B3.4 Algebraic Number Theory

Sheet 2 — HT24

Section A

1. Suppose that α is an algebraic integer of degree n, with monic minimal polynomial $m_\alpha \in \mathbf{Z}[X]$. Let $K = \mathbf{Q}(\alpha)$. Show that

$$\mathrm{disc}_{K/\mathbf{Q}}(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{n(n-1)/2} N_{K/\mathbf{Q}}(m'_\alpha(\alpha)),$$

where m'_α denotes the derivative. Using this, compute $\mathrm{disc}_{K/\mathbf{Q}}(1, \alpha, \alpha^2)$, where $K = \mathbf{Q}(\alpha)$ with $\alpha = 2^{1/3}$.

Solution: We have already observed in the course that

$$\mathrm{disc}_{K/\mathbf{Q}}(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{i<j} (\sigma_i(\alpha) - \sigma_j(\alpha))^2, \tag{1}$$

where the $\sigma_i : K \to \mathbf{C}$ are the embeddings of K. On the other hand,

$$m_\alpha(X) = \prod_i (X - \sigma_i(\alpha)),$$

and so

$$m'_\alpha(X) = \sum_j \prod_{i \neq j} (X - \sigma_i(\alpha)).$$

In particular,

$$m'_\alpha(\sigma_j(\alpha)) = \prod_{i \neq j} (\sigma_j(\alpha) - \sigma_i(\alpha)),$$

and so

$$N_{K/\mathbf{Q}}(m'_\alpha(\alpha)) = \prod_j m'_\alpha(\sigma_j(\alpha)) = \prod_j \prod_{i \neq j} (\sigma_j(\alpha) - \sigma_i(\alpha)). \tag{2}$$

This is clearly equal to the expression in (1) up to a sign, and a moment's thought shows that the sign is indeed $(-1)^{n(n-1)/2}$: to go from (2) to (1), one needs to switch the sign of the $n(n-1)/2$ pairs with $i > j$.

In the example (which, one should remark, also appeared on the first sheet), $n = 3$ and $m_\alpha(X) = X^3 - 2$, hence $m'_\alpha(\alpha) = 3\alpha^2$. Thus $N_{K/\mathbf{Q}}(m'_\alpha(\alpha)) = 3^3 N_{K/\mathbf{Q}}(\alpha)^2 = 3^3 2^2$. Thus we obtain $\mathrm{disc}_{K/\mathbf{Q}}(1, \alpha, \alpha^2) = -108$, which agrees with the answer on Sheet 1.

Ben Green: ben.green@maths.ox.ac.uk

Section B

The first five questions of Section B are related and discuss the cyclotomic field $K = \mathbf{Q}(\zeta_p)$, where $\zeta_p := e^{2\pi i/p}$ and p is an odd prime.

2. Show that the degree $[K : \mathbf{Q}]$ is $p - 1$.

Solution: $X^p - 1$ is not irreducible, since it factors as $(X - 1)f(X)$, where $f(X) := X^{p-1} + X^{p-2} + \cdots + 1$. This *is* irreducible by Eisenstein's criterion. Indeed,

$$f(X+1) = \frac{(X+1)^p - 1}{X} = \sum_{n=0}^{p-1} a_n X^n,$$

with $a_n := \binom{p}{n+1}$, and so $p \nmid a_{p-1}$, whilst $p \mid a_1, \dots, a_{p-2}$, but $p^2 \nmid a_0$.

3. Evaluate $N_{K/\mathbf{Q}}(1 - \zeta)$.

Solution: We have the factorisation

$$f(X) = \prod_{i=1}^{p-1} (X - \zeta^i),$$

since all the ζ^i are roots of $X^p - 1 = 0$ (but not of $X - 1 = 0$) and they are distinct. Since f is irreducible, the conjugates of ζ are precisely these numbers ζ^i for $i = 1, \dots, p - 1$. Therefore

$$N_{K/\mathbf{Q}}(1 - \zeta) = \prod_{i=1}^{p-1} (1 - \zeta^i) = f(1) = p.$$

4. Show that $\frac{1}{p}(\zeta - 1)^{p-1}$ is an algebraic integer.

Solution: We have the binomial expansion

$$1 = 1^p = (1 + (\zeta - 1))^p = (\zeta - 1)^p + \binom{p}{1}(\zeta - 1)^{p-1} + \cdots + \binom{p}{p-1}(\zeta - 1) + 1.$$

Therefore

$$\frac{1}{p}(\zeta - 1)^{p-1} = -\frac{1}{p} \sum_{i=0}^{p-1} \binom{p}{i} (\zeta - 1)^{p-i-1},$$

and the right-hand side is an integer since all the binomial coefficients are divisible by p.

