Problem Sheet 6, MP473, Semester 2, 2000

1. Let $K = \mathbb{Q}(\sqrt{-d}), d > 1$ squarefree.

   (a) Prove that O_K is not a UFD if one of the following holds:

      (i) $d \equiv 1 \pmod 4,\ d > 1$;

      (ii) $d \equiv 2 \pmod 4,\ d > 2$;

      (ii) $d \equiv 7 \pmod 8,\ d > 7$.

   (b) If O_K is a UFD and $d > 3$ and $d \equiv 3 \pmod 8$, prove that d is a prime and that $x^2 + x + \frac{d+1}{4}$ assumes prime values for $x = 0, \ldots, \frac{d-7}{4}$.

2. (Chinese Remainder Theorem) Let A and B be ideals of O_K with $(A, B) = (1)$. Prove that the mapping $f : O_K/AB \to O_K/A \oplus O_K/B$, given by

$$f(x + AB) = (x + A, x + B)$$

   is well–defined and an isomorphism.

3. A commutative ring is called *reduced* if $x^n = 0, n \in \mathbb{N} \Rightarrow x = 0$. Prove that if $(A, B) = (1)$, that O_K/AB is reduced if and only if O_K/A and O_K/B are reduced.

   If P is a prime ideal of O_K, prove that O_K/P^e is reduced if and only if $e = 1$. Deduce that $O_K/(p)$ is not reduced if and only if p ramifies (ie. one of the prime ideal factors of (p) occurs to an exponent $e > 1$.)

   (P. Samuel uses this result in his book *Algebraic theory of numbers* to prove Dedekind's theorem: p ramifies if and only if $p|D_K$.)

4. Find the group structure of the multiplicative group of equivalence classes of ideals in $\mathbb{Q}(\sqrt{-21})$.

5. Let $K = \mathbb{Q}(\sqrt{34})$.

   (a) Determine which primes must be examined in order to determine I_K.

   (b) Use the Kummer–Dedekind theorem to factorize the principal ideals $(2), (3)$ and (5):

$$(2) = P_2^2, \quad (3) = P_3Q_3, \quad (5) = P_5Q_5.$$

   (c) Use the equation $N_K(6 + \sqrt{34}) = 2$ to prove that $P_2 = (6 + \sqrt{34})$.

   (d) Let $\alpha = 7 + \sqrt{34}$. With a suitable choice of labelling, prove that $\alpha \in P_3$ and $\alpha \in P_5$ and deduce that

$$P_3P_5 = (\alpha).$$

   (e) Prove that $P_3^2 = (-5 + \sqrt{34})$.

   (f) Given that $\eta = 35 + 6\sqrt{34}$ is the fundamental unit of K and that $N_K(\eta) = 1$, prove that P_3 is not principal.

   (g) Determine the structure of the class group I_K.

6. Suppose that $m \equiv 3 \pmod 8$, m is a prime and that $x^2 + x + \frac{m+1}{4}$ assumes prime values for $x = 0, 1, \ldots, \frac{m-7}{4}$. Prove that $\mathbb{Q}(\sqrt{-m})$ is a UFD by showing that all ideals are principal.

7. Let $K = \mathbb{Q}(\sqrt{d})$, where d is a squarefree integer, $d \neq 1$.

   (i) If $d < 0$ and $g \in \mathbb{N}$, where $g < |D_K|/4$, prove that there does not exist an $\alpha \in O_K$ satisfying $N_K(\alpha) = g$, unless $g = m^2,\ m \in \mathbb{N}$ and $\alpha = \pm m$.

   (ii) Let $d = -14$. Prove that if $J = (3, 1 + \sqrt{-14})$ and $K = (2, \sqrt{-14})$, then

   $$J^2 = (9, -2 + \sqrt{-14}), \text{ and } J^2K = (-2 + \sqrt{-14}).$$

   Also prove that J^4 is principal and J^2 is not principal. (Use part (i).)

   (iii) Prove that $I_K \cong C_4$.

8. In $\mathbb{Z}[\sqrt{-5}]$, let

   $$A = (3, 4 + \sqrt{-5}), B = (3, 4 - \sqrt{-5}), C = (7, 4 + \sqrt{-5}), D = (7, 4 - \sqrt{-5}).$$

   Show that $AB = (3), CD = (7), AC = (4 + \sqrt{-5}), BD = (4 - \sqrt{-5})$ and that A, B, C and D are prime ideals.

   Factorize $(1 + 2\sqrt{-5})$.

Please hand in Question 5 as Assignment 4.