Michaelmas 2012, NT III/IV, Solutions to Problem Sheet 2.

1. (i) Factorization of the norm of $8+9i$ gives

$$N(8+9i) = 145 = 5 \cdot 29\,,$$

which already shows that any possibly *proper* (and non-unit) factor has either norm equal to 5 or 29. The latter two are prime in $\mathbb{Z}$ and thus irreducible, which entails that a proper (non-zero) factor of $8+9i$ must be irreducible, too. ⟦If it weren't, the corresponding decomposition would cast a "shadow" decomposition in $\mathbb{Z}$ also.⟧
Since $2^2+1^2=5$, candidates for divisors are $2 \pm i$, and trial division gives $\frac{8+9i}{2+i} = 5+2i$, and by the above argument we already know that $2+i$ and $5+2i$ must be irreducible.

(ii) We have $N(11+\sqrt{-5}) = 125 = 2 \cdot 3^2 \cdot 7$, and we can find divisors $1 \pm \sqrt{-5}$ and $2 \pm \sqrt{-5}$ with norms 6 and 9, respectively. Trial division gives

$$\frac{11+\sqrt{-5}}{1-\sqrt{-5}} = 1+2\sqrt{-5} \qquad \text{and} \qquad \frac{11+\sqrt{-5}}{2+\sqrt{-5}} = 3-\sqrt{-5}\,,$$

so that

$$(1-\sqrt{-5})(1+2\sqrt{-5}) = (2+\sqrt{-5})(3-\sqrt{-5})\,.$$

All four factors are irreducible: they have norms 6, 21 (on the left) and 9, 14 (on the right), and any proper factor of either one would have norm 2, 3 or 7, neither one of which is of the form a^2+5b^2 with $a, b \in \mathbb{Z}$.
Furthermore, since all 4 norms are mutually different, none of the factors can be associate to any of the others; thus we have two essentially different decompositions.

(iii) The norm of a proper non-unit factor of $1+\sqrt{-13}$ would need to properly divide $N(1+\sqrt{-13}) = 14 = 2 \cdot 7$ (and could not be a unit), so it would satisfy $a^2+13b^2 \in \{2,7\}$ which is not possible with a, $b \in \mathbb{Z}$. Thus $1+\sqrt{-13}$ must be irreducible.
But while $1+\sqrt{-13}$ divides its own norm $(1+\sqrt{-13})(1-\sqrt{-13}) = N(1+\sqrt{-13}) = 2 \cdot 7$ $(*)$, it neither divides 2 nor 7 ⟦e.g., $\frac{2}{1+\sqrt{-13}} = \frac{2-2\sqrt{-13}}{14} \notin \mathbb{Z}[\sqrt{-13}]$ ⟧. Hence $1+\sqrt{-13}$ is not prime in $\mathbb{Z}[\sqrt{-13}]$.
From the lectures, we know that in a UFD "prime $\Leftrightarrow$ irreducible", so $\mathbb{Z}[\sqrt{-13}]$ cannot be (our example $1+\sqrt{-13}$ violates this), Alternatively, we see that $1-\sqrt{-13}$ is similarly irreducible, as are 2 and 7 (no proper non-unit factor of their norms 2^2 and 7^2 can be a norm by the above), and so $(*)$ above two essentially different decompositions into irreducibles.

2. Let $d < -2$. The norm of 2 in $\mathbb{Z}[\sqrt{d}]$ is equal to 2^2. Any proper non-unit factor $a+b\sqrt{d}$ of it would have to have norm 2 (since d is negative, all norms are $\geqslant 0$), i.e., we would have $a^2-b^2D=2$. But $-b^2d > 2b^2$ by assumption, so necessarily $b=0$ and $a^2=2$ which is impossible for $a \in \mathbb{Z}$.

In 2 (iii) we already had two essentially different decompositions into irreducibles (see $(*)$)

$$(1+\sqrt{-13})(1-\sqrt{-13}) = 2 \cdot 7\,,$$

so neither of the 4 factors—and in particular the factor 2—can be prime.

3. (i) As we saw in Q12, Sheet2, $1+\sqrt{-26}$ is irreducible in R and, hence, so also is $1-\sqrt{-26}$.

