Algebraic number theory

Nicolas Mascot (n.a.v.mascot@warwick.ac.uk),
Aurel Page (a.r.page@warwick.ac.uk)
TAs: Chris Birkbeck (c.d.birkbeck@warwick.ac.uk),

George Turcas(g.c.turcas@warwick.ac.uk)

Version: February 20, 2017

Reminder: $\operatorname{disc}(x^n+bx+c) = (-1)^{n(n-1)/2}\big((1-n)^{n-1}b^n + n^n c^{n-1}\big)$.

Exercise 1 (10 points)

Is $\dfrac{3-2\sqrt{6}}{\sqrt{6}+2}$ *an algebraic integer ?*

Let us first express this number as a polynomial in $\sqrt{6}$. In principle, we should use the $U(x)A(x)+B(x)V(x)=1$ as in exercise 1 of sheet 1 for that, but here we are in degree only 2, so we can just apply the good old "conjugate expression" trick:

$$\frac{3-2\sqrt{6}}{\sqrt{6}+2} = \frac{(3-2\sqrt{6})(-\sqrt{6}+2)}{(\sqrt{6}+2)(-\sqrt{6}+2)} = \frac{-3\sqrt{6}+6+2(\sqrt{6})^2-4\sqrt{6}}{2^2-(\sqrt{6})^2} = -9+\frac{7}{2}\sqrt{6}.$$

Now, there are (at least) two ways to conclude:

- As $\sqrt{6}$ is algebraic of degree 2 over $\mathbb{Q}$, every element of $\mathbb{Q}(\sqrt{6})$ can be written *uniquely* as $a+b\sqrt{6}$ with $a,b\in\mathbb{Q}$; besides, 6 is squarefree and $6 \not\equiv 1 \bmod 4$ so the ring of integers is $\mathbb{Z}[\sqrt{6}]$, in other words, an element $a+b\sqrt{6}$ is an algebraic integer if and only if a and b are both integers. This is not the case for $-9+\frac{7}{2}\sqrt{6}$, so it is NOT al algebraic integer.
- The characteristic polynomial of this number (with respect to the extension $\mathbb{Q}(\sqrt{6})/\mathbb{Q}$) is

$$\left(x-\left(-9+\frac{7}{2}\sqrt{6}\right)\right)\left(x-\left(-9-\frac{7}{2}\sqrt{6}\right)\right) = x^2-18x+\frac{15}{2}$$

  (because of complex embeddings; we could also have written down the matrix of course). This does not lie in $\mathbb{Z}[x]$, so this number is NOT an algebraic integer.

Exercise 2 (40 points)

Let $f(x) = x^3 - x - 1$.

1. *The aim of this question is to prove that $f(x)$ is irreducible over $\mathbb{Q}$.*

   (a) (5 points) *Prove that if $f(x)$ were reducible, then it would have a rational root.*

   That's because the degree of f is only 3: if it factored, it would have either one factor of degree 1 and one of degree 2, or 3 factors of degree 1 (possibly not all distinct); anyway, it would have at least one factor of degree 1.

   (b) (10 points) *Prove that this root would in fact be an integer by using the notion of algebraic integer.*

   Let β be this hypothetic root. Then $\beta \in \mathbb{Q}$ by construction; besides, β is a root of $f(x)$ which is a *monic* polynomial with coefficients in $\mathbb{Z}$, so β is also an algebraic integer. As a result, $\beta \in \mathbb{Z}$.

   (c) (5 points) *Prove that this root could only be ± 1, and conclude that $f(x)$ is irreducible over $\mathbb{Q}$.*

   From $f(\beta) = 0$, we infer that $\beta(\beta^2 - 1) = 1$, so β divides 1. But neither 1 nor -1 is a root of $f(x)$, so by contradiction we deduce that $f(x)$ is irreducible over $\mathbb{Q}$.

2. (5 points) *Compute the discriminant of $f(x)$.*

   From the formula $\operatorname{disc}(x^3 + bx + c) = -4b^3 - 27c^2$, we find that

$$\operatorname{disc} f = -23.$$

3. (15 points) *Let α be a root of $f(x)$. Compute the ring of integers of $\mathbb{Q}(\alpha)$.*

   Let $K = \mathbb{Q}(\alpha)$. Since α is both an algebraic integer and a primitive element for K, $\mathbb{Z}[\alpha]$ is an order in K. The discriminant of this order is $\operatorname{disc} f$, which is -23 by the previous question. So we have

$$-23 = m^2 \operatorname{disc} K,$$

   where $m = [\mathbb{Z}_K : \mathbb{Z}[\alpha]] \in \mathbb{N}$ is the index of the order $\mathbb{Z}[\alpha]$. Since -23 is squarefree, we must have $m = 1$, so $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ (and also $\operatorname{disc} K = -23$).

