(A+) This made my day! Have a great holiday!

Algebra and Number Theory

64 i) For $\varphi : \mathbb{Z}[i] \to \mathbb{Z}_{13}$ such that $\varphi(a+bi) = \overline{a+5b}$ to be a ring homomorphism, we need that:

$$\varphi(\alpha+\beta) = \varphi(\alpha)+\varphi(\beta), \quad \text{and}$$
$$\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$$

for all $\alpha, \beta \in \mathbb{Z}[i]$.

So let $\alpha = a+bi$, $\beta = c+di \in \mathbb{Z}[i]$, with $a, b, c, d \in \mathbb{Z}$, then:

$$\begin{aligned}
\varphi(\alpha+\beta) &= \varphi((a+bi)+(c+di)) \\
&= \varphi((a+c)+(b+d)i) \\
&= \overline{(a+c)+5(b+d)} \\
&= \overline{(a+5b)+(c+5d)} \\
&= \overline{a+5b} + \overline{c+5d} \\
&= \varphi(a+bi)+\varphi(c+di) \\
&= \varphi(\alpha)+\varphi(\beta) \quad \checkmark
\end{aligned}$$

and:

$$\begin{aligned}
\varphi(\alpha\beta) &= \varphi((a+bi)(c+di)) \\
&= \varphi(ac+adi+bci-bd) \\
&= \varphi((ac-bd)+(ad+bc)i) \\
&= \overline{(ac-bd)+5(ad+bc)} \\
&= \overline{(ac+25bd)+5(ad+bc)}
\end{aligned}$$

since in $\mathbb{Z}_{13}$, $\overline{-1} = \overline{2\times 13-1} = \overline{25}$

$$\begin{aligned}
&= \overline{ac+5ad+5bc+25bd} \\
&= \overline{(a+5b)(c+5d)} \\
&= \overline{a+5b} \cdot \overline{c+5d} \\
&= \varphi(a+bi)\varphi(c+di) \\
&= \varphi(\alpha)\varphi(\beta) \quad \checkmark
\end{aligned}$$

as required. So φ is a ring homomorphism.

ii) To show that $\ker\varphi = (-5+i, 13)$, show that both $\ker\varphi \subseteq (-5+i, 13)$, and $(-5+i, 13) \subseteq \ker\varphi$, which together imply $\ker\varphi = (-5+i, 13)$. ✓

Firstly note:

$$(-5+i, 13) = \{(-5+i)\gamma + 13\delta \mid \gamma, \delta \in \mathbb{Z}[i]\}$$

— For $(-5+i, 13) \subseteq \ker\varphi$:

Take any $\alpha \in (-5+i, 13)$, then we can write $\alpha = (-5+i)\gamma + 13\delta$, for some $\gamma, \delta \in \mathbb{Z}[i]$.

Then

$$\begin{aligned}\varphi(\alpha) &= \varphi((-5+i)\gamma + 13\delta) \\ &= \varphi(-5+i)\varphi(\gamma) + \varphi(13)\varphi(\delta)\end{aligned}$$

since φ is a homomorphism of rings

$$\begin{aligned}&= \overline{-5+5\cdot 1}\,\varphi(\gamma) + \overline{13+5\cdot 0}\,\varphi(\delta) \\ &= \overline{0}\,\varphi(\gamma) + \overline{0}\,\varphi(\delta) \quad ; \text{ since } \overline{13} = \overline{0} \text{ in } \mathbb{Z}_{13}. \\ &= \overline{0} + \overline{0} \\ &= \overline{0}, \text{ so } \alpha \in \ker\varphi. \checkmark\end{aligned}$$

So for any $\alpha \in (-5+i, 13)$, $\alpha \in \ker\varphi$, so $(-5+i, 13) \subseteq \ker\varphi$. ✓

— For $\ker\varphi \subseteq (-5+i, 13)$:

Take any $\alpha \in \ker\varphi$, where $\alpha = a+bi$, with $a, b \in \mathbb{Z}$.

