Homework 15 - MATH 791

Will Thomas

In this assignment, you will verify that the ring $R = \mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ does not have the unique factorization property. The *norm* from R is $\mathbb{Z}$ is defined as follows: For $x = a + b\sqrt{-5}$, $N(x) := a^2 + 5b^2$

Problem 1:
Show that $N(xy) = N(x)N(y)$ for all $x, y \in R$
Solution:
For any $x, y \in R, \exists a_x b_x a_y b_y \in \mathbb{Z},\ x = a_x + b_x\sqrt{-5} \wedge y = a_y + b_y\sqrt{-5}$

$$N(xy) = N(a_x + b_x\sqrt{-5} \cdot a_y + b_y\sqrt{-5}) = N(a_x + b_x\sqrt{-5} \cdot a_y + b_y\sqrt{-5})$$
$$= N(a_xa_y + a_xb_y\sqrt{-5} + b_x\sqrt{-5}a_y + b_x\sqrt{-5}b_y\sqrt{-5})$$

Since $\mathbb{Z}$ is a commutative ring, we can assume that R is which will let us reduce to

$$= N((a_xa_y - 5b_xb_y) + (a_xb_y + a_yb_x)\sqrt{-5})$$
$$= (a_xa_y - 5b_xb_y)^2 + 5((a_xb_y + a_yb_x))^2$$
$$= (a_xa_y - 5b_xb_y)(a_xa_y - 5b_xb_y) + 5((a_xb_y + a_yb_x)(a_xb_y + a_yb_x))$$
$$= a_x^2a_y^2 + 25b_x^2b_y^2 - 10a_xa_yb_xb_y + 5(a_x^2b_y^2 + 2a_xa_yb_xb_y + a_y^2b_x^2)$$
$$= a_x^2a_y^2 + 5a_x^2b_y^2 + 5a_y^2b_x^2 + 25b_x^2b_y^2$$
$$= (a_x^2 + 5b_x^2)(a_y^2 + 5b_y^2) = N(x)N(y)$$
$$\therefore \forall x, y \in R,\ N(xy) = N(x)N(y)$$

Problem 2:
Use the norm to describe the units in R.
Solution:
We said that a unit was an element $u \in R$ such that $\exists u^{-1} \in R$ and $uu^{-1} = 1 = u^{-1}u$
We know from problem one that $N(1) = N(uu^{-1}) = N(u) * N(u^{-1})$ and
$N(1) = 1^2 + 0 = 1$
Since we are in the integers, we can then conclude that the only way an element can be a unit is if $N(x) = 1$, as $N(1) = 1 \implies 1 = N(u) * N(u^{-1})$ and we cannot have fractions in $\mathbb{Z}$

$$\therefore \forall x \in R, x \text{ is a unit} \iff N(x) = 1$$

Problem 3:
Show that $3, 2+\sqrt{-5}, 2-\sqrt{-5}$ are irreducible elements in R.
Solution:
An element x is "irreducible" if whenever $q = ab$ for $a, b \in R$ that either a or b is a unit. To show that those elements are irreducible, we need to show that any way to factor them must involve a unit
Let $3 = a * b$, we also know that $N(3) = N(a) * N(b) \implies N(3) = 3^2 = 9 = N(a) * N(b)$ This is also equivalent to saying that $N(a) \mid 9 \wedge N(b) \mid 9$ (in the integers not in R) The factors of 9 in $\mathbb{Z}$ are $\{1, 3, 9\}$, in the cases where we have $N(a \text{ or } b) = 1, 9$ then we will have solved that one of the factors is a unit as one of them must have $N(a \text{ or } b) = 1$ which means its a unit by problem 2.
If the factors are $N(a) = 3 \wedge N(b) = 3$, then we will arrive at a contradiction. Let us assume $a := x_a + y_a\sqrt{-5} \implies N(a) = N(x_a + y_a\sqrt{-5}) = x_a^2 + 5y_a^2 = 3$ $\implies 3 - 5y_a y_a = x_a x_a \implies x_a \mid (3 - 5y_a y_a) \implies x_a \mid 3$ However, 3 is prime in $\mathbb{Z} \implies x_a = \{1, 3\}$. Similarly, $3 - x_a x_a = 5y_a y_a \implies 3 - 1 = 2 = 5y_a y_a$ which cannot work for any $y_a \in \mathbb{Z}$. For $3 - 9 = -6 = 5y_a y_a$ this also cannot work for any $y_a \in \mathbb{Z}$

$$\therefore 3 \text{ is irreducible in } R$$

Very similar arguments can be used for the other two elements. All elements have $N(x) = 9$ and the remaining argument is based upon 9 not the original element.

Problem 4:
Use the equation $3 \cdot 3 = (2+\sqrt{-5}) \cdot (2-\sqrt{-5})$ to show that $3, 2+\sqrt{-5}, 2-\sqrt{-5}$ are not prime in R.
Conclude that R does not have the unique factorization property.
Solution:
We call a number "prime" if when $p \mid ab \implies p \mid a \vee p \mid b$
Using $3 \cdot 3 = (2+\sqrt{-5}) \cdot (2-\sqrt{-5})$, where they are all irreducible, this means that

$$3 \mid (2+\sqrt{-5}) \cdot (2-\sqrt{-5}) \implies 3 \mid (2+\sqrt{-5}) \vee 3 \mid (2-\sqrt{-5})$$

$$\implies (2 \pm \sqrt{5}i) = 3(a \pm b\sqrt{5}i)$$

$$\implies 2 = 3a \rightarrow\leftarrow$$

As $2 \neq 3a \in \mathbb{Z}$

$$\therefore 3, 2+\sqrt{-5}, 2-\sqrt{-5} \text{ are not prime in } R$$

We can conclude from this that R does not have the unique factorization property as $9 = 3 \cdot 3 = (2+\sqrt{-5}) \cdot (2-\sqrt{-5})$ cannot be factored **uniquely** in R

Problem 5:
Show that the ideal of R generated by 3 and $2+\sqrt{-5}$ is not a *principal ideal*, i.e., there does not exist $f \in R$ such that $\langle 3, 2+\sqrt{-5}\rangle = \langle f \rangle$
Solution:
Let us assume $\exists f \in R$ such that $\langle 3, 2+\sqrt{-5}\rangle = \langle f \rangle$
In order for this to occur we need an f such that $\exists n, f^n = 2+\sqrt{-5}$ and $\exists m, f^m = 3$.
However, $2+\sqrt{-5}$ is irreducible which means that $f = 2+\sqrt{-5}$ by the first equation.
We also know that $\exists m, (2+\sqrt{-5})^m = 3$ can never work as 3 is irreducible and $(2+\sqrt{-5})$ is not a unit.