   Moreover, 3 is irreducible in R. $[\![$For if $\alpha\,(=a+b\sqrt{-26}$ with $a,b\in\mathbb{Z})$ were a proper, non-unit, divisor of 3, then $\mathrm{N}(\alpha)\,(=a^2+26b^2)$ would have to be a proper divisor of $\mathrm{N}(3)=9$ other than 1. So $a^2+26b^2=3$, and this is not possible with $a,b\in\mathbb{Z}$, a contradiction.$]\!]$

   Thus we have two essentially different factorizations of 27:
$$3^3=\beta\bar{\beta}. \qquad (*)$$
   (There are 3 irreducibles on the left and only two on the right so we don't even need to point out that the irreducibles are not associate!)

   Conclusion: R is not a UFD.

4. Let $u=2+\sqrt{5}$ and $v=-2+\sqrt{5}$ then u and $v\in\mathbb{Z}[\sqrt{5}]$.
   Moreover, $uv=-4+5=1$. So u is a unit of $\mathbb{Z}[\sqrt{5}]$ and, clearly, $u>1$.
   Again $u^2v^2=(uv)^2=1$ and $u^2>u>1$.
   So $u^2\,(=9+4\sqrt{5})$ is another unit greater than 1.

5. (i) For this problem we work in $R=\mathbb{Z}[i]$. We are given that R is a UFD.
   First note that $R^*=\{\pm1,\ \pm i\}$.
   Also, $N(1+i)=2$ has no proper divisors in $\mathbb{Z}$ (except units).
   So $1+i$ is irreducible in R.
   Suppose, then, that we have x and y in $\mathbb{Z}$ such that $x^2+1=y^7$.
   Put $\alpha=x+i\in R$, so that we have $\alpha\bar{\alpha}=y^7$.
   Now if π is an irreducible of R which divides both α and $\bar{\alpha}$ then
$$\pi\mid(\alpha-\bar{\alpha})=2i=(1+i)^2.$$
   So, by uniqueness of factorization, $\pi\sim 1+i$. (1)

   We now write down a prime power factorization of α in R:
$$\alpha=u(1+i)^r\pi_1^{s_1}\pi_2^{s_2}\cdots\pi_t^{s_t}$$
   where $u\in R^*$ and the π_j are irreducibles of R which are pairwise non-associate and not associate to $1+i$, and where $r\in\mathbb{Z}^{\geq 0}$ and the $s_j\in\mathbb{N}$.
   Then (noting $1-i=(-i)(1+i)$)
$$\bar{\alpha}=\big(\bar{u}(-i)^r\big)(1+i)^r\bar{\pi}_1^{s_1}\bar{\pi}_2^{s_2}\cdots\bar{\pi}_t^{s_t}.$$
   By (1), the associates of $1+i$ are the only primes which can divide both α and $\bar{\alpha}$.
   So $\bar{\pi}_j\not\sim\pi_k$ for any j, k. Hence
$$y^7=\alpha\bar{\alpha}=(-i)^r(1+i)^{2r}\pi_1^{s_1}\pi_2^{s_2}\cdots\pi_t^{s_t}\bar{\pi}_1^{s_1}\bar{\pi}_2^{s_2}\cdots\bar{\pi}_t^{s_t}$$
   is a factorization of y^7 as a product of (a unit and) powers of non-associate irreducibles. And by uniqueness of factorization, this must arise from the seventh power of a similar factorization of y. But then the power of each irreducible must be a multiple of 7.

   So $7\mid 2r$ (whence $7\mid r$) and $7\mid s_j$ for each j.

   Now we can take $\beta=u^3(1+i)^{r/7}\pi_1^{s_1/7}\pi_2^{s_2/7}\cdots\pi_t^{s_t/7}\ \in R$.
   Noting (since $u^4=1$) that $(u^3)^7=u^{21}=u$, we have $\alpha=\beta^7$.
   Putting $\beta=a+bi$ with a, b in $\mathbb{Z}$ we have
$$x+i=a^7+7a^6bi-21a^5b^2-35a^4b^3i+35a^3b^4+21a^2b^5i-7ab^6-b^7i\,. \qquad (2)$$
   Equating imaginary parts we get
$$1=7a^6b-35a^4b^3+21a^2b^5-b^7=(7a^6-35a^4b^2+21a^2b^4-b^6)b.$$

Whence $b \mid 1$ and so $b = \pm 1$, $b^2 = 1$ and consequently $b = 7a^6 - 35a^4 + 21a^2 - 1$.

