Rings and Fields
Assignment 4

James Zoryk.
Student Number: 2663347.

Question 1. It is given that

$$R = \mathbb{Z}[\sqrt{-7}] = \{a + \hat{a}\sqrt{-7} \mid a, \hat{a} \in \mathbb{Z}\}$$

is a subring of $\mathbb{C}$ that is an integral domain.

Note. Let $R = \mathbb{Z}[\sqrt{-7}] = \{a + \hat{a}\sqrt{-7} \mid a, \hat{a} \in \mathbb{Z}\}$, since R is a subring of the complex numbers which is closed under addition, subtraction and multiplication, and contains 0 and 1, this implies that R is an integral domain.

Now we define the norm N on R, as function mapping R to $\mathbb{Z}$ by

$$N(a + \hat{a}\sqrt{-7}) = a^2 + 7\hat{a}^2.$$

To determine the units of R, find all α in R such that $N(\alpha) = 1$. If $\alpha = a + \hat{a}\sqrt{-7}$ and $N(\alpha) = 1$, then it follows that $1 = a^2 + 7\hat{a}^2$ for integers a and $\hat{a}$. The only possible solution is, $\hat{a} = 0$ and $a = \pm 1$. Hence the only units of R, are 1 and -1. We conclude that $R^* = \{\pm 1\}$.

We observe that R is not a UFD since $8 = (2)(2)(2) = (1 + \sqrt{-7})(1 - \sqrt{-7})$, where it can be proven that 2 and $(1 \pm \sqrt{-7})$ are irreducible of R. Thus being an irreducible element of R does not imply that the element is prime in R.

Part a. Show that $\sqrt{-7}$ is a prime element of R. Is it also an irreducible of R?

Proof. Suppose that $\sqrt{-7}$ is a prime element, then it follows that $\sqrt{-7}$ divides a product $\alpha\beta$ with α and β in R, such that $\alpha = a + \hat{a}\sqrt{-7}$ and $\beta = b + \hat{b}\sqrt{-7}$ for integers a and b. So that

$$\alpha\beta = (ab - 7\hat{a}\hat{b}) + (a\hat{b} + \hat{a}b)\sqrt{-7}.$$

Given that $\sqrt{-7}$ divides the product $\alpha\beta$, and since $\sqrt{-7}|\sqrt{-7}(a\hat{b} + \hat{a}b)$ we must now show that $\sqrt{-7}$ divides the rational part $(ab - 7\hat{a}\hat{b})$. We observe that $\sqrt{-7}|7$, so now $\sqrt{-7}$ must also divide ab, which is an integer. Moreover, this implies that 7 divides ab Now, since 7 is prime in the integers and with out loss of generality 7 divides a since $7|ab$, then either $7|a$ or $7|b$. Hence, we can conclude that $\sqrt{-7}$ divides $a + \hat{a}\sqrt{-7}$, indicates that $\sqrt{-7}$ is prime in R.

Since R is an integral domain and $\sqrt{-7}$ is prime in R, implies that $\sqrt{-7}$ is also an irreducible in R. $\square$

Part b. Prove that 5 is an irreducible element of R. Is it also a prime element of R?

Proof. Suppose that 5 is reducible in R, then there exists non-unit elements α, β in R such that $5 = \alpha\beta$. Applying the norm to the expression leads to

$$N(5) = 25 = N(\alpha)N(\beta).$$

This implies that either $N(\alpha) = 1, 5$ or 25. If $N(\alpha) = 1$ then $\alpha = \pm 1$ which is in R^*, thus a contradiction. Similarly, if $N(\alpha) = 25$ implies that $N(\beta) = 1$, with $\beta = \pm 1$, again this is a contradiction since ± 1 is in R^*.
Now, if $N(\alpha) = 5$, then it follows that $5 = a + \hat{a}\sqrt{-7}$ for some integers $a, \hat{a}$. However, no possible integer solution exists. Hence, we can conclude that 5 is irreducible in R.

Now suppose 5 is prime, then there exist an α and β in R such that $5|\alpha\beta$ such that 5 divides either α or β. Taking the norm of this expression, we can obtain

$$N(5) = 25|N(\alpha)N(\beta).$$

We observe that the factors of 25 are $1, 5$ and 25, which we can assume that $5|N(\alpha) = a^2 + 7\hat{a}^2$

a,b	$a^2 Mod\, 5$	$7\hat{a}^2 Mod\, 5$
0	0	0
1	1	2
2	4	3
3	4	3
4	1	2
5	0	0

□

From the table above we observe that $a^2 + 7\hat{a}^2 = 0\ Mod\, 5$ if and only if both a and $\hat{a}$ are divisible by 5. Hence if $5|\alpha\beta$ then $5|\alpha$ in R. As required, 5 is prime in R.

Question 2. Prove that $f(x) = x^4 + 2x^3 + 1$ cannot be written as $A(x)B(x)$ with $A(x)$ and $B(x)$ in $\mathbb{Q}[x]$ of degree 2.

Proof. Let $f(x) = x^4 + 2x^3 + 1$ be a polynomial in $\mathbb{Q}[x]$. Now, suppose that $f(x) = A(x)B(x)$ for $A(x)$ and $B(x)$ in $\mathbb{Q}[x]$ with a degree of 2. Then it follows that

$$f(x) = (x^2 + ax + b)(x^2 + cx + d),$$

with coefficients a, b, c and d in $\mathbb{Q}$. From this we can obtain

$$\begin{cases} a + c = 2 \\ b + ac + d = 0 \\ bc + ad = 0 \\ bd = 1 \end{cases}$$

Then it follows that $a = 2 - c$ such that $bc + (2 - c)d = 0$. Now, $bd = 1$ implies $d = d^{-1}$ so that

$$c(b - b^{-1}) + 2d = 0.$$

This leads to $2d = 0$. Moreover $d = 0$. However, if $d = 0$ then $bd = 0 \neq 1$, a contradiction.

Thus there are no quadratic factors $A(x)$ and $B(x)$ in $\mathbb{Q}[x]$ such that $f(x) = A(x)B(x)$. $\square$