Then:

$$\begin{aligned}&\alpha \in \ker\varphi \\ \Rightarrow\ &\varphi(\alpha) = \overline{0} \\ \Rightarrow\ &\overline{\varphi(a+bi)} = \overline{0} \\ \Rightarrow\ &\overline{a+5b} = \overline{0} \checkmark \\ \Rightarrow\ &a+5b = 13k, \text{ for some } k \in \mathbb{Z}. \\ \Rightarrow\ &a = 13k - 5b. \\ \Rightarrow\ &\alpha = (13k-5b) + bi \\ \Rightarrow\ &\alpha = 13k + (-5+i)b \\ \Rightarrow\ &\alpha \in (-5+i, 13) \checkmark \text{ since } k, b \in \mathbb{Z} \subseteq \mathbb{Z}[i].\end{aligned}$$

So for any $\alpha \in \ker\varphi$, $\alpha \in (-5+i, 13)$, so $\ker\varphi \subseteq (-5+i, 13)$. ✓

Together these two points show that $\ker\varphi = (-5+i, 13)$. ✓

Similarly, to show $\ker\varphi = (3+2i)$, show $\ker\varphi \subseteq (3+2i)$ and $(3+2i) \subseteq \ker\varphi$, which together give the equality.

Note that:

$$(3+2i) = \{(3+2i)\beta \mid \beta \in \mathbb{Z}[i]\}.$$

Algebra and Number Theory

— For $(3+2i) \subseteq \ker\varphi$:

Take any $\alpha \in (3+2i)$, so that $\alpha = (3+2i)\beta$, for some $\beta \in \mathbb{Z}[i]$.

Then:

$$\begin{aligned}\varphi(\alpha) &= \varphi((3+2i)\beta)\\ &= \varphi(3+2i)\,\varphi(\beta) \quad ; \text{ since } \varphi \text{ is a ring homomorphism}\\ &= \overline{3+5\cdot 2}\;\varphi(\beta)\\ &= \overline{13}\;\varphi(\beta)\\ &= \overline{0}\;\varphi(\beta)\\ &= \overline{0}, \quad \text{so } \alpha \in \ker\varphi. \checkmark\end{aligned}$$

So for any $\alpha \in (3+2i)$, $\alpha \in \ker\varphi$, so $(3+2i) \subseteq \ker\varphi$.

— For $\ker\varphi \subseteq (3+2i)$:

Take any $\alpha \in \ker\varphi$, since $\ker\varphi = (-5+i, 13)$ as shown above, then we can write $\alpha = (-5+i)\gamma + 13\delta$, for some $\gamma, \delta \in \mathbb{Z}[i]$.

Now notice that $(3+2i)(3-2i) = 3^2 - (2i)^2 = 9+4 = 13$, and $(3+2i)(-1+i) = -3+3i-2i-2 = -5+i$. ✓

So we find:

$$\begin{aligned}\alpha &= (-5+i)\gamma + 13\delta\\ &= (3+2i)(-1+i)\gamma + (3+2i)(3-2i)\delta\\ &= (3+2i)\big((-1+i)\gamma + (3-2i)\delta\big)\\ &= (3+2i)\beta, \quad \text{for some } \beta \in \mathbb{Z}[i],\\ &\qquad \text{putting } \beta = (-1+i)\gamma + (3-2i)\delta. \checkmark\end{aligned}$$

So $\alpha \in (3+2i)$

So for any $\alpha \in \ker\varphi$, $\alpha \in (3+2i)$, so $\ker\varphi \subseteq (3+2i)$

Hence $\ker\varphi = (3+2i)$ ✓

So indeed we have $\ker\varphi = (-5+i, 13) = (3+2i)$.

Beautiful!

67) To show that $(3, 1+\sqrt{-5})$ is not a principal ideal of $\mathbb{Z}[\sqrt{-5}]$, argue by contradiction.

Suppose that $(3, 1+\sqrt{-5})$ is a principal ideal, then $(3, 1+\sqrt{-5}) = (a)$ for some $a \in \mathbb{Z}[\sqrt{-5}]$.

