MATH7421 Problems Week 4

Primes, Irreducibles and Unique Factoristion

1. Show that if $p \in \mathbb{Z}$ is irreducible then it is prime, i.e. if $p|ab$ then $p|a$ or $p|b$.

   (Hint: If $p \nmid a$ then $\gcd(p, a) = 1$. Use Euclid's Algorithm to get a relation between p and a.)

2. Let R be an integral domain. Show that every prime $\pi \in R\backslash(R^\times \cup \{0\})$ is irreducible.

3. Let K be a number field and $\mathcal{O}_K$ be its ring of integers. Suppose that $\alpha \in \mathcal{O}_K$ is such that $N(\alpha) \in \mathbb{Z}$ is prime. Show that α is irreducible.

4. Show that the ring $\mathbb{Z}[\sqrt{-10}]$ is not a UFD by giving, with proof, two inequivalent factorisations of 14 into irreducibles. You may assume that the units of this ring are $\mathbb{Z}[\sqrt{-10}]^\times = \{\pm 1\}$.

5. In Chapter 1 of the notes we promised that the ring $\mathbb{Z}[i]$ is a UFD (and we might have even proved it in the lectures by now!). If this is the case then explain the following factorisation:

$$65 = 5 \cdot 13 = (-1 + 8i)(-1 - 8i).$$

Euclidean Domains

6. In Chapter 1 we promised that the ring $\mathbb{Z}[\sqrt{2}]$ is a UFD. Prove this by showing that it is a Euclidean Domain with function $\delta(\alpha) = |N(\alpha)| \in \mathbb{N}_{\geq 0}$.

7. Consider the ring of integers $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ of $\mathbb{Q}(\sqrt{-3})$. Prove that this ring is a UFD by showing that it is a Euclidean Domain with function $\delta(\alpha) = N(\alpha) \in \mathbb{N}_{\geq 0}$.

8. We know that the ring $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, so it can't be a Euclidean Domain. Show explicitly that it cannot be Euclidean with respect to the function $\delta(\alpha) = N(\alpha) \in \mathbb{N}_{\geq 0}$. (Hint: Consider $\alpha = 3$ and $\beta = 1 + \sqrt{-5}$).

9. The ring $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ turns out to be a UFD, but it is not a Euclidean Domain. Show that it cannot be Euclidean with respect to the function $\delta(\alpha) = N(\alpha) \in \mathbb{N}_{\geq 0}$. (Hint: Consider $\alpha = \frac{1+\sqrt{-19}}{2}$ and $\beta = 2$).

10. As we saw in the introduction, one way you might try to prove Fermat's Last Theorem is to use the factorisation:

$$x^n + y^n = \prod_{i=0}^{n-1}(x + \zeta_n^i y)$$

in the ring $\mathbb{Z}[\zeta_n]$ with $\zeta_n = e^{\frac{2\pi i}{n}}$ a primitive nth root of unity. This was the strategy used by Lamé in the 1800's, but it relies on $\mathbb{Z}[\zeta_n]$ being a UFD. Show, as Kummer did, that $\mathbb{Z}[\zeta_{23}]$ is not a UFD.

(Hint: Show that the product:

$$(1 + \zeta_{23}^2 + \zeta_{23}^4 + \zeta_{23}^5 + \zeta_{23}^6 + \zeta_{23}^{10} + \zeta_{23}^{11})(1 + \zeta_{23} + \zeta_{23}^5 + \zeta_{23}^6 + \zeta_{23}^7 + \zeta_{23}^9 + \zeta_{23}^{11})$$

is divisible by 2. Finish the proof, given that $\mathbb{Z}[\zeta_{23}]$ is the ring of integers of the number field $\mathbb{Q}(\zeta_{23})$ and that 2 is an irreducible element of this ring).