak{p}_5 = 5\mathbb{Z}_K$  itself. It has degree 2, so its norm is  $5^2$ , and so the only way of producing the factor  $5^2 \mid 900$  is to take  $\mathfrak{p}_5$ .

To sum up, for 2 and for 5 we have only one choice, whereas for 3 we have three choices. So there are exactly three ideals of norm 900 in K, namely  $\mathfrak{p}_2^2\mathfrak{p}_3^2\mathfrak{p}_5$ ,  $\mathfrak{p}_2^2\mathfrak{p}_3'^2\mathfrak{p}_5$ , and  $\mathfrak{p}_2^2\mathfrak{p}_3\mathfrak{p}_5$ .

Note that we can simplify these expressions a bit: since  $\mathfrak{p}_2^2 = 2\mathbb{Z}_K$ ,  $\mathfrak{p}_3\mathfrak{p}_3' = 3\mathbb{Z}_K$ , and  $\mathfrak{p}_5 = 5\mathbb{Z}_K$ , we find that our three ideals of norm 900 are  $10\mathfrak{p}_3^2$ ,  $10\mathfrak{p}_3'^2$ , and  $30\mathbb{Z}_K$ .

2. Same principle. First, 80 is 2<sup>4</sup>5, so we must study how 2 and 5 decompose in  $L = \mathbb{Q}(\zeta)$ . This is a number field of degree

$$d = \varphi(60) = 60 \cdot (1 - 1/2) \cdot (1 - 1/3) \cdot (1 - 1/5) = 16,$$

but fortunately we have a theorem that tells us exactly how primes decompose in this field.

Namely, for p = 2 we write  $60 = 2^2 \cdot 15$ , which shows us that the ramification index of the primes above 2 in L is  $e = \varphi(2^2) = 2$ , and then we compute  $2^i \mod 15$  for  $i = 1, 2, 3, \cdots$ . We find 2, 4, 8, and then 1, so the multiplicative order of 2 mod 15 is f = 4, so that the primes above 2 in L have residual degree f = 4. So there must be d/ef = 2 such primes, whence

$$2\mathbb{Z}_L = \mathfrak{p}_2^2 \mathfrak{p}_2^{\prime 2}$$

where both  $\mathbf{p}_2$  and  $\mathbf{p}_2$  are prime ideals of norm  $p^f = 2^4$ . This is precisely the factor of 80 that we want to contribute to with these primes, so we have two ways to do so: either take  $\mathbf{p}_2$  or  $\mathbf{p}'_2$ .

Next, for p = 5, we write  $60 = 5^1 \cdot 12$ , so the ramification index of the primes above 5 is  $e = \varphi(5^1) = 4$ , and compute the powers of 5 mod 12. Since  $5^2 \equiv 1 \mod 12$ , the residual degree of the primes above 5 is f = 2. Finally, there are g = d/ef = 2 of them, whence

$$5\mathbb{Z}_L = \mathfrak{p}_5^4 \mathfrak{p}_5^{\prime 4}$$

where each factor has norm  $p^f = 5^2$ . But... but this means that there is no way to contribute only for  $5^1 | 80 !$  So there are actually no ideals of norm 80 in  $\mathbb{Z}_L$ , just because of that.

Actually, with the benefit of hindsight, we could have stopped the computation as soon as we had noticed that the multiplicative order of 5 mod 12 is strictly greater than the exponent of 5 in 80, that is to say 1. We didn't even have to compute how 2 decomposes in L, since we already have an obstruction with the prime 5.

## Exercise 3.4: Similar-looking yet non-isomorphic number fields

The goal of this exercise is to prove that the number fields  $\mathbb{Q}(\sqrt[3]{6})$  and  $\mathbb{Q}(\sqrt[3]{12})$  have the same degree and discriminant, but are not isomorphic.

To ease notation, we let  $\alpha = \sqrt[3]{6}$ ,  $\beta = \sqrt[3]{12}$ ,  $K = \mathbb{Q}(\alpha)$  and  $L = \mathbb{Q}(\beta)$ .

- 1. Prove that  $[K : \mathbb{Q}] = 3$ .
- 2. Prove that  $\mathbb{Z}_K = \mathbb{Z}[\alpha]$  and compute disc K.
- 3. Prove that  $[L : \mathbb{Q}] = 3$  and that disc L is of the form  $-2^a 3^5$  for some integer  $a \ge 0$ . What are the possible values of a ?
- 4. Prove that  $L \simeq \mathbb{Q}(\sqrt[3]{18})$ . Hint: Take a look at  $\gamma = \beta^2/2$ .
- 5. Deduce that disc  $L = \operatorname{disc} K$ .
- 6. Which primes  $p \in \mathbb{N}$  ramify in K? What about L?
- 7. Compute explicitly the decomposition of 7 in K and in L.
- 8. Deduce that K and L are not isomorphic.
- 9. Compute explicitly the decomposition of 2 and 3 in K and in L.
- 10. Deduce the factorisation of the ideals  $\alpha \mathbb{Z}_K$ ,  $\beta \mathbb{Z}_L$  and  $\gamma \mathbb{Z}_L$  into primes.