Note that $(3, 1+\sqrt{-5}) = \{3\alpha + (1+\sqrt{-5})\beta \mid \alpha, \beta \in \mathbb{Z}[\sqrt{-5}]\}$ and $(a) = \{a\gamma \mid \gamma \in \mathbb{Z}[\sqrt{-5}]\}$. Since $3, 1+\sqrt{-5} \in (3, 1+\sqrt{-5})$, then $3, 1+\sqrt{-5} \in (a)$ so $3 = a\gamma$, $1+\sqrt{-5} = a\delta$, for some $\gamma, \delta \in \mathbb{Z}[\sqrt{-5}]$, so $a \mid 3$, and $a \mid 1+\sqrt{-5}$. ✓

Using the norm from Question 12, $N: \mathbb{Z}[\sqrt{-5}] \longrightarrow \mathbb{Z}_{\geq 0}$ such that $x + y\sqrt{-5} \longmapsto x^2 - y^2(-5) = x^2 + 5y^2 \geq 0$. This was shown to preserve multiplication, so if for $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$, $\alpha \mid \beta$, then $N(\alpha) \mid N(\beta)$ in $\mathbb{Z}$. ✓

Since $a \mid 3$, then $N(a) \mid N(3)$, where $N(3) = 3^2 + 5 \cdot 0^2 = 9$, so $N(a) = \pm 1, \pm 3, \pm 9$; and $a \mid 1+\sqrt{-5}$, then $N(a) \mid N(1+\sqrt{-5})$, where $N(1+\sqrt{-5}) = 1^2 + 5 \cdot 1^2 = 6$, so $N(a) = \pm 1, \pm 2, \pm 3$.

Combining these two restrictions, and using that N is non-negative gives that $N(a) = 1, 3$. ✓ good.

Case $N(a) = 3$:

let $a = x + y\sqrt{-5}$, with $x, y \in \mathbb{Z}$. Then $N(a) = 3 \Rightarrow x^2 + 5y^2 = 3$.

If $y = 0$, then $N(a) = x^2 + 5y^2 = x^2 + 5 \cdot 0^2 = x^2$. But $N(a) = 3$ requires $x^2 = 3$, which is not possible if x is an integer, since $\sqrt{3}$ is irrational. ✓

But if $y \neq 0$, then $y \leq -1$ or $y \geq 1$, so $y^2 \geq 1$, and $N(a) = x^2 + 5y^2 \geq x^2 + 5 \cdot 1 \geq 5 > 3$, so we cannot have $N(a) = 3$. ✓

So there is no $a \in \mathbb{Z}[\sqrt{-5}]$, with $N(a) = 3$, so $N(a) = 3$ is not possible. ✓

Case $N(a) = 1$:

let $a = x + y\sqrt{-5}$, with $x, y \in \mathbb{Z}$. Then $N(a) = 1 \Rightarrow x^2 + 5y^2 = 1$.

As above, we need $y = 0$, otherwise $y^2 \geq 1$, so $x^2 + 5y^2 \geq x^2 + 5 \cdot 1 \geq 5 > 1$, so $N(a) \neq 1$.

Algebra and Number Theory.

With $y = 0$, then $x^2 + 5y^2 = 1 \Rightarrow x^2 = 1$, so $x = \pm 1$, and only $a = \pm 1$ has $N(a) = 1$. ✓

For $a = 1$, $(a) = (1)$. Since $1 \in (1)$, then for any $\alpha \in \mathbb{Z}[\sqrt{-5}]$, $1 \cdot \alpha \in (1)$, since (1) is an ideal. But $1 \cdot \alpha = \alpha$, so for any $\alpha \in \mathbb{Z}[\sqrt{-5}]$, $\alpha \in (1)$, so $\mathbb{Z}[\sqrt{-5}] \subseteq (1)$. And since $(1) \subseteq \mathbb{Z}[\sqrt{-5}]$, by the definition of an ideal, then $(1) = \mathbb{Z}[\sqrt{-5}]$. ✓

For $a = -1$, $(a) = (-1)$. Since $-1 \in (-1)$, and $-1 \in \mathbb{Z}[\sqrt{-5}]$, then $-1 \cdot -1 = 1 \in (-1)$, since (-1) is an ideal. But by the above $1 \in (-1)$ implies $(-1) = \mathbb{Z}[\sqrt{-5}]$.

