

# Algebraic number theory — Exercise sheet 1

<https://www.maths.tcd.ie/~mascoth/teaching/2026/MAU34109/index.html>

Version: October 8, 2026

Submit your answers in class or to [neumayec@tcd.ie](mailto:neumayec@tcd.ie) by Thursday October 8, 1pm.

## Exercise 1.1: A polynomial of degree 3 (100 pts)

Let  $F(x) = x^3 - 4x + 1 \in \mathbb{Q}[x]$ . We admit without proof that  $F(x)$  has three real roots, which are approximately  $-2.11$ ,  $0.25$ , and  $1.86$ .

Let  $K = \mathbb{Q}(\alpha)$ , where  $\alpha$  is a root of  $F(x)$ , and let  $\beta = \alpha^2 - 4 \in K$ .

1. (5 pts) Prove that  $F(x)$  is irreducible over  $\mathbb{Q}$ .
2. (5 pts) Why is it important that  $F(x)$  be irreducible over  $\mathbb{Q}$  for the definition of  $K$ ?
3. (5 pts) What is the extension degree  $[K : \mathbb{Q}]$ ?
4. (10 pts) What is the signature of  $K$ ?
5. (10 pts) Write down the matrix of multiplication by  $\alpha$  with respect to the  $\mathbb{Q}$ -basis of  $K$  of your choice (clearly say which basis you are using).
6. (20 pts) Hence or otherwise, determine  $\text{Tr}_{\mathbb{Q}}^K(\beta)$  and  $N_{\mathbb{Q}}^K(\beta)$ . Your results must be exact; approximations are not good enough (unless you somehow manage to prove that they are exact).
7. (15 pts) Explain how the approximate values of the roots of  $F(x)$  may be used to confirm that your calculations for  $\text{Tr}_{\mathbb{Q}}^K(\beta)$  and  $N_{\mathbb{Q}}^K(\beta)$  are correct, at least approximately.
8. (10 pts) Prove that there exist rational numbers  $a, b, c \in \mathbb{Q}$  such that  $1/\beta = a + b\alpha + c\alpha^2$ . Are  $a, b, c$  unique? Justify your answer.
9. (20 pts) Sketch two different methods that you could use to determine  $a, b, c$  as in the previous question (but do not actually determine them).

## Solution 1.1:

1. Since  $\deg F = 3$ , if  $F$  were not irreducible, it would have a linear factor, and thus a rational root (note that this is NOT true in higher degree, for instance a polynomial of degree 4 can factor into two polynomials of degree 2).

The rational root theorem shows that the only possible rational roots of  $F$  are  $\pm 1$ . As none of these are actual roots, we conclude that  $F$  is irreducible over  $\mathbb{Q}$ .

2. Since  $F$  is irreducible over  $\mathbb{Q}$ , we have  $\mathbb{Q}(\alpha) \simeq \mathbb{Q}[x]/(F(x))$  no matter which root  $\alpha$  we pick, so  $K$  is well-defined up to isomorphism. In contrast, if for example  $F$  had factored as  $F = AB$  with  $A$  and  $B$  irreducible, then  $\mathbb{Q}(\alpha)$  would have been isomorphic to  $\mathbb{Q}[x]/(A(x))$  or to  $\mathbb{Q}[x]/(B(x))$  depending on whether the  $\alpha$  we pick is a root of  $A$  or of  $B$ . Since those two quotients of  $\mathbb{Q}[x]$  are likely not isomorphic to each other (for example, they would not even have the same degree as field extensions of  $\mathbb{Q}$  unless  $\deg A = \deg B$ ), the rest of the exercise would not have made sense.
3. Since  $F$  is monic and irreducible over  $\mathbb{Q}$ , it is the minimal polynomial of  $\alpha$  over  $\mathbb{Q}$ ; therefore  $[K : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg F = 3$ .
4. We know that the embeddings of  $K$  into  $\mathbb{C}$  correspond to the complex roots of the minimal polynomial  $F(x)$  of the generator  $\alpha$  of  $K$ , in that each such embedding  $\sigma : K \rightarrow \mathbb{C}$  is completely determined by  $\sigma(\alpha)$  (as  $K = \mathbb{Q}(\alpha)$ ), and that the possible values of  $\sigma(\alpha)$  are the complex roots of  $F$ . Therefore, we get three real embeddings  $\alpha \mapsto -2.11$ ,  $\alpha \mapsto 0.25$ , and  $\alpha \mapsto 1.86$  (approximately). These are all real, and none of them is imaginary, so the signature of  $K$  is  $(3, 0)$ .
5. Since  $K = \mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$  with  $\alpha$  algebraic of degree 3, we know that  $1, \alpha, \alpha^2$  is a  $\mathbb{Q}$ -basis of  $K$ . As multiplication by  $\alpha$  takes these numbers to  $\alpha$ ,  $\alpha^2$ , and  $\alpha^3 = 4\alpha - 1$  respectively, the matrix of multiplication by  $\alpha$  with respect to this  $\mathbb{Q}$ -basis of  $K$  is

$$M_\alpha = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 4 \\ 0 & 1 & 0 \end{pmatrix}.$$