#### Solution 3.4:

- 1. Clearly,  $\alpha$  is a root of the polynomial  $f(x) = x^3 6 \in \mathbb{Z}[x]$ . This polynomial is Eisenstein at 2 (and also at 3), so it is irreducible over  $\mathbb{Q}$ ; it is therefore the minimal polynomial of  $\alpha$ . This shows that  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg f(x) = 3$ .
- 2. Since  $f(x) \in \mathbb{Z}[x]$  is monic,  $\alpha \in \mathbb{Z}_K$ . Also,  $\alpha$  is a primitive element of K by definition of K, so  $\mathbb{Z}[\alpha]$  is an order in K.

The discriminant of this order is

disc 
$$\mathbb{Z}[\alpha] = \text{disc } f = -3^3 6^2 = -2^2 3^5$$
,

so the only primes at which  $\mathbb{Z}[\alpha]$  might not be maximal are 2 and 3. However, f(x) is Eisenstein at 2 and 3, so  $\mathbb{Z}[\alpha]$  is in fact maximal at 2 and 3, whence  $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ , and so disc  $K = \text{disc } \mathbb{Z}[\alpha] = -2^2 3^5$ .

3. Just as in question 1, the fact that  $g(x) = x^3 - 12$  is Eisenstein at 3 implies that it is irreducible, so it is the minimal polynomial of  $\beta$ , whence

$$[\mathbb{Q}(\beta):\mathbb{Q}] = \deg g(x) = 3.$$

Next, for the same reasons as in question 2, we find that  $\mathbb{Z}[\beta]$  is an order in L, of discriminant

disc 
$$g = -3^3 12^2 = -2^4 3^5$$
.

As a result, this order is maximal at every prime except maybe 2 and 3. Since g(x) is Eisenstein at 3, this order is actually maximal at 3; however this argument does **not** apply at 2 because  $2^2|12$ . So all we can say is that

$$\operatorname{disc} L = \frac{-2^4 3^5}{m^2},$$

where m is the index of  $\mathbb{Z}[\beta]$ , which is thus a power of 2 (possibly m = 1). Thus

$$\operatorname{disc} L = -2^a 3^5$$

with  $a \in \{0, 2, 4\}$ .

4. We have  $\gamma^3 = \beta^6/2^3 = 18$ . Since  $h(x) = x^3 - 18$  is Eisenstein at 2, it is irreducible over  $\mathbb{Q}$ , so h(x) is the minimal polynomial both of  $\gamma$  and of  $\sqrt[3]{18}$ . This shows that the fields  $\mathbb{Q}(\gamma)$  and  $\mathbb{Q}(\sqrt[3]{18}$  have degree 3 and are isomorphic. As  $\gamma \in L$ , we deduce that L contains  $\mathbb{Q}(\gamma)$ , which is a copy of  $\mathbb{Q}(\sqrt[3]{18})$ . Actually, since both L and  $\mathbb{Q}(\sqrt[3]{18})$  have degree 3, the inclusion  $\mathbb{Q}(\gamma) \subset L$  is an equality, and thus

$$L = \mathbb{Q}(\gamma) \simeq \mathbb{Q}(\sqrt[3]{18}).$$

5. Again,  $\mathbb{Z}[\gamma]$  is an order in L, of discriminant

disc 
$$\mathbb{Z}[\gamma] = \text{disc } h = -3^3 18^2 = -2^2 3^7.$$

But h is Eisenstein at 2, so as in question 3 we deduce that

$$\operatorname{disc} L = -2^2 3^b$$

with  $b \in \{1, 3, 5, 7\}$  this time.

By comparing this information with what we have found in question 3, we deduce that

$$\operatorname{disc} L = -2^2 3^5 = \operatorname{disc} K$$

(By the way, this means that neither  $\mathbb{Z}[\beta]$  nor  $\mathbb{Z}[\gamma]$  are maximal; in fact, we see that their respective indices are 2 and 3.)

6. The primes that ramify in K are exactly the ones that divide disc K, that is to say 2 and 3. Since disc L = disc K, these are also the primes that ramify in L.

7. Since  $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ , we can read the decomposition of 7 in  $\mathbb{Z}_K$  off the factorisation of  $f(x) \mod 7$ . In order to compute this factorisation, let us make a table of the values of  $x^3 \mod 7$ , so as to look for roots of  $f(x) \mod 7$ :

$x \bmod 7$	0	1	2	3	-3	-2	-1
$x^3 \mod 7$	0	1	1	-1	1	-1	-1

As  $f(x) \equiv x^3 + 1 \mod 7$ , we see that 3, -2 and -1 are roots of  $f(x) \mod 7$ , whence

 $f(x) \equiv (x-3)(x+2)(x+1) \mod 7.$ 

So 7 splits completely in K, more precisely

$$7\mathbb{Z}_K = (7, \alpha - 3) \cdot (7, \alpha + 2) \cdot (7, \alpha + 1)$$

where each of the three factors is a prime ideal of  $\mathbb{Z}_K$ .

