

## NUMBER FIELDS HW 2

- (1) Show that the ring of integers of  $\mathbb{Q}(\sqrt{-6})$  is not a UFD.
- (2) This exercise shows that the unit group of a real quadratic field  $K = \mathbb{Q}(\sqrt{d})$ ,  $d > 0$  squarefree, is isomorphic to  $\langle \pm 1 \rangle \times \mathbb{Z}$ .
- (a) Show that given  $N > 0$ , there exists  $(a, b) \in \mathbb{Z}^2$ ,  $(a, b) \neq (0, 0)$ , satisfying  $|a - b\sqrt{d}| < \frac{1}{N}$  and  $0 \leq b \leq N$ . (Hint: consider the  $N + 1$  numbers  $\{b\sqrt{d}\}$ ,  $b = 0, 1, \dots, N$ , where  $\{x\}$  denotes the fractional part of  $x$ .)
- (b) Deduce from (a) that there are infinitely many  $a - b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$  such that  $|a - b\sqrt{d}| < \frac{1}{b}$ . Show then that there are infinitely many  $\alpha \in \mathbb{Z}[\sqrt{d}]$  such that  $|N(\alpha)| \leq 1 + 2\sqrt{d}$ .
- (c) Show that there is an  $\eta > 1$  in  $\mathbb{Z}[\sqrt{d}]$  such that  $N(\eta) = \pm 1$ . (Hint: from (b), there is an integer  $n \in (0, 1 + 2\sqrt{d})$  such that there are infinitely many  $\alpha_i \in \mathbb{Z}[\sqrt{d}]$  with  $|N(\alpha_i)| = n$ .)
- (d) Let  $S = \{\alpha \in \mathcal{O}_K^\times \mid 1 < \alpha < \eta\}$ , where  $\eta$  is the element found in (c). Show that  $S$  is finite, and that if  $\eta_0$  is the smallest element in  $S$ , then  $\mathcal{O}_K^\times = \langle \pm 1 \rangle \times \eta_0^\mathbb{Z}$ .
- (3a) Find the fundamental unit for  $\mathbb{Q}(\sqrt{5})$  and  $\mathbb{Q}(\sqrt{7})$ .
- (b) Find all the integer solutions to the Diophantine equation  $x^2 - 5y^2 = -1$ .
- (4a) Let  $K_d = \mathbb{Q}(\sqrt{-d})$ , with  $d > 0$  squarefree and ring of integers  $\mathcal{O}_d$ . Show that  $K_d$  is norm Euclidean if  $d = 1, 2, 3, 7$  or  $11$ .
- (b) The rest of the exercise shows that for other values of  $d > 0$ ,  $K_d$  is not Euclidean. Suppose that  $K_d$  is Euclidean with respect to a function  $\phi : \mathcal{O}_d \rightarrow \mathbb{Z}_{>0}$ , but  $d$  is not equal to one of the 5 values in (a). Let  $\alpha \in \mathcal{O}_d$  be a non-unit such that  $\phi(\alpha)$  is minimum among the values taken by  $\phi$  on non-units (why does such an  $\alpha$  exist?). Show that each coset in  $\mathcal{O}_d/(\alpha)$  can be represented by a unit and conclude that  $N_{K_d/\mathbb{Q}}(\alpha) = 2$ . Deduce a contradiction from this.
- (5) Find the factorization of the following into product of prime ideals:
- (a)  $K = \mathbb{Q}(\sqrt{-6})$  and  $I = (2)$ ;
- (b)  $K = \mathbb{Q}(\sqrt[3]{3})$  and  $I = (5)$ ;
- (c)  $K = \mathbb{Q}(\sqrt{3}, \text{sqrt}5)$  and  $I = (13)$ .
- (d)  $K = \mathbb{Q}(\zeta_5)$  and  $I = (2)$  and  $I = (5)$ .

- (6) For which primes  $p$  is the equation  $p = x^2 + 19y^2$  solvable in integers.
- (7) This exercise shows that there is a sequence of number fields  $K_n$ , with  $[K_n : \mathbb{Q}] \rightarrow \infty$ , such that  $\mathcal{O}_{K_n}$  can only be generated as a ring (or a  $\mathbb{Z}$ -algebra) by  $[K_n : \mathbb{Q}] - 1$  elements.

(a) Show that there are infinitely many primes which are congruent to 1 mod 8.

(b) Let  $p_1, p_2, \dots$  be a sequence of primes which are congruent to 1 mod 8. Let

$$K_n = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$$

with ring of integers  $\mathcal{O}_n$ . Show that 2 splits completely in  $K_n$  and deduce that

$$\mathcal{O}_n/(2) \cong (\mathbb{Z}/2\mathbb{Z})^{2^n}.$$

(c) Show that the  $\mathbb{Z}/2\mathbb{Z}$ -algebra  $(\mathbb{Z}/2\mathbb{Z})^k$  cannot be generated by  $< k - 1$  generators, but can be generated by  $k - 1$  generators.

(d) Deduce from (b) and (c) that the minimal number of generators of  $\mathcal{O}_n$  as a ring is  $2^n - 1$ .

(8) Let  $d > 0$  be a squarefree integer and let  $K = \mathbb{Q}(\sqrt{d})$ .

(a) If  $d$  is composite and  $p|d$  is an odd prime, show that  $(p) = \mathfrak{p}^2$ , where  $\mathfrak{p}$  is a non-principal ideal.

(b) Suppose that  $d = 1$  or  $2 \pmod{4}$ . Show that  $(2) = \mathfrak{p}^2$  where  $\mathfrak{p}$  is non-principal unless  $d = 1$  or  $2$ .

(c) Suppose that  $d = 7 \pmod{8}$ . Show that  $d = \mathfrak{p} \cdot \bar{\mathfrak{p}}$  where  $\mathfrak{p}$  is non-principal unless  $d = 7$ .

(d) Show that if  $\mathcal{O}$  is a UFD, then either  $d = 1, 2, 7$  or  $d$  is prime and  $d = 3 \pmod{8}$ .

(9) Find the ideal class group of the following:  $\mathbb{Q}(\sqrt{10})$ ,  $\mathbb{Q}(\sqrt{-14})$ ,  $\mathbb{Q}(\sqrt{30})$  and  $\mathbb{Q}(\zeta_5)$ .