6. Since  $\beta = \alpha^2 - 4$ , the matrix of multiplication by  $\beta$  (with respect to the same  $\mathbb{Q}$ -basis as before) is

$$M_\beta = M_\alpha^2 - 4I = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 4 \\ 0 & 1 & 0 \end{pmatrix}^2 - \begin{pmatrix} 4 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \end{pmatrix} = \cdots = \begin{pmatrix} -4 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Alternatively, we can write down  $M_\beta$  directly by evaluating  $\beta \cdot 1$ ,  $\beta \cdot \alpha$ , and  $\beta \cdot \alpha^2$  (had you noticed that in the calculation above, the first column of  $M_\beta$  is made up of the coordinates of  $\beta = \alpha^2 - 4$ ?). Either way, we immediately see that  $\text{Tr}_{\mathbb{Q}}^K(\beta) = -4$ , and with a little bit more effort, that  $N_{\mathbb{Q}}^K(\beta) = 1$ .

7. Since  $\sigma(\beta) = \sigma(\alpha^2 - 4) = \sigma(\alpha)^2 - 4$  for any embedding  $\sigma$  of  $K$  into  $\mathbb{C}$ , we can calculate approximately that the images of  $\beta$  under these embeddings are

$$(-2.11)^2 - 4 \approx 0.45, \quad (0.25)^2 - 4 \approx -3.94, \quad (1.86)^2 - 4 \approx -0.54.$$

The trace (resp. norm) of  $\beta$  is the sum (resp. product) of these values, which works out to approximately  $-4$  (resp.  $1$ ).

Those are of course merely approximations, but it is good to confirm our matrix calculations, especially if (like me!) you tend to mess those up. Furthermore,

we point out that since  $F(x) \in \mathbb{Z}[x]$ ,  $\alpha$  is an algebraic integer, and therefore so is  $\beta$  since algebraic integers form a ring, so that the trace and norm of  $\beta$  must be integers, which justifies that our approximations are in fact exact. However, this would be Chapter 2 material, whereas this assignment is meant to be about Chapter 1.

8.  $K$  is a field and  $\beta$  is nonzero in  $K$  since it has nonzero coordinates  $(-4, 0, 1)$  on the  $\mathbb{Q}$ -basis  $(1, \alpha, \alpha^2)$  of  $K$ , so  $\beta^{-1}$  exists in  $K$  and is therefore of the form  $a1 + b\alpha + c\alpha^2$  since  $(1, \alpha, \alpha^2)$  is a basis, with coordinates  $a, b, c \in \mathbb{Q}$  since it is a  $\mathbb{Q}$ -basis (meaning we think of  $K$  as a vector space over  $\mathbb{Q}$ ). These coordinates are unique since we have a basis (otherwise it would be linearly dependent).
9.
  - We can apply Euclid's algorithm to  $B(x) = x^2 - 4$  and  $F(x)$  so as to check that  $\gcd(B, F) = 1$  and thus find polynomials  $U(x), V(x) \in \mathbb{Q}[x]$  such that  $U(x)B(x) + V(x)F(x) = 1$ , whence  $U(\alpha) = 1/\beta$  by evaluating at  $x = \alpha$ . (And if  $\deg U \geq 3$ , we replace  $U$  with the remainder of its division by  $F$ .)
  - Since we have worked out the matrix  $M_\beta$  of multiplication by  $\beta$  in a previous question, we can solve the linear system

$$M_\beta \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

since the right-hand side encodes  $1 \in K$  on our basis. Equivalently, we can solve  $(2\alpha^2 - 1)(a + b\alpha + c\alpha^2) = 1$  for  $a, b, c$ .