But then $b \equiv -1 \mod 7$ and so $b = -1$.

And now we have $7a^6 - 35a^4 + 21a^2 = 0$. i.e. $a^2(a^4 - 5a^2 + 3) = 0$.

So either $a = 0$ or, solving the quadratic, $a^2 = (5 \pm \sqrt{13})/2 \notin \mathbb{Z}$.

Hence $a = 0$ and $x + i = -(-1)^7 i = i$. So $x = 0$ and $y = 1$. This is the only solution.

(ii) We work in $R = \mathbb{Z}[\sqrt{-2}]$ — a UFD. We sort out some preliminaries.

Firstly, $R^* = \{\pm 1\}$.

Secondly, $N(\sqrt{-2}) = 2$ has no proper (non-unit) divisors in $\mathbb{Z}$.

So $\sqrt{-2}$ is irreducible in R.

Suppose then that we have x and y in $\mathbb{Z}$ such that $x^2 + 8 = y^3$.

Put $\alpha = x + \sqrt{-2} \in R$ so that we have $\alpha\bar{\alpha} = y^3$.

Now if π is an irreducible of R which divides both α and $\bar{\alpha}$ then

$$\pi \mid (\alpha - \bar{\alpha}) = 4\sqrt{-2} = (\sqrt{-2})^5.$$

So, by uniqueness of factorization, $$\pi \sim \sqrt{-2}. \tag{1}$$

We now write down a prime power factorization of α in R:

$$\alpha = \pm(\sqrt{-2})^r \pi_1^{s_1} \pi_2^{s_2} \cdots \pi_t^{s_t},$$

where the π_i are irreducibles of R, pairwise non-associate and not associate to $\sqrt{-2}$, and where $r \in \mathbb{N} \cup \{0\}$ and the $s_i \in \mathbb{N}$. Then

$$\bar{\alpha} = \pm(-1)^r(\sqrt{-2})^r \bar{\pi}_1^{s_1} \bar{\pi}_2^{s_2} \cdots \bar{\pi}_t^{s_t}.$$

By (1), the associates of $\sqrt{-2}$ are the only irreducibles of R which can divide both α and $\bar{\alpha}$. So $\bar{\pi}_i \not\sim \pi_j$ for any i, j. Hence

$$y^3 = \alpha\bar{\alpha} = (-1)^r(\sqrt{-2})^{2r} \pi_1^{s_1} \pi_2^{s_2} \cdots \pi_t^{s_t} \bar{\pi}_1^{s_1} \bar{\pi}_2^{s_2} \cdots \bar{\pi}_t^{s_t}$$

is a factorization of y^3 as a product of (a unit and) powers of non-associate irreducibles and, by uniqueness of factorization, this must arise from the third power of a similar factorization of y.

But then the power of each irreducible must occur as a cube.

So $3 \mid 2r$ (whence $3 \mid r$) and $3 \mid s_i$ for each i.

Now we can take $\beta = \pm(\sqrt{-2})^{r/3} \pi_1^{s_1/3} \pi_2^{s_2/3} \cdots \pi_t^{s_t/3} \in R$ and we have $\alpha = \beta^3$.

Putting $\beta = a + b\sqrt{-2}$ with a, b in $\mathbb{Z}$ we have

$$x + 2\sqrt{-2} = a^3 + 3a^2 b\sqrt{-2} - 6ab^2 - 2b^3\sqrt{-2}\,. \tag{2}$$

Equating imaginary parts (i.e. coefficients of $\sqrt{-2}$) we get

$$2 = 3a^2 b - 2b^3 = b(3a^2 - 2b^2). \tag{3}$$

Whence $b \mid 2$ and so $b = \pm 1$, or ± 2.

Reducing (3) mod 3 we find $-2b^3 \equiv 2 \mod 3$.

