Algebraic number theory

Solutions sheet 2

February 4, 2011

1. (a) The multiplicativity is clear, so we just need to check that $N(\mathcal{O}_K) \subset \mathbb{Z}$ which is an issue when d is 1 mod 4. But then any element of $\mathcal{O}_K$ is either in $\mathbb{Z}[\sqrt{d}]$, or is one half of $n + m\sqrt{d}$, where n and m are both odd. Then $n^2 - dm^2$ is 0 mod 4, so it's OK.

(b) This is clear by taking norms.

(c) Let's first do the easy case when d is not 1 mod 4. Then every element of $\mathcal{O}_K^*$ can be written as $n + m\sqrt{d}$ and we need to find all pairs of integers n, m for which $(n + m\sqrt{d})(a + b\sqrt{d}) = 1$ for some a, $b \in \mathbb{Z}$. Taking norms we get

$$(n^2 + |d|m^2)(a^2 + |d|b^2) = 1,$$

which implies $n^2 + |d|m^2 = 1$. If $d < -1$, then $m = 0$ and $n = \pm 1$, so $\mathcal{O}_K^* = \{\pm 1\}$. If $d = -1$ we see that $\mathcal{O}_K^* = \{\pm 1, \pm i\}$.

If d is 1 mod 4 we know that any element of $\mathcal{O}_K$ is as before or one half of $n + m\sqrt{d}$. So we need to solve the equation

$$(n^2 + |d|m^2)(a^2 + |d|b^2) = 4.$$

The factors can be 1, 2 or 4. We already listed all solutions with $n^2 + |d|m^2 = 1$. Note that $|d|$ is 3 mod 4, so $n^2 + |d|m^2 = 2$ has no solutions. Finally, the solutions of $n^2 + |d|m^2 = 4$ are $(\pm 2, 0)$, or $(\pm 1, \pm 1)$ if $d = -3$. Therefore, for $d = -3$ the group $\mathcal{O}_K^*$ is cyclic of order 6 formed by the 6th roots of 1 in $\mathbb{C}$, for $d = -1$ the group $\mathcal{O}_K^*$ is the group of 4th roots of 1, and so is the product of two groups of order 2, and $\mathcal{O}_K^* = \{\pm 1\}$ in all other cases.

(d) is an application of (b).

2. (a) This element is clearly non-zero, and not a unit by Q1. If it is a product of two non-units, then its norm is a product of two integers of modulus greater than 1, a contradiction.

(b) For $n = 0$ and $n = 6$ we can use (a). A calculation as in Q1 shows that $\mathcal{O}_K$ has no elements of norm 2, 3 or 7. Since the norm of an element of $\mathcal{O}_K$ which is not a unit and not an irreducible, is a product of two integers > 1 which are norms, we see that for $n = 1, 2, 3, 4$ the element $n + \sqrt{-5}$ is irreducible. It is clear that $5 + \sqrt{-5} = \sqrt{-5}(1 - \sqrt{-5})$ is not irreducible. It remains to understand $7 + \sqrt{-5}$ whose norm is 54. So let's find all elements of norm 6 and 9. Apart from ± 3, which is useless, we have $\pm 1 \pm \sqrt{-5}$ and $\pm 2 \pm \sqrt{-5}$. A little experimentation shows that

$$7 + \sqrt{-5} = (1 + \sqrt{-5})(2 - \sqrt{-5}),$$

so this one is certainly not irreducible.

3. (a) If y is even, then the LHS is congruent to 2 mod 4, then the RHS is even, then the RHS is congruent to 0 mod 4. Contradiction.

(b) If $a + b\sqrt{-2}$ is a common divisor of $y + \sqrt{-2}$ and $y - \sqrt{-2}$, it divides their sum and difference, that is, $2y$ and $2\sqrt{-2}$. On taking norms we get $a^2 + 2b^2 | 4y^2$ and $a^2 + 2b^2 | 8$. By (a) it follows that $a^2 + 2b^2 | 4$, hence $(a, b) = (\pm 1, 0)$ or $(a, b) = (\pm 2, 0)$ or $(a, b) = (0, \pm 1)$. The first solution corresponds to units. Since y is odd, $y + \sqrt{-2}$ is not divisible by $\sqrt{-2}$, neither is it divisible by 2. Thus the second and the third solutions do not lead to divisors of $y + \sqrt{-2}$. Hence $y + \sqrt{-2}$ and $y - \sqrt{-2}$ are coprime.

(c) Comparing the coefficients at $\sqrt{-2}$ in $y + \sqrt{-2} = (c + d\sqrt{-2})^3$ one gets $1 = d(3c^2 - 2d^2)$. The rest is immediate.

4. We note that p is odd and coprime with d, so that p can only be split or inert. If p is a norm, then $p = z.\overline{z}$, for some $z \in \mathcal{O}_K$. The ideal $I = (z)$ contains (p) and is different from the whole ring. Since the norm of z is p, and the norm of p is p^2, we have $z \notin (p)$. Hence $I \neq (p)$. By the classifications of prime ideals in $\mathcal{O}_K$ we know that I must be a prime ideal over p, which is distinct from (p). Therefore p is split. This is known to be equivalent to $(\frac{d}{p}) = 1$.

A more direct proof is this. We have $p = N(z)$, for some $z \in \mathcal{O}_K$. Then $2z$ can be written as $a + \sqrt{d}b$ with integer a and b. Then $4p = a^2 - db^2$. Since $p \neq 2$ and $(p, d) = 1$, it follows that a and b are not divisible by p. Reducing modulo p we conclude that d is a square modulo p.

The converse. If p is split, then $(p) = (p, a + \sqrt{d})(p, a - \sqrt{d})$. Let z be a generator of the first of these ideals, then $\overline{z}$ generates the second one. Hence $(p) = (N(z))$ as ideals in $\mathcal{O}_K$. This implies $p = u.N(z)$, where $u \in \mathcal{O}_K^*$. Since p and $N(z)$ are positive integers, $u = 1$. Thus p is a norm.