- We could even calculate the inverse matrix  $M_\beta^{-1} = M_{\beta^{-1}}$ , and read  $a, b, c$  off its first column (whereas the other columns would give us the coordinates of  $\alpha/\beta$  and of  $\alpha^2/\beta$ ). This is a slightly more wasteful variant of the previous method.
- We could find the polynomial  $P(x) = a + bx + cx^2$  by thinking in terms of complex embeddings: for each  $\sigma : K \rightarrow \mathbb{C}$ , this polynomial must take  $\sigma(\alpha)$  to  $\sigma(\beta^{-1}) = \frac{1}{2\sigma(\alpha)^2 - 1}$ , so  $P(x)$  is the unique polynomial of degree 2 which takes  $z$  to  $\frac{1}{2z^2 - 1}$  for each root  $z$  of  $F(x)$ . The Lagrange interpolation formulas allow us to compute the coefficients  $a, b, c$ , of this polynomial, but only as approximations since we can only get approximations of these roots. Still, I thought I'd mention this method since it can shed a new light on the use of complex embeddings.

**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 (especially the warm-up exercise just below), 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 1.2: Warm up: review of methods

Let  $K = \mathbb{Q}(\sqrt{3})$ , and let  $\alpha = a + b\sqrt{3}$  ( $a, b \in \mathbb{Q}$ ) be an element of  $K$ . Express the trace, norm, and characteristic polynomial of  $\alpha$  (with respect to the extension  $K/\mathbb{Q}$ ) in terms of  $a$  and  $b$

1. by writing down the matrix of the multiplication-by- $\alpha$  map with respect to the  $\mathbb{Q}$ -basis of  $K$  of your choice,
2. by considering complex embeddings (*Hint:  $K = \mathbb{Q}(\alpha)$  where  $\alpha^2 = 3$* ).

*Remark: This exercise is meant as a warm up for the next exercises, so as to remind you that some computations can be done in different ways. In the other exercises, remember that depending on the situation, some methods require less efforts than others!*

### Solution 1.2:

1. Since  $x^2 - 3 \in \mathbb{Q}[x]$  is irreducible by Eisenstein at  $p = 3$ , we find that  $\sqrt{3}$  is algebraic over  $\mathbb{Q}$  of degree 2, so that  $(\sqrt{3})^0 = 1$  and  $(\sqrt{3})^1 = \sqrt{3}$  form a  $\mathbb{Q}$ -basis of  $K$ .

With respect to this basis, the matrix of the multiplication-by- $\alpha$  map is

$$M = \begin{pmatrix} a & 3b \\ b & a \end{pmatrix}$$

since  $\alpha \cdot 1 = a + b\sqrt{3}$  and  $\alpha \cdot \sqrt{3} = 3b + a\sqrt{3}$ , so that

$$\mathrm{Tr}_{\mathbb{Q}}^K(\alpha) = \mathrm{Tr} M = 2a,$$

$$N_{\mathbb{Q}}^K(\alpha) = \det M = a^2 - 3b^2,$$

$$\text{and } \chi_{\mathbb{Q}}^K(\alpha) = \chi_M = x^2 - 2ax + (a^2 - 3b^2).$$

2. Since  $\alpha$  is algebraic of degree 2, we have  $[K : \mathbb{Q}] = 2$ , so there are 2 embeddings of  $K$  into  $\mathbb{C}$ , which correspond to the complex roots of the minimal polynomial  $x^2 - 3$  of  $\alpha$  in that they send  $\alpha$  to the root they correspond to. Here, these complex roots are  $\pm\sqrt{3}$ , so one of the embeddings sends  $\alpha$  to  $\sqrt{3}$ , and the other one sends  $\alpha$  to  $-\sqrt{3}$ . As they are embeddings, they are also  $\mathbb{Q}$ -linear, so the first one sends  $\alpha$  to  $u = a + b\sqrt{3}$ , and the other one sends  $\alpha$  to  $v = a - b\sqrt{3}$  (so actually both these embeddings are actually embeddings in  $\mathbb{R} \subset \mathbb{C}$ ). As a result,

$$\mathrm{Tr}_{\mathbb{Q}}^K(\alpha) = u + v = 2a,$$

$$N_{\mathbb{Q}}^K(\alpha) = uv = a^2 - 3b^2,$$

$$\text{and } \chi_{\mathbb{Q}}^K(\alpha) = (x - u)(x - v) = x^2 - 2ax + (a^2 - 3b^2).$$

### Exercise 1.3: A biquadratic extension

1. Let  $K = \mathbb{Q}(\sqrt{2})$ . Prove that  $\sqrt{5} \notin K$ .
2. Let  $L = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ . Determine  $[L : \mathbb{Q}]$ , and find a  $\mathbb{Q}$ -basis of  $L$ .
3. What is the signature of  $L$ ?
4. Let  $\alpha = \sqrt{2} + \sqrt{5} \in L$ . Write down the matrix of

$$\begin{aligned} \mu_\alpha : L &\longrightarrow L \\ x &\longmapsto \alpha x \end{aligned}$$

with respect to the  $\mathbb{Q}$ -basis of  $L$  that you found in question 2.