But $b^3 \equiv b \mod 3$ (Fermat) and so $b \equiv -1 \mod 3$. So $b = -1$ or 2.

Putting $b = 2$ in (3) gives $a^2 = 3$. So $b = -1$ and and (3) gives $a = 0$.

Hence, from (2), $x = 0$ and so $y = 2$. This is the only solution.

6. (i) Suppose that $\alpha = a + b\sqrt{-2}$ $(a, b \in \mathbb{Z})$ is a proper divisor of 5 in R then $a^2 + 2b^2 = \alpha\bar{\alpha}$ is a proper divisor of 5^2.

So $a^2 + 2b^2 = 1$ or 5.

If $|b| \geq 2$ the LHS is too big and $|b| = 1$ is clearly not possible.

So $b = 0$, $a = 1$, $\alpha\bar{\alpha} = 1$ and α is a unit.

Thus the only proper divisors of 5 in R are units and so 5 is irreducible.

So $5 = 5$, as a product of one or more irreducibles.

$19 = (1+3\sqrt{-2})(1-3\sqrt{-2})$ and we claim that this is a product of irreducibles.
Suppose that $\alpha = a + b\sqrt{-2}$ $(a, b \in \mathbb{Z})$ is a proper divisor of $1+3\sqrt{-2}$ in R.
Then $a^2+2b^2 = \alpha\bar{\alpha}$ is a proper divisor of $(1+3\sqrt{-2})(1-3\sqrt{-2}) = 19$ (and 19 is prime in $\mathbb{Z}$).

So $a^2 + 2b^2 = 1$, $\alpha\bar{\alpha} = 1$ and α is a unit.

Thus the only proper divisors of $1+3\sqrt{-2}$ in R are units.

Hence $1+3\sqrt{-2}$ and (similarly) $1-3\sqrt{-2}$ are irreducible, as claimed.

$43 = (5+3\sqrt{-2})(5-3\sqrt{-2})$ and we claim that this is a product of irreducibles.
Suppose that $\alpha = a + b\sqrt{-2}$ $(a, b \in \mathbb{Z})$ is a proper divisor of $5+3\sqrt{-2}$ in R.
Then $a^2+2b^2 = \alpha\bar{\alpha}$ is a proper divisor of $(5+3\sqrt{-2})(5-3\sqrt{-2}) = 43$ (and 43 is prime in $\mathbb{Z}$).

So $a^2 + 2b^2 = 1$, $\alpha\bar{\alpha} = 1$ and α is a unit.

Thus the only proper divisors of $5+3\sqrt{-2}$ in R are units and so $5+3\sqrt{-2}$ and (similarly) $5-3\sqrt{-2}$ are irreducible, as claimed.

(ii) Note that, since $R^\times = \{\pm 1\}$, no pair of the irreducibles found in (a) can be associate. So, since R is a UFD,

$817 (= 19 \times 43) = (1+3\sqrt{-2})^1(1-3\sqrt{-2})^1(5+3\sqrt{-2})^1(5-3\sqrt{-2})^1$

is a prime power factorization of 817 (in powers of non-associate primes of R). So (using Uniqueness of Factorization) 817 has the following 32 factors

$$\alpha = \pm(1+3\sqrt{-2})^r(1-3\sqrt{-2})^s(5+3\sqrt{-2})^t(5-3\sqrt{-2})^u \qquad (*)$$

where r, s, t and u are 0 or 1.

(iii) Putting $\alpha = a + b\sqrt{-2} \in R$, we require $\alpha\bar{\alpha} = 817$. In particular, $\alpha \mid 817$ in R so α is as in $(*)$.

But, with α as in $(*)$, $\alpha\bar{\alpha} = 19^{r+s}43^{t+u}$.

So $\alpha\bar{\alpha} = 817$ iff $r+s = 1$ and $t+u = 1$. So we have a free choice of the sign and r and t (to be 0 or 1), giving 8 solutions to $\alpha\bar{\alpha} = 817$ and 8 (integer) solutions to $a^2 + 2b^2 = 817$.
We find that

$(1+3\sqrt{-2})(5+3\sqrt{-2}) = -13 + 18\sqrt{-2}$ and $(1+3\sqrt{-2})(5-3\sqrt{-2}) = 23 + 12\sqrt{-2}$.

