Rings and Fields
Assignment 2

James Zoryk.
Student Number: 2663347.

It is given that

$$R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$$

is a subring of $\mathbb{C}$. For each $c = 0, 1, 2$, we consider the map $\rho \to \mathbb{Z}/3\mathbb{Z}$ with

$$\rho(a + b\sqrt{-5}) \mapsto \overline{a + bc}$$

Question 1a. Determine for which of those c the resulting ρ is a ring homomorphism.

Proof. For each c we will prove that whether ρ_c is a homomorphism.

I) For $c = 0$, consider the $\rho_0 \to \mathbb{Z}/3\mathbb{Z}$ with $\rho_0(a + b\sqrt{-5}) \mapsto \overline{a}$.
Let $x, y \in R$ such that $x = a_1 + b_1\sqrt{-5}$ and $y = a_2 + b_2\sqrt{-5}$, with $a_k, b_k \in \mathbb{Z}$.
Then it follows that

$$\rho_0(xy) = \rho_0\big((a_1a_2 - 5b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{-5})\big).$$

This produces a map of

$$\rho_0(xy) \mapsto \overline{a_1a_2 - 5b_1b_2} = \overline{a_1a_2 + b_1b_2}.$$

However

$$\rho(x)\rho(y) \mapsto \overline{a_1a_2}.$$

Hence the map ρ_0 is not a homomorphism.

II) For $c = 1$ consider the map $\rho_1 \to \mathbb{Z}/3\mathbb{Z}$ with $\rho_1(a + b\sqrt{-5}) \mapsto \overline{a + b}$.
Let $x, y \in R$ such that $x = a_1 + b_1\sqrt{-5}$ and $y = a_2 + b_2\sqrt{-5}$, with $a_k, b_k \in \mathbb{Z}$. Then it follows that

i) Given $\rho_1(x + y)$ can be expressed as

$$\rho_1\big((a_1 + a_2) + (b_1 + b_2)\sqrt{-5}\big) \mapsto \overline{(a_1 + a_2) + (b_1 + b_2)}$$

Since $\rho_1(x) \mapsto \overline{a_1 + b_1}$ and $\rho_1(y) \mapsto \overline{a_2 + b_2}$, then it follows that

$$\rho_1(x) + \rho_1(y) \mapsto \overline{a_1 + a_2 + b_1 + b2}$$

This shows that $\rho_0(a + b) = \rho_0(a) + \rho_0(b)$

ii) Now, $\rho_1(xy)$ is expressed by

$$\rho_0\big((a_1a_2 - 5b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{-5})\big) \mapsto \overline{a_1a_2 - 5b_1b_2 + (a_1b_2 + a_2b_1)}$$

Since this is in an modular class of three, the term $\overline{-5b_1b_2}$ equals $\overline{1b_1b_2}$ so this results in a map of

$$\overline{a_1a_2 + b_1b_2 + a_1b_2 + a_2b_1}.$$

Then for the other side, we have

$$\rho(x)\rho(y) \mapsto \overline{a_1a_2 + a_1b_2 + b_1a_2 + b_1b_2}.$$

This shows that $\rho_1(xy) = \rho_1(x)\rho_1(y)$.
Hence the map ρ_1 is a homomorphism.

III) For $c = 2$ consider the map $\rho_2 \to \mathbb{Z}/3\mathbb{Z}$ with $\rho_2(a + b\sqrt{-5}) \mapsto \overline{a + 2b}$.
Let $x, y \in R$ such that $x = a_1 + b_1\sqrt{-5}$ and $y = a_2 + b_2\sqrt{-5}$, with $a_k, b_k \in \mathbb{Z}$. Then it follows that

i) Given $\rho_2(x + y)$ can be expressed as

$$\rho_2\big((a_1 + a_2) + (b_1 + b_2)\sqrt{-5}\big) \mapsto \overline{(a_1 + a_2) + 2(b_1 + b_2)}$$

Since $\rho_2(x) \mapsto \overline{a_1 + 2b_1}$ and $\rho_1(y) \mapsto \overline{a_2 + 2b_2}$, then it follows that

$$\rho_2(x) + \rho_2(y) \mapsto \overline{a_1 + a_2 + 2(b_1 + b2)}$$

This shows that $\rho_2(a + b) = \rho_2(a) + \rho_2(b)$

ii) Now, $\rho_2(xy)$ is expressed by

$$\rho_2\big((a_1a_2 - 5b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{-5})\big) \mapsto \overline{a_1a_2 + b_1b_2 + 2(a_1b_2 + b_1a_2)}.$$

Then for the other side, we have

$$\rho(x)\rho(y) \mapsto \overline{a_1a_2 + 4b_1b_2 + 2(a_1b_2 + b_1a_2)} = \overline{a_1a_2 + b_1b_2 + 2(a_1b_2 + b_1a_2)}$$

This shows that $\rho_2(xy) = \rho_2(x)\rho_1(y)$.
Hence the map ρ_2 is a homomorphism.