5. Deduce the value of  $\text{Tr}_{\mathbb{Q}}^L(\alpha)$ .
6. Determine the norm  $N_{\mathbb{Q}}^L(\alpha)$  of  $\alpha$ .  
*Note: It is possible to do this without computing a big determinant.*
7. The characteristic polynomial  $\chi_{\mathbb{Q}}^L(\alpha)$  of  $\alpha$  turns out to be  $x^4 - 14x^2 + 9$  (we admit this without proof). Is it squarefree? What does this tell us about  $\alpha$ ?
8. Compute the characteristic polynomial  $\chi_K^L(\alpha)$  of  $\alpha$  with respect to the extension  $L/K$ .

### Solution 1.3:

1. The minimal polynomial of  $\sqrt{2}$  over  $\mathbb{Q}$  is  $x^2 - 2$ , because it is irreducible over  $\mathbb{Q}$  by Eisenstein. Therefore  $((\sqrt{2})^0 = 1, (\sqrt{2})^1 = \sqrt{2})$  is a  $\mathbb{Q}$ -basis of  $K$ . So if  $\sqrt{5} \in K$ , we would have (unique)  $a, b \in \mathbb{Q}$  such that  $\sqrt{5} = a + b\sqrt{2}$ . Squaring yields  $5 = (a^2 + 2b^2) + 2ab\sqrt{2} \in K$ . As  $(1, \sqrt{2})$  is a  $\mathbb{Q}$ -basis, we may conclude that  $a^2 + 2b^2 = 5$  and that  $2ab = 0$ , whence  $a = 0$  or  $b = 0$ . Neither alternative yields rational solutions to  $a^2 + 2b^2 = 5$ , whence a contradiction.
2. Because  $\sqrt{5} \notin K$ , the polynomial  $x^2 - 5 \in K[x]$  must be irreducible over  $K$  (else it would split into factors of degree 1 whence  $\pm\sqrt{5} \in K$ , absurd), so it is the minimal polynomial of  $\sqrt{5}$  over  $K$ . Therefore  $[L : K] = 2$ , and  $(1, \sqrt{5})$  is a  $K$ -basis of  $L$ . The tower law then shows that

$$[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}] = 2 \times 2 = 4,$$

and that

$$(1 \cdot 1, 1 \cdot \sqrt{2}, \sqrt{5} \cdot 1, \sqrt{5} \cdot \sqrt{2}) = (1, \sqrt{2}, \sqrt{5}, \sqrt{10})$$

is a  $\mathbb{Q}$ -basis of  $L$ .

3. We have  $L = \mathbb{Q}(\beta, \gamma)$  where  $\beta^2 = 2$  and  $\gamma^2 = 5$ . Therefore, if  $\sigma$  is one of the  $[L : \mathbb{Q}] = 4$  embeddings of  $L$  into  $\mathbb{C}$ , then  $\sigma(\beta)^2 = \sigma(\beta^2) = \sigma(2) = 2$  so  $\sigma(\beta) = \pm\sqrt{2} \in \mathbb{R}$ , and similarly  $\sigma(\gamma) = \pm\sqrt{5} \in \mathbb{R}$ . Besides  $\sigma$  must act as the identity on  $\mathbb{Q}$ , so either way  $\sigma(L) \subset \mathbb{R}$ . Therefore  $L$  is totally real and has signature  $(4, 0)$ .

4. We look at the effect of multiplying by  $\alpha$  on the elements of our basis. We find

- $\alpha \cdot 1 = \sqrt{2} + \sqrt{5}$ ,
- $\alpha \cdot \sqrt{2} = 2 + \sqrt{10}$ ,
- $\alpha \cdot \sqrt{5} = 5 + \sqrt{10}$ ,
- $\alpha \cdot \sqrt{10} = 5\sqrt{2} + 2\sqrt{5}$ ,

so the matrix is

$$\begin{pmatrix} 0 & 2 & 5 & 0 \\ 1 & 0 & 0 & 5 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

5.  $\text{Tr}_{\mathbb{Q}}^L(\alpha)$  is the trace of this matrix, which is clearly 0.