So the eight solutions to $a^2 + 2b^2 = 817$ must be

$(a, b) = (\pm 13, \pm 18)$ or $(\pm 23, \pm 12)$.

Therefore there are two solutions with a and b positive:

$(a, b) = (13, 18)$ or $(23, 12)$.

7. (i) $\underline{HJ}$: By definition HJ is the subgroup generated by the elements hj where $h \in H$ and $j \in J$.

$\underline{H+J}$: Let a and b be elements of $H+J$.

We must show $a \pm b \in H+J$. ($H+J$ is clearly non-empty.)

Well, $a = h + j$ and $b = k + l$ for some h and $k \in H$ and j and $l \in J$.
But H and J are subgroups. So $h \pm k \in H$ and $j \pm l \in J$.

Whence $a \pm b = (h \pm k) + (j \pm l) \in H + J$, as required.

(ii) $H(I+J)$ is the subgroup of R generated by

all elements hk where $h \in H$ and $k \in I + J$,
i.e. all elements $h(i+j)$ where $h \in H$ and $i \in I$ and $j \in J$.
But $h(i+j) = hi + hj \in HI + HJ$.
So $HI + HJ$ contains all the generators of $H(I+J)$.
Hence $HI + HJ$ contains $H(I+J)$.

OTOH, HI and HJ are contained in $H(I+J)$. So $H(I+J)$ contains $HI + HJ$.
Thus $H(I+J) = HI + HJ$.

(iii) (Using the associative and commutative rules: $H(IJ) = (HI)J$ and $HI = IH$ and (iv).)

We know that HI is a subgroup.
Moreover, $R(HI) = (RH)I = (HR)I = H(RI) = HI$.
So, by (iv), HI is an ideal.

(iv) If $RI = I$ then, for all $r \in R$ and $i \in I$, $ri \in I$. So I is an ideal.

OTOH suppose that I is an ideal.

RI is the subgroup of R generated by all elements ri where $r \in R$ and $i \in I$.
But all these elements lie in I, as I is an ideal.
So $RI \subseteq I$.

But $1 \in R$. So, for all $i \in I$, $i = 1i \in RI$. So $I \subseteq RI$.
Hence $RI = I$.

8. (i) $(a)_R = \{ra \mid r \in R\}$ and $(b)_R = \{sb \mid s \in R\}$.
So $(a)_R(b)_R$ is generated by the elements $rasb = rsab$, with $r, s \in R$.
All these generators lie in $(ab)_R$. So $(a)_R(b)_R \subseteq (ab)_R$.

OTOH, clearly ab and all its multiples lie in $(a)_R(b)_R$. So $(a)_R(b)_R \supseteq (ab)_R$.
Thus $(a)_R(b)_R = (ab)_R$.

(ii) $\langle a\rangle_{\mathrm{gp}} = \{ra \mid r \in \mathbb{Z}\}$ and $\langle b\rangle_{\mathrm{gp}} = \{sb \mid s \in \mathbb{Z}\}$.
So $\langle a\rangle_{\mathrm{gp}}\langle b\rangle_{\mathrm{gp}}$ is generated by the elements $rasb = rsab$, with $r, s \in \mathbb{Z}$.
All these generators lie in $\langle ab\rangle_{\mathrm{gp}}$. So $\langle a\rangle_{\mathrm{gp}}\langle b\rangle_{\mathrm{gp}} \subseteq \langle ab\rangle_{\mathrm{gp}}$.

OTOH, clearly ab and all its integer multiples lie in $\langle a\rangle_{\mathrm{gp}}\langle b\rangle_{\mathrm{gp}}$.
So $\langle a\rangle_{\mathrm{gp}}\langle b\rangle_{\mathrm{gp}} \supseteq \langle ab\rangle_{\mathrm{gp}}$.
Thus $\langle a\rangle_{\mathrm{gp}}\langle b\rangle_{\mathrm{gp}} = \langle ab\rangle_{\mathrm{gp}}$.