$\square$

Question 1b. Let $c = 2$, Show that the first isomorphism theorem for ring gives a ring isomorphism $R/(3, 1 + \sqrt{-5}) \simeq \mathbb{Z}/3\mathbb{Z}$

$$\begin{tikzcd}
R \arrow[rr, dash] \arrow[d, dash] \arrow[drr, dash, "\rho_2 : (a + b\sqrt{-5}) \mapsto \overline{a + 2b}"] & & \mathbb{Z} \arrow[d, dash] \\
\dfrac{R}{(3, 1 + \sqrt{-5})} \arrow[rr, dash] & & \mathbb{Z}/3\mathbb{Z}
\end{tikzcd}$$

Proof. We can compose a natural homomorphism

$$\phi : \mathbb{Z} \to R \to R/(3, 1 + \sqrt{-5})$$

which maps any n in $\mathbb{Z}$ to a class $n + (3, 1 + \sqrt{-5}) \in R/(1, 1 + \sqrt{-5})$.
Show that this homomorphism has a $K = ker(\phi) = (3, 1 + \sqrt{-5})$ and is surjective.
Since

$$6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \ \in (3, 1 + \sqrt{-5})$$

This shows that $6\mathbb{Z} \subset K$, which suggest either that; $K = (1)$, $K = (2)$, $K = (3)$, or $K = (6)$. Now, suppose that $K = (1)$, then there should exist an $a, b \in \mathbb{Z}$ such that

$$1 = (a + b\sqrt{-5})(1 + \sqrt{-5}).$$

Which leads us to

$$1 = a - 5b, \quad \text{and} \quad 0 = (a + b)(\sqrt{-5}).$$

This system has no solution with $a, b \in \mathbb{Z}$. However, we see that

$$6 = a - 5b, \quad \text{and} \quad 0 = (a + b)(\sqrt{-5})$$

does have a solution, given by $a = -1$ and $b = 1$, which implies that $6\mathbb{Z} \subseteq K$. However, with this we see that $\phi(3) = 3$ while the $\phi\big((a + b\sqrt{-5})(1 + \sqrt{-5})\big) = 0$. This indicates that $(3) \subseteq K$.

Show that ϕ is subjective.
Given an arbitrary element $x \in R/(3, 1 + \sqrt{-5})$, there exists an element $y \in R$ such that $\phi(y) = x$.
We can write x in the form $a + K$ for some $a \in R$. So need to show there is $y \in R$ such that $\phi(y) = a + K$. As $\phi(y) = y + K$. $\square$

Question 1c. Show that the ideal $(3, (1+\sqrt{-5}))$ of R is not principal.

Proof. We see that the ideal generated by $K = (3, (1+\sqrt{-5}))$ which is a subring with elements of the form $\{3x + (1+\sqrt{-5})y \mid x, y \in R\}$. Assume that K is a principal ideal such that K is generated by a single element $K = (\alpha)$ for some $(\alpha) \in R$.
Since $3 \in (\alpha)$ and $1+\sqrt{-5} \in (\alpha)$, then there exists $r_1, r_2 \in R$ such that $3 = r_1\alpha$ and $1+\sqrt{-5} = r_2\alpha$.
Define the norm map $N : R \to \mathbb{Z}$, with

$$N(a + b\sqrt{-5}) \mapsto a^2 + 5b^2 \quad \text{and} \quad N(\alpha_i\alpha_j) = N(\alpha_i)N(\alpha_j), \text{ with } \alpha_i, \alpha_j \in K.$$

Then it implies

$$N(r_1)N(\alpha) = N(r_1\alpha) = N(3) \mapsto 9,$$

and also

$$N(r_2)N(\alpha) = N(r_1\alpha) = N(1+\sqrt{-5}) \mapsto 6.$$

This shows that $N(\alpha)|9$ and $N(\alpha)|6$, which implies that either $N(\alpha) = 1$ or $N(\alpha) = 3$. We can see that $a^2 + 5b^2 = 3$ has no solution with a and b in $\mathbb{Z}$. This leaves $a^2 + 5b^2 = 1$ which has a solution of $a = \{\pm 1\}$ and $b = 0$. However this implies that ideal K is generated by $K = (\pm 1)$, which clearly is not true.
This contradiction prove that K is not a principal ideal of R. □