6. We use the transitivity of the norm to write  $N_{\mathbb{Q}}^L(\alpha) = N_{\mathbb{Q}}^K N_K^L(\alpha)$ . Now  $L = K(\sqrt{5}) = K(\beta)$  where  $\beta^2 = 5$ , so the  $[L : K] = 2$  embeddings of  $L$  into  $\mathbb{C}$  which restrict to the identity on  $K$  are characterised by  $\beta \mapsto \pm\sqrt{5}$ . In particular, they take  $\alpha = \sqrt{2} + \beta$  to  $\sqrt{2} \pm \sqrt{5}$ , whence

$$N_K^L(\alpha) = (\sqrt{2} + \sqrt{5})(\sqrt{2} - \sqrt{5}) = 2 - 5 = -3.$$

As a result,

$$N_{\mathbb{Q}}^L(\alpha) = N_{\mathbb{Q}}^K(3) = 3^2 = 9$$

(because multiplication  $\mu_3$  by 3 on  $K$  has a scalar matrix, or if you prefer, because the  $[K : \mathbb{Q}] = 2$  embeddings of  $K$  into  $\mathbb{C}$  must take 3 to 3 because  $3 \in \mathbb{Q}$ ).

7. We could determine if this polynomial is squarefree by computing its GCD with its derivative by successive Euclidian divisions, but this would be rather tedious. Instead, we can just notice from the logic of the previous question that the complex roots of this characteristic polynomial, which are the images of  $\alpha$  under the  $[L : \mathbb{Q}] = 4$  embeddings of  $L$  into  $\mathbb{C}$ , are the  $\pm\sqrt{2} \pm \sqrt{5}$ , which are distinct; therefore  $\chi_{\mathbb{Q}}^L(\alpha)$  is squarefree.

Now as  $\chi_{\mathbb{Q}}^L(\alpha)$  is always a power of the minimal polynomial  $m_{\alpha}$  of  $\alpha$ , it follows that actually  $\chi_{\mathbb{Q}}^L(\alpha) = m_{\alpha}$ . In particular,

$$[L : \mathbb{Q}(\alpha)] = \frac{[L : \mathbb{Q}]}{[\mathbb{Q}(\alpha) : \mathbb{Q}]} = \frac{\deg \chi_{\mathbb{Q}}^L(\alpha)}{\deg m_{\alpha}} = 1,$$

so  $L = \mathbb{Q}(\alpha)$ ; in other words,  $\alpha$  is a *primitive element* for  $L/\mathbb{Q}$ .

8. Again, two methods : matrix and complex embeddings. Here, both are reasonable, so we explain both.

Matrix: With respect to the  $K$ -basis  $1, \sqrt{5}$  of  $L$ , the matrix of the multiplication by  $\alpha$  is

$$\begin{pmatrix} \sqrt{2} & 5 \\ 1 & \sqrt{2} \end{pmatrix},$$

whose characteristic polynomial is

$$\chi_K^L(\alpha) = x^2 - 2\sqrt{2}x - 3.$$

Embeddings: As discussed in our answer to question 6, the  $[L : K] = 2$  embeddings of  $L$  into  $\mathbb{C}$  which restrict to the  $\sigma = \text{Id}$  on  $K$  take  $\alpha = \sqrt{2} + \beta$  to  $\sqrt{2} \pm \sqrt{5}$ , so

$$\chi_K^L(\alpha)^\sigma = (x - (\sqrt{2} + \sqrt{5}))(x - (\sqrt{2} - \sqrt{5})) = x^2 - 2\sqrt{2}x - 3.$$

To recover  $\chi_K^L(\alpha)$  from  $\chi_K^L(\alpha)^\sigma$ , we apply  $\sigma^{-1}$  to the coefficients and we find

$$\chi_K^L(\alpha) = x^2 - 2\sqrt{2}x - 3 \in K[x].$$

Just for completeness, here is what would happen if, for some obscure reason, we had picked  $\sigma$  such that  $\sigma(\sqrt{2}) = -\sqrt{2}$ : The embeddings of  $L$  that extend  $\sigma$  send  $\alpha$  to  $-\sqrt{2} \pm \sqrt{5}$ , so

$$\chi_K^L(\alpha)^\sigma = (x - (-\sqrt{2} + \sqrt{5}))(x - (-\sqrt{2} - \sqrt{5})) = x^2 + 2\sqrt{2}x - 3.$$