Exercise 3 (50 points)

Let $f(x) = x^4 - 2x + 4$, which you may assume without proof is irreducible over $\mathbb{Q}$, and let $K = \mathbb{Q}(\alpha)$, where α satisfies $f(\alpha) = 0$.

1. (10 points) *Compute and factor the discriminant of $\mathbb{Z}[\alpha]$.*

   Hint: $2^{10} - 3^3 = 997$ is prime.

   We know that $\operatorname{disc} \mathbb{Z}[\alpha] = \operatorname{disc} f$, and according to the formula

   $$\operatorname{disc}(x^n + bx + c) = (-1)^{n(n-1)/2}\big((1-n)^{n-1}b^n + n^n c^{n-1}\big),$$

   we have

   $$\operatorname{disc} \mathbb{Z}[\alpha] = +(-3^3 \cdot 2^4 + 4^4 \cdot 4^3) = 2^{14} - 3^3 \cdot 2^4 = 2^4 \cdot (2^{10} - 3^3) = 2^4 \cdot 997.$$

2. (12 points) *At this point, what are the possibilities for* $\operatorname{disc} K$*, and the corresponding values of the index of $\mathbb{Z}[\alpha]$?*

   We know that

   $$\operatorname{disc} \mathbb{Z}[\alpha] = m^2 \operatorname{disc} K,$$

   where m is the index of $\mathbb{Z}[\alpha]$. Since 997 is prime, this leaves 3 possibilities:

   - Either $m = 1$ (which means that $\mathbb{Z}_K = \mathbb{Z}[\alpha]$), and so $\operatorname{disc} K = 2^4 \cdot 997$,
   - or $m = 2$ (so $\mathbb{Z}[\alpha]$ is not 2-maximal, but is p-maximal for all primes $p \neq 2$), and $\operatorname{disc} K = 2^2 \cdot 997$,
   - or $m = 2^2$ (so again $\mathbb{Z}[\alpha]$ is not 2-maximal, but is p-maximal for all primes $p \neq 2$), and $\operatorname{disc} K = 997$.

   In the last two cases, the fact that $\mathbb{Z}[\alpha]$ is not 2-maximal would imply that the elements of $\mathbb{Z}_K$ would in general have denominators which are powers of 2 when we write then as polynomial of degree $< 4 = \deg f$ in α. In the first case, the elements of $\mathbb{Z}_K$ would have no denominators at all.

3. (4 points) *Let $\beta = \frac{\alpha^3}{2} \in K$, and consider the lattice $\mathcal{O} \subset K$ with $\mathbb{Z}$-basis*

   $$1, \alpha, \alpha^2, \beta.$$

   Prove that $\mathcal{O}$ is stable under multiplication by β.

   Hint: what is $\beta \cdot \alpha$?.

   We have $\mathcal{O} = \{a + b\alpha + c\alpha^2 + d\beta,\ a, b, c, d \in \mathbb{Z}\}$.

   The relation $f(\alpha) = 0$ yields $\alpha^4 = 2\alpha - 4$, whence $\beta \cdot \alpha = \alpha - 2 \in \mathcal{O}$. Similarly, we find that $\beta \cdot \alpha^2 \in \mathcal{O}$, $\beta \cdot \beta \in \mathcal{O}$, and of course $\beta \cdot 1 \in \mathcal{O}$. Therefore,

   $$\beta \cdot (a + b\alpha + c\alpha^2 + d\beta) = a\beta \cdot 1 + b\beta \cdot \alpha + c\beta \cdot \alpha^2 + d\beta \cdot \beta \in \mathcal{O}$$

   as soon as $a, b, c, d \in \mathbb{Z}$, so $\beta \cdot \mathcal{O} \subset \mathcal{O}$.

4. (6 points) *Deduce that β is an algebraic integer.*

   Multiplication by β stabilises a lattice, so β is an algebraic integer (Recall the proof: we can write down the matrix of multiplication by β w.r.t. a $\mathbb{Z}$-basis of $\mathcal{O}$, and this matrix will have coefficients in $\mathbb{Z}$ since $\beta \cdot \mathcal{O} \subset \mathcal{O}$, so the characteristic polynomial of β lies in $\mathbb{Z}[x]$).

5. (2 points) *Which of the possibilities listed in question 2. remain ?*

   We have just seen that $\beta \in \mathbb{Z}_K$, but $\beta \notin \mathbb{Z}[\alpha]$ (because $\mathbb{Z}[\alpha] = \{a + b\alpha + c\alpha^2 + d\alpha^3,\ a, b, c, d \in \mathbb{Z}\}$ since α is an algebraic integer), so $\mathbb{Z}_K \neq \mathbb{Z}[\alpha]$. So only the second and third possibilities remain.