Ben Green: ben.green@maths.ox.ac.uk

5. Evaluate $\operatorname{disc}_{K/\mathbf{Q}}(1, \zeta, \dots, \zeta^{p-2})$. (*Hint: you may want to use Question 1 and the answer to Question 3.*)

Solution: The answer is $(-1)^{(p-1)/2} p^{p-2}$. We apply Question 1. Note that $f = m_\zeta$ is the minimal polynomial of ζ, thus it suffices to show (since p is odd) that

$$N_{K/\mathbf{Q}}(f'(\zeta)) = p^{p-2}. \tag{3}$$

Here, we noted that $(-1)^{(p-1)(p-2)/2}$, the quantity which features in Question 1, is equal to $(-1)^{(p-1)/2}$, since p is odd. By the quotient rule for derivatives,

$$f(X) = \frac{(X-1)pX^{p-1} - (X^p - 1)}{(X-1)^2}.$$

Evaluating at $X = \zeta$, we obtain

$$f'(\zeta) = \frac{-p\zeta^{p-1}}{1-\zeta}.$$

Now we have

$$N_{K/\mathbf{Q}}(-p) = (-p)^{p-1},$$

$$N_{K/\mathbf{Q}}(\zeta) = 1$$

and, by Question 3,

$$N_{K/\mathbf{Q}}(1-\zeta) = p.$$

The claim (3) follows immediately.

6. (i) Suppose that $c_0, c_1, \dots, c_{p-2}$ are integers and that

$$\frac{1}{p}(c_0 + c_1(\zeta - 1) + \cdots + c_{p-2}(\zeta-1)^{p-2}) \in \mathcal{O}_K.$$

Show that all the c_i are divisible by p. (*Hint: suppose not, and let r be minimal such that $p \nmid c_r$. You may wish to recall Questions 3 and 4.*)

(ii) Show that $1, \zeta, \dots, \zeta^{p-2}$ is an integral basis for $\mathcal{O}_K$.

Solution: (i) Suppose not, and that r is minimal such that $p \nmid c_r$. Subtracting off elements of $\mathbf{Z}[\zeta - 1]$, we have

$$\alpha := \frac{1}{p}(c_r(\zeta-1)^r + \cdots + c_{p-1}(\zeta-1)^{p-1}) \in \mathcal{O}_K. \tag{4}$$

Now use the result of Question 4, that is to say

$$\frac{1}{p}(\zeta-1)^{p-1} \in \mathcal{O}_K.$$

Ben Green: ben.green@maths.ox.ac.uk

Thus, multiplying (4) through by $(\zeta-1)^{p-2-r}$, we see that

$$\frac{1}{p}c_r(\zeta-1)^{p-2}\in\mathcal{O}_K.$$

However by Question 3 the norm of the left-hand side is c_r^{p-1}/p. This is not an integer, and so we get a contradiction.

(ii) A slick way to proceed here is notice that $m_{\zeta-1}(X)=m_\zeta(X+1)$, and so $m'_{\zeta-1}(\zeta-1)=m'_\zeta(\zeta)$, and so by Questions 1 and 5,

$$\begin{aligned}\mathrm{disc}_{K/\mathbf{Q}}(1,(\zeta-1),(\zeta-1)^2,\dots,(\zeta-1)^{p-2}) &= \mathrm{disc}_{K/\mathbf{Q}}(1,\zeta,\dots,\zeta^{p-2})\\ &= (-1)^{(p-1)/2}p^{p-2}.\end{aligned}\tag{5}$$

Since p is the only prime dividing this discriminant, a result from lectures shows that any element of $\mathcal{O}_K$ is of the form $\frac{1}{p}(c_r(\zeta-1)^r+\cdots+c_{p-1}(\zeta-1)^{p-1})$, and hence by part (i) of the question lies in $\mathbf{Z}[\zeta-1]$, which is contained in $\mathbf{Z}[\zeta]$.