Applying  $\sigma^{-1}$  affects the coefficient of  $x$  nontrivially, and we find again that

$$\chi_K^L(\alpha) = x^2 - 2\sqrt{2}x - 3 \in K[x].$$

### Exercise 1.4: Computations in $\mathbb{Q}(\sqrt[3]{2})$

1. Prove that  $x^3 - 2$  is irreducible over  $\mathbb{Q}$ .
2. Let  $K = \mathbb{Q}(\sqrt[3]{2})$ , and let  $\alpha = \frac{\sqrt[3]{2}+1}{\sqrt[3]{2}-1} \in K$ . Find  $a, b, c \in \mathbb{Q}$  such that  $\alpha = a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2$ .
3. Are these rational numbers  $a, b, c$  unique ?
4. What is the degree of  $K$  over  $\mathbb{Q}$  ?
5. Prove that  $\sqrt{2} \notin K$ .  
*Hint: Think in terms of degrees.*
6. Prove that  $K = \mathbb{Q}(\alpha)$ .
7. Compute the trace, norm, and characteristic polynomial of  $\alpha$ .
8. What is the minimal polynomial of  $\alpha$  over  $\mathbb{Q}$ ?

### Solution 1.4:

1. This is because it is Eisenstein at  $p = 2$ . Alternatively, because it has degree 3, if it factored, it would have a factor of degree 1 and therefore a root, which it does not because the only possible roots are  $\pm 1$  and  $\pm 2$  by the rational root theorem, and none of those are actual roots.
2. Let us first express  $\frac{1}{\sqrt[3]{2}-1}$  as a polynomial in  $\sqrt[3]{2}$ . For this, we want to find polynomials  $U, V \in \mathbb{Q}[x]$  such that  $U(x)(x^3 - 2) + V(x)(x - 1) = 1$ ; indeed, evaluating at  $x = \sqrt[3]{2}$  will then yield  $V(\sqrt[3]{2})(\sqrt[3]{2} - 1) = 1$  (notice that this is a concrete example of the argument used in the proof of the fact that  $K[\alpha]$  is a field whenever  $\alpha$  is algebraic over  $K$ ).

To find  $U$  and  $V$ , we perform the Euclidian division of  $x^3 - 2$  by  $x - 1$ , which yields

$$x^3 - 2 = (x^2 + x + 1)(x - 1) - 1.$$

We may thus take  $U = -1$ ,  $V = x^2 + x + 1$ , and we find that

$$\frac{1}{\sqrt[3]{2}-1} = \sqrt[3]{2}^2 + \sqrt[3]{2} + 1.$$

Therefore,

$$\alpha = (\sqrt[3]{2} + 1)(\sqrt[3]{2}^2 + \sqrt[3]{2} + 1) = 2\sqrt[3]{2}^2 + 2\sqrt[3]{2} + 3,$$

we may thus take  $a = 3$ ,  $b = c = 2$ .

3. Yes. Indeed, since  $x^3 - 2$  is irreducible over  $\mathbb{Q}$ , it is the minimal polynomial of  $\sqrt[3]{2}$  over  $\mathbb{Q}$ , so  $1, \sqrt[3]{2}, \sqrt[3]{2}^2$  is a  $\mathbb{Q}$ -basis of  $K$ .
4. This degree is the same as the degree of the minimal polynomial of  $\sqrt[3]{2}$  over  $\mathbb{Q}$ , that is to say 3.
5. If we had  $\sqrt{2} \in K$ , then we would have  $\mathbb{Q}(\sqrt{2}) \subseteq K$ . But this would imply

$$3 = [K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2[K : \mathbb{Q}(\sqrt{2})],$$

which is impossible since  $[K : \mathbb{Q}(\sqrt{2})]$  is an integer.

6. (7 pts) If  $\alpha$  were rational, then writing  $\alpha = a + 0 \cdot \sqrt[3]{2} + 0 \cdot (\sqrt[3]{2})^2$  would contradict the unicity of the rationals  $a, b, c$ . So  $\alpha \notin \mathbb{Q}$ , and thus  $[\mathbb{Q}(\alpha) : \mathbb{Q}] > 1$ .

But we also have

$$3 = [K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}],$$

and since 3 is prime and  $[\mathbb{Q}(\alpha) : \mathbb{Q}] > 1$ , we must have  $[K : \mathbb{Q}(\alpha)] = 1$ , which means that  $\mathbb{Q}(\alpha) = K$ .