(iii)

$$\begin{aligned}
\langle a,b\rangle_{\mathrm{gp}}\langle c,d\rangle_{\mathrm{gp}} &= (\langle a\rangle_{\mathrm{gp}} + \langle b\rangle_{\mathrm{gp}})(\langle c\rangle_{\mathrm{gp}} + \langle d\rangle_{\mathrm{gp}}) \\
&= \langle a\rangle_{\mathrm{gp}}(\langle c\rangle_{\mathrm{gp}} + \langle d\rangle_{\mathrm{gp}}) + \langle b\rangle_{\mathrm{gp}}(\langle c\rangle_{\mathrm{gp}} + \langle d\rangle_{\mathrm{gp}}) \\
&= \langle a\rangle_{\mathrm{gp}}\langle c\rangle_{\mathrm{gp}} + \langle a\rangle_{\mathrm{gp}}\langle d\rangle_{\mathrm{gp}} + \langle b\rangle_{\mathrm{gp}}\langle c\rangle_{\mathrm{gp}} + \langle b\rangle_{\mathrm{gp}}\langle d\rangle_{\mathrm{gp}} \\
&= \langle ac\rangle_{\mathrm{gp}} + \langle ad\rangle_{\mathrm{gp}} + \langle bc\rangle_{\mathrm{gp}} + \langle bd\rangle_{\mathrm{gp}} = \langle ac, ad, bc, bd\rangle_{\mathrm{gp}}
\end{aligned}$$

9. Suppose $\quad (\alpha, \beta)_R = (\gamma) \quad (*)$

We have to show that γ is a gcd for α and β. i.e that
(i) γ divides α and β and
(ii) if $\delta \in R$ and δ divides α and β then δ divides γ.

But from $(*)$, α and $\beta \in (\gamma)_R$. So $\gamma \mid \alpha$ and β. whence (i)

OTOH, $\quad (\alpha, \beta)_R = \{l\alpha + \mu\beta \mid l, \mu \in R\}$.
So, again from $(*)$, we can write $\gamma = l\alpha + \mu\beta$ for some l, $\mu \in R$.
Thus if $\delta \in R$ and $\delta \mid \alpha$ and β then $\delta \mid l\alpha + \mu\beta = \gamma$. whence (ii)
Hence γ is a gcd for α and β.

10. Multiplying the two ideals gives (denoting generators by $g_1, g_2, \dots$)

$$\begin{aligned}
(5, 2+\sqrt{-21})(3, \sqrt{-21}) &= (15, 5\sqrt{-21}, 6+3\sqrt{-21}, -21+2\sqrt{-21}) \\
&= (15, 5\sqrt{-21}, 6+3\sqrt{-21}, -27-\sqrt{-21}) \qquad (g_4 \to g_4 - g_3) \\
&= (15, -135, 6+3\sqrt{-21}, -27-\sqrt{-21}) \qquad (g_2 \to g_2 + 5g_4) \\
&= (15, -135, -75, -27-\sqrt{-21}) \qquad (g_3 \to g_3 + 3g_4) \\
&= (15, -27-\sqrt{-21}) \qquad (-135 \text{ and } -75 \text{ are multiples of } g_1 = 15)\,.
\end{aligned}$$

Hence e.g. $N = 15$ and $\alpha = -27 - \sqrt{-21}$ will do.

11. See Problems Class.

12. (i) Put $\beta = 1 + \sqrt{-26}$. Note that β is irreducible in R.
⟦If $\alpha\,(= a + b\sqrt{-26}$ with $a, b \in \mathbb{Z})$ is a proper, non-unit, divisor of β, then $\mathrm{N}(\alpha)\,(= a^2 + 26b^2)$ must be a proper divisor of $\mathrm{N}(\beta) = 27$ other than 1. So $a^2 + 26b^2 = 3$ or 9, giving $b = 0$, $\alpha = a = \pm 3$ and $\beta/\alpha = \pm(1+\sqrt{-26})/3 \notin R$, a contradiction.⟧

