NUMBER FIELDS, EXX. SHEET 2

N. I. SHEPHERD-BARRON

(1*) Which of the following are algebraic integers: $\cos 2\pi/n$; $(i+\sqrt{5})/2$; $(1+10^{1/3}+10^{2/3})/3$.

(2) If p is an odd prime, find the minimal polynomial of $\cos 2\pi/p$.

(3*) Suppose that $d \neq 0, 1$ is a square-free integer. Calculate the discriminant and ring of integers of the quadratic field $\mathbb{Q}(\sqrt{d})$.

(4) Show that a ring of integers $\mathcal{O}_K$ is a PID if and only if it is a UFD.

(5*) Calculate the class group of the quadratic fields $\mathbb{Q}(\sqrt{d})$, where d is a square-free integer between ± 15. (Of course, this is about 20 separate questions.)[1]

(6) Show that $\mathcal{O}_K = \mathbb{Z}[(1+\sqrt{-19})/2]$ is a PID, but is not Euclidean. (Recall from GRM that the point of the Euclidean property is that Euclidean implies PID. But the natural way of proving that this ring is a PID is to use the ideas of this course.) [2]

(7*) Suppose that K is a number field of degree n, with r real embeddings and s conjugage pairs of complex embeddings. Show that the group of units in $\mathcal{O}_K$ is finitely generated of rank at most $r+s-1$, and state an exact result. [Any results about lattices that you need may be assumed without proof, but they must be stated clearly.]

(8*) Show that $8+3\sqrt{7}$ is a fundamental unit in the field $\mathbb{Q}(\sqrt{7})$. In terms of this unit, describe all integer solutions to the equation $x^2 - 7y^2 = 2$.

(9) (i) Show that $f := X^3 - 3X + 1$ is irreducible over $\mathbb{Q}$, and compute its discriminant.

Fix one of its roots, say x. Put $R = \mathbb{Z}[X]/(f) = \mathbb{Z}[x]$ and $K = \mathbb{Q}(x) = \mathbb{Q}[x]$.
(ii) Show that if $a + bx + cx^2 \in \mathcal{O}_K$ with $a, b, c \in \mathbb{Q}$, then a, b, c have only a 3 in the denominator.

---

[1] [Given what this course has covered, the basic technique is to use Minkowski's bound to write a list (short, one hopes) of prime ideals that generate the class group, and then find elements of small norm to give relations between these generators.]

[2] [First, use Minkowski etc. to prove the UFD property, then use a previous exercise to deduce the PID property. Use the units theorem to show that the only units in $\mathcal{O}_K$ are ± 1. Assume that $\phi : \mathcal{O}_K - \{0\} \to \mathbb{N}$ is a Euclidean function. Choose $x \in \mathcal{O}_K, x \neq 0, \pm 1$ with $\phi(x)$ minimal. Show that the elements of $\mathcal{O}_K/(x)$ are the images of $0, \pm 1$, so that $\#\mathcal{O}_K/(x) \leq 3$. Make a list of rings with at most 3 elements. Show that the minimal polynomial of $(1+\sqrt{-19})/2$ is $x^2 + x + 5$, and that this polynomial does not split in any ring with at most 3 elements.]

(iii) Show that $x, x+2$ are units in R and that $(x+1)^3 = 3x(x+2)$. Show that $x+1$ is a prime element of R and that $P = (x+1)R$ is the only prime ideal of R that contains 3.
(iv) Deduce that R_P is a DVR and that $R = \mathcal{O}_K$.
(v) Compute the class group of $\mathcal{O}_K$.

(10) (i) Show that $f := X^3 + X^2 - 2X + 8$ is irreducible over $\mathbb{Q}$.
Fix one of its roots, say x. Put $R = \mathbb{Z}[X]/(f) = \mathbb{Z}[x]$ and $K = \mathbb{Q}(x) = \mathbb{Q}[x]$.
(ii) Show that the discriminant of f is -4.503 (use a symbolic package).
(iii) Show that $y = 4/x \in \mathcal{O}_K$ and that $y \notin \mathbb{Z}[x]$.
(iv) Deduce that $\mathcal{O}_K = \mathbb{Z}[x, y]$.
(v) Show that (2) is the product of 3 distinct prime ideals in $\mathcal{O}_K$, and show that $\mathcal{O}_K/(2)$ cannot be written as $\mathcal{O}_K/(2) = \mathbb{F}_2[z]$.
(vi) Deduce that $\mathcal{O}_K$ canot be written as $\mathcal{O}_K = \mathbb{Z}[z]$, for any z.

References

E-mail address: nisb@dpmms.cam.ac.uk