

## ALGEBRAIC NUMBER THEORY W4043

HOMEWORK, WEEK 4, DUE OCTOBER 3

1. Do Exercise 6.11 from Hindry's book, pp. 118-9.

2. Let  $d > 0$  be a square-free positive integer congruent to 3 (mod 4).

(a) Every unit  $u \in \mathbb{Z}[\sqrt{d}]$  is of the form  $a - b\sqrt{d}$  where  $a^2 - db^2 = \pm 1$ , and the group  $\Gamma$  of units is the product of an infinite cyclic group with  $\{\pm 1\}$ . Consider the subset  $\Sigma$  of  $\Gamma$  consisting of  $u_i = a_i - b_i\sqrt{d}$  with  $a_i > 0, b_i > 0$ , ordered so that  $b_1 \leq b_2 \leq b_3 \dots$ . Show that  $u_1$  and  $-1$  are generators of  $\Gamma$ . The element  $u_1$  is called the *fundamental unit* of  $\mathbb{Z}[\sqrt{d}]$ .

(b) Show that the following algorithm finds  $u_1$ : Letting  $b = 1, 2, 3, \dots$ , consider the quantities  $q^\pm(b) = db^2 \pm 1$ . Let  $b_1$  be the smallest positive integer such that either  $q^+(b_1)$  or  $q^-(b_1)$  is a perfect square. Let  $a_1$  be the positive square root of  $q(b_1)$ ; then  $u_1 = a_1 - b_1\sqrt{d}$ .

(c) Use this algorithm to find the fundamental units  $u_1$  of  $\mathbb{Z}[\sqrt{7}]$ ,  $\mathbb{Z}[\sqrt{11}]$ ,  $\mathbb{Z}[\sqrt{15}]$ . In each case determine  $N_{K/\mathbb{Q}}(u_1)$ , where  $K = \mathbb{Q}(\sqrt{d})$  in each case.

3. As Hindry shows on p. 99, the ring  $R = \mathbb{Z}[\sqrt{10}]$ , which is equal to the ring of integers in  $\mathbb{Q}(\sqrt{10})$ , is not a principal ideal domain. Indeed, the integer 9 has two inequivalent factorizations:

$$9 = 3^2 = (\sqrt{10} - 1)(\sqrt{10} + 1).$$

(a) Show that  $3 + \sqrt{10}$  is a unit in  $R$ . Use this fact to confirm that the two factorizations are indeed inequivalent.

(b) The integer 10 is definitely a square modulo 3. What is the prime factorization of the ideal  $(3) \subset R$ ?

4. Let  $R$  be a Dedekind ring with only finitely many prime ideals. Show that  $R$  is a PID. (Hint: say  $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_r$  are the prime ideals. Find an element  $x_i \in \mathfrak{p}_i$  that is not in any of the  $\mathfrak{p}_j$  with  $j \neq i$ , and factor the ideal  $(x_i)$ . Another piece of information is necessary.)