ALGEBRAIC NUMBER THEORY- SHEET 5

CHRISTOPHER BIRKBECK

For this problem sheet you have a choice:

- Option 1: Hand in solutions to 5.2 and 5.3.
- Option 2: Hand in a solution to 5.8

Solutions should be uploaded to moodle by: 11:59pm on 28/02/2021

Exercise 5.1. Let p be a prime number and let α be a root of $x^p - p$. Set $K = \mathbb{Q}(\alpha)$.

(1) Find the minimal polynomial of α.
(2) Calculate the discriminant of the basis $B := \{1, \alpha, \dots, \alpha^{p-1}\}$.
(3) Show that B is an integral basis. In other words show that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

Exercise 5.2. Let α be a root of $x^3 - 2x + 2$ and let $K = \mathbb{Q}(\alpha)$.

(1) Find the minimal polynomial of α.
(2) Calculate the discriminant of the basis $B := \{1, \alpha, \alpha^2\}$.
(3) Show that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

Exercise 5.3. Let α be a root of $x^5 - 37$ and let $K = \mathbb{Q}(\alpha)$.

(1) Find the minimal polynomial of α.
(2) Calculate the discriminant of the basis $B := \{1, \alpha, \alpha^2, \alpha^3, \alpha^4\}$.
(3) Show that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

[Hint: Look for a change of variables that will make the polynomial Eisenstein at all the places you need simultaneously. Then use question 5.6 and extra arguments to conclude.]

Exercise 5.4. Let α be a root of $x^4 - 3$ and let $K = \mathbb{Q}(\alpha)$.

(1) Find the minimal polynomial of α.
(2) Calculate the discriminant of the basis $B := \{1, \alpha, \alpha^2, \alpha^3\}$.
(3) Show that B is an integral basis. In other words show that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

Exercise 5.5. Let α be a root of $x^3 + 3x + 6$ and let $K = \mathbb{Q}(\alpha)$.

(1) Find the minimal polynomial of α.
(2) Calculate the discriminant of the basis $B := \{1, \alpha, \alpha^2\}$.
(3) Show that B is an integral basis. In other words show that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

Exercise 5.6. Let K be a number field, $\alpha \in \mathcal{O}_K$ and $m \in \mathbb{Z}$. Let $\beta = \alpha + m$.

(1) Show that α and β have minimal polynomials m_α, m_β of the same degree.
(2) Let $\deg(m_\alpha) = n$, $B_\alpha = \{1, \alpha, \dots, \alpha^{n-1}\}$, $B_\beta = \{1, \beta, \dots, \beta^{n-1}\}$. Show that
$$\Delta(B_\alpha) = \Delta(B_\beta).$$

Exercise* 5.7. Let $K = \mathbb{Q}(\sqrt{7}, \sqrt{10})$ and let $\alpha \in \mathcal{O}_K$.

(1) Let $f \in \mathbb{Z}[x]$ and let $\overline{f}$ denote the reduction modulo 3 of f. Show that $f(\alpha)$ is divisible by 3 in $\mathbb{Z}[\alpha]$ if and only if $\overline{f}$ is divisible by $\overline{m}_\alpha$ in $\mathbb{F}_3[x]$.

(2) Suppose that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Let

$$\alpha_1 = (1+\sqrt{7})(1+\sqrt{10})$$
$$\alpha_2 = (1+\sqrt{7})(1-\sqrt{10})$$
$$\alpha_3 = (1-\sqrt{7})(1+\sqrt{10})$$
$$\alpha_4 = (1-\sqrt{7})(1-\sqrt{10}).$$

Show that for all $i \neq j$, the product $\alpha_i\alpha_j$ is divisible by 3 in $\mathbb{Z}[\alpha]$ but that 3 does not divide any power of any α_i. [Hint: Look at the trace of $\alpha_i^n/3$ to deduce it is not an algebraic integer. To do this, show that $\mathrm{Tr}(\alpha_i^n) = \alpha_1^n + \alpha_2^n + \alpha_3^n + \alpha_4^n$ and compare with $(\alpha_1+\alpha_2+\alpha_3+\alpha_4)^n$.]

(3) For $i = 1, \ldots, 4$, let $f_i \in \mathbb{Z}[x]$ be such that $f_i(\alpha) = \alpha_i$. Show that (modulo 3), $\overline{m}_\alpha$ divides $\overline{f}_i\overline{f}_j$ for $i \neq j$ and that $\overline{m}_\alpha$ does not divide $\overline{f}_i^n$ for any $n \in \mathbb{Z}_{\geq 1}$.

Hence deduce that for each i, $\overline{m}_\alpha$ has an irreducible factor in $\mathbb{F}_3[x]$ which does not divide $\overline{f}_i$ but which does divide all $\overline{f}_j$ for $j \neq i$. [You may want to use that $\mathbb{F}_3[x]$ is a UFD.]

(4) Show that $\overline{m}_\alpha$ has at least four distinct irreducible factors in $\mathbb{F}_3[x]$. From this and the fact that $\overline{m}_\alpha$ has degree at most 4, show that we cannot have $\mathcal{O}_K = \mathbb{Z}[\alpha]$ and thus there is no α such that $\mathcal{O}_K$ is generated by a single element. [Hint: How many monic polynomials of degree 1 are there in $\mathbb{F}_3[x]$?]

Exercise* 5.8. (1) Let p be a prime, k a positive integer and ζ_{p^k} be a (primitive) p^k-th root of unity and let $\lambda_{p^k} = 1 - \zeta_{p^k}$. Show that

$$\mathbb{Z}[\zeta_{p^k}] = \mathbb{Z}[\lambda_{p^k}]$$

and

$$\Delta(\{1, \zeta_{p^k}, \ldots, \zeta_{p^k}^{\varphi(p^k)-1}\}) = \Delta(\{1, \lambda_{p^k}, \ldots, \lambda_{p^k}^{\varphi(p^k)-1}\}).$$

Here φ is the usual Euler totient function.

(2) Show that $\Delta(\{1, \zeta_{p^k}, \ldots, \zeta_{p^k}^{\varphi(p^k)-1}\})$ divides $p^{k\varphi(p^k)}$.

(3) Let p be a prime and $n = p^k$. Let $S = \{1 \leq x \leq n \mid p \nmid x\}$ (i.e the set of elements less than n which are not divisible by p). Show that

$$\prod_{r \in S}(1 - \zeta_{p^k}^r) = p$$

and from this deduce that $\lambda_{p^k}^{\varphi(p^k)}$ divides p in $\mathbb{Z}[\zeta_{p^k}]$.

(4) Using the above prove that if $K = \mathbb{Q}(\zeta_{p^k})$ then $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^k}] = \mathbb{Z}[\lambda_{p^k}]$.