## NUMBER FIELDS, EXX. SHEET 1

## N. I. SHEPHERD-BARRON

- (1\*) Which of the following are algebraic integers:  $\sqrt{5}$ ,  $\sqrt{5}/\sqrt{2}$ ,  $(1 + \sqrt{5})/2$ ,  $\sqrt{(1 + \sqrt{5})/\sqrt{2}}$ ,  $(1 + \sqrt{3})/2$ ,  $(1 + \sqrt{-3})/2$ ?
- (2\*) Define number field, algebraic number, algebraic integer. Prove that the algebraic integers in a given number field K form a ring  $\mathcal{O}_K$ . [Bookwork, but do it anyway.]
- (3\*) If K is a number field and  $a \in K$ , what are the conjugates of a? What are the conjugates of  $2^{1/3}$ ? Explain how to use the conjugates of a to check whether a is an algebraic integer.
- (4\*) Define the trace bilinear pairing  $T = T_{K/k}$  of a finite field extension K/k, and use it to prove that  $\mathcal{O}_K$  is a f.g.  $\mathbb{Z}$ -module when K is a number field. [Bookwork, but do it anyway.]
- (5\*) Define the discriminant of a subring R of  $\mathcal{O}_K$  such that K is the fraction field of R. Show that if  $R = \mathbb{Z}[a]$  and f is the minimal polynomial of a, then the discriminant of R equals that of f.

Assuming that D is a square-free integer and is prime to 3, compute a  $\mathbb{Z}$ -basis of  $\mathcal{O}_K$  when  $\theta = D^{1/3}$  and  $K = \mathbb{Q}(\theta)$ .

[In an exam you would be told to take for granted the useful result that if  $x = a + b\theta + c\theta^2$  with  $a, b, c \in \mathbb{Q}$ , then the elementary symmetric polynomials  $e_1, e_2, e_3$  in x and its conjugates are  $e_1 = 3a$ ,  $e_2 = 3a^2 - 3Dbc$ ,  $e_3 = a^3 + Db^3 + D^2c^3 - 3Dabc$ .]

- (6\*) Suppose that d is a square-free integer,  $d \neq 0, 1$ . Describe the ring of integers in the quadratic field  $K = \mathbb{Q}(\sqrt{d})$  and compute the discriminant  $D_K$  of this field. Show that if  $f \in \mathbb{Z}[x]$  is a monic quadratic polynomial of discriminant  $D_K$ , then  $\mathcal{O}_K \equiv \mathbb{Z}[x]/(f)$ .
- (7) Suppose that K is a number field of degree n = r + 2s in the usual notation (r is the number of real embeddings of K and s the number of pairs of complex embeddings). Show that the sign of the discriminant  $D_K$  is  $(-1)^s$ .
- (8) Prove Stickelberger's criterion, that  $D_K \equiv 0, 1 \pmod{4}$ .

<sup>&</sup>lt;sup>1</sup>[Hint: Suppose first that  $K/\mathbb{Q}$  is Galois, with group G. If  $(x_1,...,x_n)$  is a  $\mathbb{Z}$ -basis of  $\mathcal{O}_K$  and  $\sigma_1,...,\sigma_n$  are the real and complex embeddings of K, then  $D_K=\Delta^2$ , where  $\Delta=\det((\sigma_i(x_j))$ . Write  $\Delta=P-N$ , where P corresponds to the even permutations of n things and N to the odd ones. So  $D_K=(P+N)^2-4PN$ . Since  $K/\mathbb{Q}$  is Galois, the conjugates  $\sigma_i(x)$ , for any  $x\in K$ , are exactly the images  $g_i(x)$  of x under the various elements  $g_i$  of G. Deduce that P+N and PN are G-invariant, so in  $\mathbb{Q}$ . Notice that P,N are algebraic integers, so  $P+N,PN\in\mathbb{Z}$ . For the general case, embed K in a Galois closure  $L/\mathbb{Q}$ .

- (9) Show that  $f = x^3 x + 2$  is irreducible over  $\mathbb{Q}$  and that the ring of integers in  $\mathbb{Q}[x]/(f)$  is  $\mathbb{Z}[x]/(f)$ .
- (10) Suppose that p is an odd prime and that  $\zeta = \zeta_p = \exp(2\pi i/p)$ . Put  $K = \mathbb{Q}(\zeta)$  and  $A = \mathbb{Z}[\zeta]$ , a subring of  $\mathcal{O}_K$  (why?).
  - (i) Write down the minimal polynomial of  $\zeta$  and the conjugates of  $\zeta$ .
  - (ii) Show that if r, s are prime to p, then  $(\zeta^r 1)/(\zeta^s 1)$  is a unit in A.
- (iii) Show that  $\zeta 1$  is a prime element of A and that  $(p) = (\zeta 1)^{p-1}$  as principal ideals in A.
- (iv) Deduce that  $P = (\zeta^s 1)$  is the only prime ideal of A that lies over p, and that the local ring  $A_P$  is a DVR.
  - (v) Show that the discriminant of A is (up to sign) a power of p.
- (vi) Deduce that  $A_Q$  is a DVR for all prime ideals Q of A, and that therefore  $A = \mathcal{O}_K$ .
- (11\*) Find factorizations of ideals (in rings of integers  $\mathcal{O}_K$ ) of the form  $(p) = P_1^{e_1}...P_r^{e_r}$  in the following cases:
- $K = \mathbb{Q}(\sqrt{17}), p = 2, 3, 5; K = \mathbb{Q}(\zeta_5), p = 2, 3, 5.$  [That is, find the integers r and the exponents  $e_i$ , and the norm of each  $P_i$ .]

## References

 $E ext{-}mail\ address: nisb@dpmms.cam.ac.uk}$