An alternative way to proceed (the one I originally had in mind) is to note that

$$\mathbf{Z}[\zeta-1]=\mathbf{Z}[\zeta].\tag{6}$$

This is true because, for any algebraic integer t, $\mathbf{Z}[t\pm1]\subseteq\mathbf{Z}[t]$, by binomial expansion of each power $(t\pm1)^i$. Applying this with $t=\zeta-1$ and the $+$ sign gives $\mathbf{Z}[\zeta]\subseteq\mathbf{Z}[\zeta-1]$, and applying it with $t=\zeta$ and the $-$ sign gives the opposite inclusion $\mathbf{Z}[\zeta-1]\subseteq\mathbf{Z}[\zeta]$.

Now, by lectures and Question 5, any element $x\in\mathcal{O}_K$ lies in $\frac{1}{p}\mathbf{Z}[\zeta]$, and hence by (6) lies in $\frac{1}{p}\mathbf{Z}[\zeta-1]$. By part (i) of the question, x therefore lies in $\mathbf{Z}[\zeta-1]$, and so finally by (6) again, we have $x\in\mathbf{Z}[\zeta]$.

7. Let K be a number field. We say that K is *norm-Euclidean* if $\mathcal{O}_K$ is a Euclidean domain with respect to the norm function: that is, given $a,b\in\mathcal{O}_K\setminus\{0\}$ we may find $q,r\in\mathcal{O}_K$ such that $a=qb+r$ with $|N_{K/\mathbf{Q}}(r)|<|N_{K/\mathbf{Q}}(b)|$.
   (i) Show that a norm Euclidean domain is a principal ideal domain.
   (ii) Let $K=\mathbf{Q}(\sqrt{-7})$. Show that K is norm-Euclidean.

Solution: (i) A norm Euclidean domain is clearly a Euclidean domain, so this ought to be just revision from rings and modules. Let's recall the argument: let $\mathfrak{a}$ be an ideal, and let $\alpha\in\mathfrak{a}\setminus\{0\}$ have $|N_{K/\mathbf{Q}}(\alpha)|$ minimal. Let $\beta\in\mathfrak{a}$. We have $\beta=q\alpha+r$ with $q,r\in\mathcal{O}_K$ and $|N_{K/\mathbf{Q}}(r)|<|N_{K/\mathbf{Q}}(\beta)|$. Clearly $r\in\mathfrak{a}$. By minimality, $r=0$, and therefore $\beta\in(\alpha)$.

Ben Green: ben.green@maths.ox.ac.uk

(ii) Let $x = \frac{a}{b} \in K$. We need only show that there is $q \in \mathcal{O}_K$ such that $|N_{K/\mathbf{Q}}(x-q)| < 1$. Set $\theta := \frac{1+\sqrt{-7}}{2}$, so by results of the course $\mathcal{O}_K = \mathbf{Z}[\theta]$ (since $-7 \equiv 1 \pmod 4$). Write $x = u + \theta v$; we look for $q = m + \theta n$, with $m, n \in \mathbf{Z}$. We may compute

$$N_{K/\mathbf{Q}}(x-q) = (u + \frac{1}{2}v - m - \frac{1}{2}n)^2 + 7(\frac{v-n}{2})^2. \tag{7}$$

There is some value of n such that $|v - n| \leqslant \frac{1}{2}$, so the second term is $\leqslant \frac{7}{16}$. Then, there is some value of m such that $|u + \frac{1}{2}v - m - \frac{1}{2}n| \leqslant \frac{1}{2}$, so the first term in (7) is at most $\frac{1}{4}$. The result follows since $\frac{1}{4} + \frac{7}{16} < 1$.