7. Using complex embeddings would lead us to computing with both  $\sqrt[3]{2}$  and  $e^{2\pi i/3}$ , which sounds really tedious, so instead we compute that the matrix of the multiplication-by- $\alpha$  map with respect to the  $\mathbb{Q}$ -base  $1, \sqrt[3]{2}, \sqrt[3]{2}^2$  of  $K$ , which turns out to be

$$\begin{pmatrix} 3 & 4 & 4 \\ 2 & 3 & 4 \\ 2 & 2 & 3 \end{pmatrix}.$$

We then compute  $\chi_{\mathbb{Q}}^K(\alpha)$  as the characteristic polynomial of this matrix; after some effort, we find

$$\chi_{\mathbb{Q}}^K(\alpha) = x^3 - 9x^2 + 3x - 3.$$

From the coefficients of  $x^2$  and  $x^0$  respectively, we finally deduce that  $\text{Tr}_{\mathbb{Q}}^K(\alpha) = 9$  and that  $N_{\mathbb{Q}}^K(\alpha) = 3$ .

8. Since  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [K : \mathbb{Q}] = 3$  by the previous questions, the degree of the minimal polynomial of  $\alpha$  over  $\mathbb{Q}$  is 3. But  $\chi_{\mathbb{Q}}^K(\alpha) = x^3 - 9x^2 + 3x - 3$  has degree 3, kills  $\alpha$ , and is monic, so it *is* the minimal polynomial of  $\alpha$  over  $\mathbb{Q}$ . (Remember that in general, the characteristic polynomial is a power of the minimal polynomial).

### Exercise 1.5: Resultant practice

1. Let  $\gamma = \sqrt{3} - \sqrt[3]{2}$ . Express a non-zero polynomial in  $\mathbb{Q}[x]$  vanishing at  $\gamma$  as a resultant, and then express this resultant as a determinant.

*You are not required to compute this determinant explicitly. All this questions asks is to express this polynomial as a resultant, and then as a determinant, but you are not required to compute this polynomial explicitly.*

2. Let  $K = \mathbb{Q}(\alpha)$  be a number field, let  $A(x) \in \mathbb{Q}[x]$  be the minimal polynomial of  $\alpha$ , and let  $\beta = B(\alpha) \in K$ , where  $B(x) \in \mathbb{Q}[x]$  is some polynomial. Express the characteristic polynomial  $\chi_{\mathbb{Q}}^K(\beta)$  of  $\beta$  in terms of a resultant involving  $A$  and  $B$ .

*Hint: Think in terms of complex embeddings.*

### Solution 1.5:

1.  $\alpha = \sqrt[3]{2}$  is killed by  $A(x) = x^3 - 2$ , and  $\beta = \sqrt{3}$  is killed by  $x^2 - 3$ . (These are in fact minimal polynomials, but it does not matter here.) Therefore, a polynomial killing  $\gamma = \beta - \alpha$  is

$$C(x) = \prod_{\substack{a \in \mathbb{C} \\ A(a)=0}} B(x+a) = \text{Res}_y (A(y), B(x+y)).$$

Since the coefficients of  $B(x + y) = (x + y)^2 - 3 = y^2 + 2xy + x^2 - 3$  are  $(1, 2x, x^2 - 3)$  when seen as a polynomial in  $y$ , we have

$$C(x) = \begin{vmatrix} 1 & 0 & 0 & -2 & 0 \\ 0 & 1 & 0 & 0 & -2 \\ 1 & 2x & x^2 - 3 & 0 & 0 \\ 0 & 1 & 2x & x^2 - 3 & 0 \\ 0 & 0 & 1 & 2x & x^2 - 3 \end{vmatrix}.$$

*Remark: Although the exercise explicitly said you did not have to do it, this evaluates to  $x^6 - 9x^4 + 4x^3 + 27x^2 + 36x - 23$ , if you wanted to know. In fact this is irreducible over  $\mathbb{Q}$  (I checked on a computer that it is irreducible mod 7), so this is the minimal polynomial of  $\gamma$  over  $\mathbb{Q}$ .*

2. Let  $\Sigma$  be the set of embeddings of  $K$  into  $\mathbb{C}$ . When  $\sigma$  ranges over  $\Sigma$ ,  $\sigma(\alpha)$  ranges over the complex roots of  $A(x)$ , so that

$$\begin{aligned} \chi_{\mathbb{Q}}^K(\beta) &= \prod_{\sigma \in \Sigma} (x - \sigma(\beta)) \\ &= \prod_{\sigma \in \Sigma} (x - \sigma(B(\alpha))) \\ &= \prod_{\sigma \in \Sigma} (x - B(\sigma(\alpha))) \\ &= \prod_{\substack{\alpha \in \mathbb{C} \\ A(\alpha)=0}} (x - B(\alpha)) \\ &= \text{Res}_y (A(y), x - B(y)). \end{aligned}$$

*Remark: Algorithmically speaking, this is in general the fastest way to compute characteristic polynomials.*

### Exercise 1.6: (Non)-repeated values of complex embeddings

Let  $K$  be a number field of degree  $n = [K : \mathbb{Q}]$ , fix  $\alpha \in K$ , and let  $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ .

Prove that  $\alpha$  is a primitive element for  $K/\mathbb{Q}$  if and only if the values  $\{\sigma(\alpha), \sigma \in \text{Hom}(K, \mathbb{C})\}$  are all distinct.

More generally (without assuming that  $\alpha$  is a primitive element), relate the values  $\{\sigma(\alpha), \sigma \in \text{Hom}(K, \mathbb{C})\}$  to the roots of the characteristic polynomial and of the minimal polynomial of  $\alpha$ . How many times is each value  $\sigma(\alpha)$  repeated in  $\{\sigma(\alpha), \sigma \in \text{Hom}(K, \mathbb{C})\}$ ?

### Solution 1.6:

Let  $m_{\alpha}$  and  $\chi_{\alpha}$  be the minimal and characteristic polynomials of  $\alpha$ , respectively. We know that  $\deg m_{\alpha} = d$  and that  $\deg \chi_{\alpha} = n$ ; besides  $\chi_{\alpha}$  is a power of  $m_{\alpha}$ , so necessarily  $\chi_{\alpha} = m_{\alpha}^{n/d}$  by considering the degrees.

Therefore, if  $\alpha$  is a primitive element, then  $\mathbb{Q}(\alpha) = K$  so  $d = n$  so  $\chi_{\alpha} = m_{\alpha}$  is irreducible and therefore has no repeated roots. Conversely, if  $\chi_{\alpha} = m_{\alpha}^{n/d}$  has no

repeated roots, then  $n/d = 1$ , so  $[K : \mathbb{Q}(\alpha)] = [K : \mathbb{Q}]/[\mathbb{Q}(\alpha) : \mathbb{Q}] = n/d = 1$ , so  $K = \mathbb{Q}(\alpha)$ , so  $\alpha$  is a primitive element.

In general, we know that

$$\chi_\alpha = \prod_{\sigma: K \hookrightarrow \mathbb{C}} (x - \sigma(\alpha)),$$

so the roots of  $\chi_\alpha$  are the  $\sigma(\alpha)$  counted **with** multiplicity.

In contrast, the roots of  $m_\alpha$  are the  $\sigma(\alpha)$  counted **without** multiplicity. To see why, first notice that  $m_\alpha$  has no repeated roots, as it is irreducible; therefore all we have to show is that a complex number is a root of  $m_\alpha$  if and only if it is of the form  $\sigma(\alpha)$  for some  $\sigma : K \hookrightarrow \mathbb{C}$ . And indeed, first of all that the  $\sigma(\alpha)$  are roots of  $m_\alpha$  since  $0 = \sigma(0) = \sigma(m_\alpha(\alpha)) = m_\alpha(\sigma(\alpha))$ , and conversely, if  $z \in \mathbb{C}$  is a root of  $m_\alpha$ , then there exists an embedding  $\tau$  of  $\mathbb{Q}(\alpha) \simeq \mathbb{Q}[x]/(m_\alpha)$  that takes  $\alpha$  to  $z$ , and this  $\tau$  extends (in exactly  $[L : \mathbb{Q}(\alpha)] = n/d$  ways) to  $K$ , so that there does exist a  $\sigma : K \hookrightarrow \mathbb{C}$  (and in fact  $n/d$  of them) such that  $\sigma(\alpha) = z$ .

This logic also shows that the quantity  $\sigma(\alpha)$  assumes  $d = \deg m_\alpha$  distinct values as  $\sigma$  ranges over  $\text{Hom}(K, \mathbb{C})$ , each value being repeated  $n/d$  times. This is also visible on the identity

$$\prod_{\sigma: K \hookrightarrow \mathbb{C}} (x - \sigma(\alpha)) = \chi_\alpha = m_\alpha^{n/d}.$$

The case  $d = n$  corresponds to the special case where  $\alpha$  is a primitive element (so in  $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq K$ , the **right** inclusion is an equality). The other extreme case is  $d = 1$ , which happens iff.  $\alpha \in \mathbb{Q}$  (meaning that in  $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq K$ , the **left** inclusion is an equality), in which case  $m_\alpha = x - \alpha$  and  $\chi_\alpha = (x - \alpha)^n = m_\alpha^{n/1}$ .