Algebraic number theory

Problem sheet 2

February 4, 2011

Let d be a square-free integer, and let $K = \mathbb{Q}(\sqrt{d})$. The *norm* of a quadratic number $z = x + y\sqrt{d}$, where $x, y \in \mathbb{Q}$, is

$$N(z) = (x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2.$$

1. (a) Prove that N is a multiplicative function $\mathcal{O}_K \to \mathbb{Z}$.

(b) Prove that $\mathcal{O}_K^*$ is the set of elements of $\mathcal{O}_K$ of norm ± 1.

(c) Let $d < 0$. Find all the elements of $\mathcal{O}_K^*$, hence determine the structure of the group $\mathcal{O}_K^*$.

(d) Which of the following are units: $4 + \sqrt{17}$, $2 + \sqrt{3}$, $2 + \sqrt{5}$, $2 + \sqrt{-5}$?

2. (a) Prove that any element of $\mathcal{O}_K$ whose norm is $\pm p$, where p is a prime number, is irreducible.

(b) When is $n + \sqrt{-5}$ irreducible for $n = 0, 1, \ldots, 7$?

3. *Application to a Diophantine equation.* This is a harder question!

A Euclidean domain is a PID hence a UFD, so every element is a product of finitely many irreducible elements, and such a factorisation is unique up to order and multiplication of irreducible factors by units. This is true for $\mathbb{Z}[\sqrt{-2}]$ (let's assume this). Pierre Fermat stated that

the only integer solutions of $y^2 + 2 = x^3$ *are* $(3, \pm 5)$.

Prove his theorem in the following steps:

(a) Show that y must be odd.

(b) Rewrite the equation as $(y + \sqrt{-2})(y - \sqrt{-2}) = x^3$. If $a + b\sqrt{-2}$ is a common divisor of $y + \sqrt{-2}$ and $y - \sqrt{-2}$, it divides their sum and difference. Deduce that $y + \sqrt{-2}$ and $y - \sqrt{-2}$ are coprime (i.e., have no non-unit common divisors).

(c) Using the unique factorization conclude that $y + \sqrt{-2}$ and $y - \sqrt{-2}$ are cubes, say, $y + \sqrt{-2} = (c + d\sqrt{-2})^3$. Prove that the only solutions of this equation are $c + d\sqrt{-2} = \pm 1 + \sqrt{-2}$. Deduce Fermat's statement.

4. Let $d < 0$ be such that $\mathcal{O}_K$ is a PID. (For example, this is the case when $\mathcal{O}_K$ is a Euclidean domain, e.g. for $d = -1, -2, -3, -7, -11$.) Prove that an odd prime number p that does not divide d is a norm of an element of $\mathcal{O}_K$ if and only if the Legendre symbol $(\frac{d}{p})$ equals 1.