8. Let $K = \mathbf{Q}(\sqrt{-p})$, where p is a prime congruent to $1 \pmod 4$. By considering factorisations of 2, or otherwise, show that $\mathcal{O}_K$ is not a principal ideal domain.

Solution: Since $-p \equiv 3 \pmod 4$, $\mathcal{O}_K = \mathbf{Z}[\sqrt{-p}]$. Now observe that

$$(2) = (2, 1 + \sqrt{-p})^2.$$

Indeed,

$$\begin{aligned}
(2, 1 + \sqrt{-p})^2 &= (4, 2 + 2\sqrt{-p}, 1 - p + 2\sqrt{-p}) \\
&= (4, 2 + 2\sqrt{-p}, 2\sqrt{-p}) \text{ since } p \equiv 1 \pmod 4 \\
&= (2).
\end{aligned}$$

(Or, if you like,

$$2 = 2(1 + \sqrt{-p}) - (1 + \sqrt{-p})^2 - (\frac{p-1}{4})2^2)$$

But $(2, 1 + \sqrt{-p})$ cannot be principal, as $\mathcal{O}_K$ has no element of norm 2.

Ben Green: ben.green@maths.ox.ac.uk

Section C

9. Let $K = \mathbf{Q}(\sqrt{-7})$. In this question you may assume (as follows from Question 7) that $\mathcal{O}_K$ is a PID.

   (i) Factor 2 and $\sqrt{-7}$ into irreducibles in $\mathcal{O}_K$.

   (ii) Suppose that $7 \nmid x$. Show that $2x + \sqrt{-7}$ and $2x - \sqrt{-7}$ are coprime.

   (iii) Show that there are no integer solutions to the equation $4x^2 + 7 = y^3$.

Solution: (i) We have $N_{K/\mathbf{Q}}(\sqrt{-7}) = 7$ so $\sqrt{-7}$ is itself irreducible. However, $2 = \theta\overline{\theta}$ where $\theta = \frac{1}{2}(1 + \sqrt{-7})$ (which is in $\mathcal{O}_K$). These both have norm 2, so are irreducible. Since the only units in $\mathcal{O}_K$ are ± 1, they are not associates.

(ii) Suppose d divides both these expressions. Then d divides $2\sqrt{-7} = \theta\overline{\theta}\sqrt{-7}$. If $\sqrt{-7}$ divides both expressions then 7 divides $4x^2 + 7$, hence $7|x$, contrary to assumption. Suppose that $\theta | 2x + \sqrt{-7}, 2x - \sqrt{-7}$. Then, taking conjugates, $\overline{\theta} | 2x + \sqrt{-7}, 2x - \sqrt{-7}$, and so $2 = \theta\overline{\theta}$ divides both $2x + \sqrt{-7}$ and $2x + \sqrt{-7}$. This is impossible, since $x + \frac{1}{2}\sqrt{7}$ is not an algebraic integer.

(iii) Such a solution cannot have $7|x$, since otherwise $7^2 | y^3 - 4x^2 = 7$. Factor the equation as $(2x + \sqrt{-7})(2x - \sqrt{-7}) = y^3$. By the first part, the two factors are coprime. Thus they are both cubes, in particular

$$2x + \sqrt{-7} = (a + b\theta)^3$$

with $a, b \in \mathbf{Z}$. (Note again that the only units are ± 1, which are both cubes). Expanding out and comparing coefficients gives

$$(a + \frac{b}{2})^3 - \frac{21}{4}(a + \frac{b}{2})b^2 = 2x, \tag{8}$$

$$3(a + \frac{b}{2})^2 \frac{b}{2} - 7(\frac{b}{2})^3 = 1. \tag{9}$$

The second of these factors as

$$b(3(2a + b)^2 - 7b^2) = 8,$$

thus $b = \pm 1, \pm 2, \pm 4, \pm 8$. One may check that none of these leads to an integral value of a.

Remark. Solving $x^2 + 7 = y^3$ for x odd is actually quite tricky and well beyond the scope of this course. It was done by Ljunggren in the 1940s ($x = \pm 1$ and $x = \pm 181$ are the only solutions).

Ben Green: ben.green@maths.ox.ac.uk