So for either possible a, we get $(a) = \mathbb{Z}[\sqrt{-5}]$, which then implies $(3, 1+\sqrt{-5}) = \mathbb{Z}[\sqrt{-5}]$ since we assumed $(3, 1+\sqrt{-5}) = (a)$. ✓

Since $1 \in \mathbb{Z}[\sqrt{-5}]$, then if $(3, 1+\sqrt{-5}) = \mathbb{Z}[\sqrt{-5}]$, we have $1 \in (3, 1+\sqrt{-5})$, so we can write $1 = 3\alpha + (1+\sqrt{-5})\beta$, for some $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$.

Let $\alpha = x_1 + y_1\sqrt{-5}$, $\beta = x_2 + y_2\sqrt{-5}$, for some $x_1, x_2, y_1, y_2 \in \mathbb{Z}$.

Then:

$$\begin{aligned} 1 &= 3\alpha + (1+\sqrt{-5})\beta \\ &= 3(x_1 + y_1\sqrt{-5}) + (1+\sqrt{-5})(x_2 + y_2\sqrt{-5}) \\ &= (3x_1 + x_2 - 5y_2) + (3y_1 + x_2 + y_2)\sqrt{-5} \end{aligned}$$ ✓

So that:

$$\begin{cases} 3x_1 + x_2 - 5y_2 = 1 \\ 3y_1 + x_2 + y_2 = 0 \end{cases}$$

Subtracting the second from the first gives:

$$\begin{aligned} & 3x_1 - 3y_1 - 5y_2 - y_2 = 1 - 0 \\ \Rightarrow \quad & 3x_1 - 3y_1 - 6y_2 = 1 \end{aligned}$$

Since $3 \mid 3$, and $3 \mid 6$, we see that 3 divides the left hand side, and so 3 must divide the right hand side, but $3 \nmid 1$, contradiction. So $N(a) = 1$ is not possible. ✓ good.

Hence neither $N(a) = 1$, nor $N(a) = 3$ is possible, but these were the only possibilities for such an a.

So $(3, 1+\sqrt{-5}) \neq (a)$ for any $a \in \mathbb{Z}[\sqrt{-5}]$, so $(3, 1+\sqrt{-5})$ is not a principal ideal. ✓ Well done!

68) For $a, b \in \mathbb{Z}$, with $d = \gcd(a,b)$, to show $(a,b) = (d)$, show that both $(a,b) \subseteq (d)$, and $(d) \subseteq (a,b)$, which then implies the required equality.

Note that:

$$(a,b) = \{ ax + by \mid x, y \in \mathbb{Z} \}$$
$$(d) = \{ dk \mid k \in \mathbb{Z} \}.$$ ✓

— For $(a,b) \subseteq (d)$:

Take any $n = ax + by \in (a,b)$, with $x, y \in \mathbb{Z}$.

Since $d = \gcd(a,b)$, then d divides a and b, since d is the greatest common <u>divisor</u> of a and b. So we can write $a = d\alpha$, $b = d\beta$, for some $\alpha, \beta \in \mathbb{Z}$.

Then:

$$\begin{aligned} n &= ax + by \\ &= (d\alpha)x + (d\beta)y \\ &= d(\alpha x + \beta y) \\ &= dk, \text{ for some } k = \alpha x + \beta y \in \mathbb{Z}. \end{aligned}$$

So $n \in (d)$, and $(a,b) \subseteq (d)$. ✓

— For $(d) \subseteq (a,b)$:

Take any $n = kd \in (d)$.

Since $d = \gcd(a,b)$; then by the Extended Euclidean algorithm we can write $d = a\alpha + b\beta$, for some $\alpha, \beta \in \mathbb{Z}$. ✓

Then:

$$\begin{aligned} n &= kd \\ &= k(a\alpha + b\beta) \\ &= a(k\alpha) + b(k\beta) \\ &= ax + by, \text{ for some } x = k\alpha,\ y = k\beta \in \mathbb{Z}. \end{aligned}$$ ✓

Algebra and Number Theory

So $n \in (a,b)$, and $(d) \subseteq (a,b)$

So we have $(a,b) = (d)$ as required. ✓

Absolutely perfect!
Thank you!