   Alternative, quicker proof : $\beta = \alpha^3/2 \in \mathbb{Z}_K$ has a denominator divisible by the prime 2, so $\mathbb{Z}[\alpha]$ is not 2-maximal.

6. (6 points) *Prove that $\mathcal{O}$ is an order in K.*

   Hint: Prove that $\mathcal{O}$ is also stable under multiplication by α.

   We find that $\alpha \cdot 1$, $\alpha \cdot \alpha$, $\alpha \cdot \alpha^2$ and $\alpha \cdot \beta$ all lie in $\mathcal{O}$, which as in question 3. proves that $\mathcal{O}$ is stable under multiplication by α. It is therefore also stable under multiplication by α^2, and also by β by question 3., and of course also by 1. Therefore, $\mathcal{O}$ is stable under multiplication by any $\mathbb{Z}$-linear combination of $1, \alpha, \alpha^2$ and β, i.e. $\mathcal{O} \cdot \mathcal{O} \subset \mathcal{O}$. As $1 \in \mathcal{O}$, this proves that $\mathcal{O}$ is a subring of K. By construction, $\mathcal{O}$ is also a lattice in K, so it is an order in K.

7. (10 points) *It turns out that $\mathbb{Z}_K = \mathcal{O}$. Give the discriminant of K in factored form.*

   Thanks to the relation
   $$\operatorname{disc} \mathbb{Z}[\alpha] = m^2 \operatorname{disc} K,$$
   finding $\operatorname{disc} K$ amounts to computing the index m of $\mathbb{Z}[\alpha]$ in $\mathbb{Z}_K = \mathcal{O}$. We do so by writing a change-of-basis matrix between a $\mathbb{Z}$-basis of $\mathcal{O}$ and a $\mathbb{Z}$-basis of $\mathbb{Z}[\alpha]$.

   A $\mathbb{Z}$-basis of $\mathcal{O}$ is $1, \alpha, \alpha^2, \beta = \alpha^3/2$, and a $\mathbb{Z}$-basis of $\mathbb{Z}[\alpha]$ is $1, \alpha, \alpha^2, \alpha^3$ since α is an algebraic integer of degree $4 = \deg f$. (Technically we could use any $\mathbb{Z}$ bases, but why make things complicated ?). The matrix expressing the latter in terms of the former is
   $$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix},$$
   whose determinant is clearly 2, so the index is
   $$m \overset{\text{def}}{=} [\mathcal{O} : \mathbb{Z}[\alpha]] = 2.$$

   Therefore, we are in the second of the three cases listed in question 2., so
   $$\operatorname{disc} K = 2^2 \cdot 997.$$

In conclusion, the factor 2^4 of disc $\mathbb{Z}[\alpha]$ actually came *both* from disc K and from the index !

Note that we could also have expressed $1, \alpha, \alpha^2, \beta = \alpha^3/2$ in terms of $1, \alpha, \alpha^2, \alpha^3$; this would lead us to the inverse change-of-basis matrix

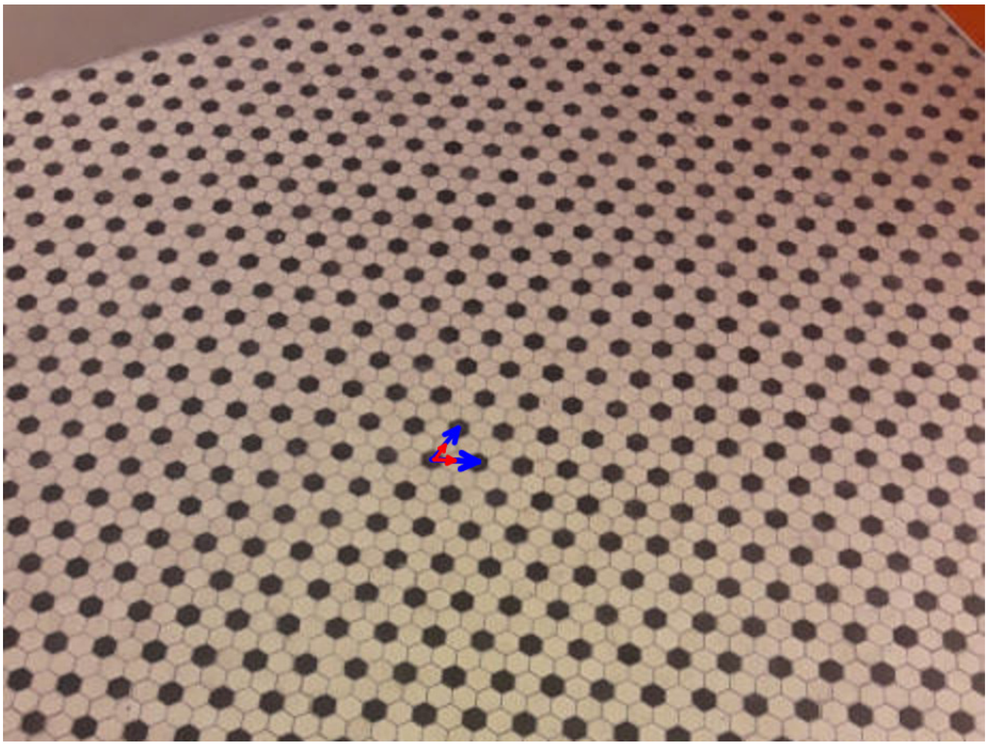
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{pmatrix}$$