Let us move on to the decomposition of 7 in  $\mathbb{Z}_L$ . The order  $\mathbb{Z}[\beta] \subset \mathbb{Z}_L$  may not be maximal, but it is maximal at 7, so we can still read the decomposition of 7 in  $\mathbb{Z}_K$  off the factorisation of  $g(x) \mod 7$  (we could just as well consider h(x)since  $\mathbb{Z}[\gamma]$  is maximal at 7 too).

Thanks to the table above, we see that  $x^3 \not\equiv 12 \mod 7$  for all  $x \in \mathbb{Z}/7\mathbb{Z}$ , so g(x) has no root mod 7. Since it has degree 3, this means that it is irreducible over  $\mathbb{Z}/7\mathbb{Z}$  (because else it would have at least one linear factor). As a consequence, 7 is inert in  $\mathbb{Z}_L$ , i.e.

 $7\mathbb{Z}_L$ 

is a prime ideal (of degree 3) of  $\mathbb{Z}_L$ .

- 8. That's because the splitting behaviour of 7 is not the same in K and L: by the previous question, 7 splits completely in K, but not at all in L.
- 9. For K, this is easy. Indeed, the fact that  $\mathbb{Z}_K = \mathbb{Z}[\alpha]$  implies that we can compute the decomposition of any prime p (in particular 2 and 3) by factoring  $f(x) \mod p$ .

As  $f(x) \equiv x^3 \mod 2$ , we have

$$2\mathbb{Z}_K = \mathfrak{p}_2^3$$

where  $\mathfrak{p}_2 = (2, \alpha) \subset \mathbb{Z}_K$  is a prime ideal. Also,  $f(x) \equiv x^3 \mod 3$ , so

$$3\mathbb{Z}_K = \mathfrak{p}$$

where  $\mathfrak{p}_3 = (3, \alpha) \subset \mathbb{Z}_K$  is another prime ideal.

In particular, both 2 and 3 are totally ramified in K. We already knew that they are ramified from question 6, and in fact we already knew that they are totally ramified because f(x) is Eisenstein at 2 and 3.

Let us now deal with L. Here things are a bit more complicated since we do not know a nice form for  $\mathbb{Z}_L$  (it is not too difficult to prove that  $\mathbb{Z}_L = \mathbb{Z}[\beta, \gamma] = \mathbb{Z} \oplus \mathbb{Z}\beta \oplus \mathbb{Z}\gamma$ , but this does not help to compute how primes decompose in L). So, for p = 2, we cannot read the decomposition of 2 off the factorisation of  $g(x) \mod 2$  because  $\mathbb{Z}[\beta]$  is unfortunately not maximal at 2 (or, at least, we do not know if it is). But  $\mathbb{Z}[\gamma]$  is ! So we can use h(x) instead. We have  $h(x) \equiv x^3 \mod 2$ , whence

$$2\mathbb{Z}_L = \mathfrak{q}_2^3,$$

where  $\mathbf{q}_2$  is the prime ideal  $(2, \gamma)$  of  $\mathbb{Z}_L$ . Similarly, for p = 3 we must not use h(x), but we can use g(x), and since  $g(x) \equiv x^3 \mod 3$ , we have

$$3\mathbb{Z}_L = \mathfrak{q}_3^3,$$

where  $\mathfrak{q}_3$  is the prime ideal  $(3,\beta)$  of  $\mathbb{Z}_L$ .

So again 2 and 3 are both totally ramified in L (even though K and L are not isomorphic, as we now know). And again, we already knew this: for 2, is it because h(x) is Eisenstein at 2, and for 3, it is because g(x) is Eisenstein at 3.

10. We know that the norm of the ideal  $\alpha \mathbb{Z}_K$  is  $|N_{\mathbb{Q}}^K(\alpha)| = 6 = 2 \cdot 3$  (because  $x^3 - 6$  is in fact the characteristic polynomial of  $\alpha$  as it has the same degree as  $[K : \mathbb{Q}]$ , and the determinant of a matrix is up to sign the constant coefficient of its characteristic polynomial). So this ideal must be the product of a prime of degree 1 above 2 and of a prime of degree 1 above 3. Luckily, we have just seen that there is only one prime above 2 and one prime above 3 in  $\mathbb{Z}_K$ , so necessarily

$$\alpha \mathbb{Z}_K = \mathfrak{p}_2 \mathfrak{p}_3.$$

Next, the norm of  $\beta \mathbb{Z}_L$  is  $|N_{\mathbb{Q}}^L(\beta)| = 12 = 2^2 \cdot 3$ , which means that this ideal is the product of a prime of degree 1 above 3 and of either two primes of degree 1 above 2 (possibly twice the same), or of one prime of degree 2 above 2. But again, we are in luck, as there are only one prime above 2 and one prime above 3 in  $\mathbb{Z}_L$ . So we must have

$$eta \mathbb{Z}_L = \mathfrak{q}_2^2 \mathfrak{q}_3.$$

Similarly,  $\gamma \mathbb{Z}_L$  has norm 18, and so

 $\gamma \mathbb{Z}_L = \mathfrak{q}_2 \mathfrak{q}_3^3.$