Algebraic number theory

Solutions to test 1

February 20, 2012

1. **7 marks** for any complete proof.

We have $\mathbb{Z} \subset R \subset \mathbb{Q}$, and $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$. Hence $\mathbb{Q}$ is also the field of fractions of R. We must prove that a fraction $a/p^m b$ in lowest terms, where $m \geq 1$, cannot be integral over R. Otherwise, $f(a/p^m b) = 0$ for some monic polynomial $f(t) = t^n + c_{n-1}t^{n-1} + \ldots$ in $R[t]$. Multiplying by $p^{nm-1}b^n/a^n$ we see that $p^{-1} \in R$, a contradiction.

2. **4 marks**

From lectures we know that these ideals are $(2, \delta)$ and $(2, \delta + 1)$, where $\delta = (1 + \sqrt{-15})/2$.

3. **9 marks**, 3 marks for each complete case.

If d is 1 modulo 4, then 2 is not ramified, so the primes that are ramified must be two odd primes p and q. Then $d = \pm pq$, where the sign is 1 if pq is 1 modulo 4, and -1 is pq is 3 modulo 4.

If d is 2 modulo 4, then 2 is ramified, so only one odd prime p is ramified. Hence $d = \pm 2p$ for any choice of sign.

If d is 3 modulo 4, then 2 is ramified, so only one odd prime p is ramified. In this case $d = \pm p$, where the sign is 1 if p is 3 modulo 4, and -1 is p is 1 modulo 4.