whose determinant is (up to sign) the inverse of the index. Doing things this way is sometimes easier. Also, don't worry if you can't remember if you should express this basis in terms of that basis, or the other way round: you'll either get a matrix with integer coefficients, whose determinant is (up to sign) the index, or a matrix with rational coefficients, whose determinant is (up to sign) the inverse of the index, and since the index is an integer, the result that you get will tell you which case you are in !

UNASSESSED QUESTIONS

Exercise 4

1. *In the picture below, the centre of the hexagonal floor tiles (both black and white ones) form a lattice, and the centre of the black tiles form a sublattice. Compute the index of this sublattice by writing down a change-of-basis matrix. What is the proportion of black tiles ?*

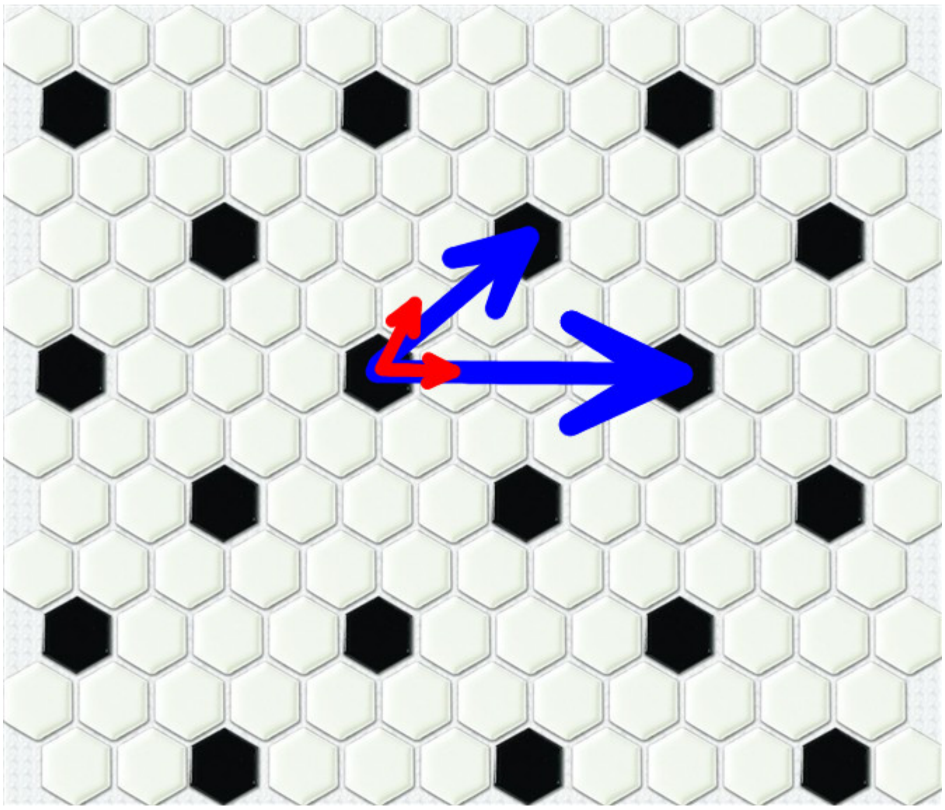


Let us choose a $\mathbb{Z}$-basis (in red) for the whole lattice, and another (in blue) for the black sublattice, as shown on the picture. The change-of-basis matrix expressing the blue vectors in terms of the red ones is

$$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix},$$

whose determinant is 4, so the index is 4. In other words, 1 out of 4 tiles is black.

2. *Same questions for this other tiling pattern.*



Let us choose again $\mathbb{Z}$-basis (in red) for the whole lattice, and another (in blue) for the black sublattice. This time, the change-of-basis matrix looks like

$$\begin{pmatrix} 4 & 1 \\ 0 & 2 \end{pmatrix}$$

(depending on how you order the bases). The determinant is 8, so the index is 8. In other words, 1 out of 8 tiles is black.