Now, denoting by g_i the i-th generator in a given presentation of an ideal, we can deduce

$$\begin{aligned}
J^3 &= (\beta, 3)_R^2(\beta, 3)_R = (\beta^2, 3\beta, 3^2)_R(\beta, 3)_R \\
&= (\beta^3, 3\beta^2, 3^2\beta, 3^3)_R \\
&= \beta(\beta^2, 3\beta, 9, \bar{\beta})_R = \beta(-25+2\sqrt{-26}, 3+3\sqrt{-26}, 9, 1-\sqrt{-26})_R \\
&= \beta(-23, 6, 9, 1-\sqrt{-26})_R, \quad \text{replace } g_1 \text{ by } g_1 + 2g_4 \text{ and } g_2 \text{ by } g_2 + 3g_4, \\
&= \beta(1, 6, 9, 1-\sqrt{-26})_R, \qquad \text{replace } g_1 \text{ by } g_1 + 4g_2, \\
&= \beta R = (\beta)_R.
\end{aligned}$$

since any ideal containing 1 is R. Thus J^3 is a principal ideal.

⟦Note that if an ideal I is generated by multiples of a given element x, say $I = (a_1x, \dots, a_nx)_R$, one can only deduce that it is *contained* in the principal ideal $(x)_R$ but need not itself contain x; the latter still needs to be shown if equality is to be proved.⟧

Now suppose that J were principal, i.e. $J = (\gamma)_R$ with $\gamma \in R$.
Then $(\beta)_R = J^3 = (\gamma^3)_R$. So $\beta = u\gamma^3$ where $u \in R^\times$.
This is impossible, since β is irreducible.
Conclusion: J is not principal.

(ii) Again, suppose, for a contradiction, that J^2 were principal, say $J^2 = (\delta)_R$.
Then $(\delta^3)_R = (\delta)_R^3 = J^6 = (\beta)_R^2 = (\beta^2)_R$ with β as in (i).
So $\delta^3 = u\beta^2$, for some unit $u \in R^\times$.
And, hence, $(\delta\bar{\delta})^3 = (\mathrm{N}(\beta))^2 = 3^6$, and $\mathrm{N}(\delta) = 9$.
But $\beta \in J^3 \subseteq J^2 = (\delta)_R$.
Since $\mathrm{N}(\delta) < \mathrm{N}(\beta)$, δ is a proper divisor of the irreducible β but is not a unit. There are no such elements δ.
Conclusion: J^2 is not principal. (There are many ways to show this.)

(iii) Consider $\phi : \mathbb{Z}[\sqrt{-26}] \to \mathbb{Z}_3$, by $\phi : a + b\sqrt{-26} \mapsto a - b \mod 3$.
Note that the coefficient in front of b on the RHS has to be a square root of -26, viewed mod 3, i.e. has to be a residue r which satisfies $r^2 \equiv -26 \pmod 3$.

Claim: ϕ is a ring homomorphism:

- $\phi(1) = \phi(1 + 0\sqrt{-26}) = 1 \mod 3$. ⟦We can usually drop this check.⟧

- $$\begin{aligned} \phi\big((a+b\sqrt{-26}) \;+\; (a'+b'\sqrt{-26})\big) &= \phi((a+a') + (b+b')\sqrt{-26})) \\ &= a + a' - (b+b') \mod 3 \\ &= a - b + a' - b' \mod 3 \\ &= \phi(a+b\sqrt{-26}) + \phi(a'+b'\sqrt{-26}). \end{aligned}$$

- $$\begin{aligned} \phi\big((a+b\sqrt{-26})(a'+b'\sqrt{-26})\big) &= \phi((aa' - 26bb') + (a'b + ab')\sqrt{-26}) \\ &= aa' - 26bb' - (a'b + ab') \mod 3 \\ &= aa' + bb' - (a'b + ab') \mod 3 \\ &= (a-b)(a'-b') \mod 3 \\ &= \phi(a+b\sqrt{-26})\phi(a'+b'\sqrt{-26}). \end{aligned}$$

So ϕ is a ring homomorphism.

Claim: $\ker\phi = J$.

Now $\phi(3) = 0 = \phi(1+\sqrt{-26})$ whence 3 and $1+\sqrt{-26}$ lie in $\ker\phi$. So $J = (3, 1+\sqrt{-26})_R \subseteq \ker\phi$.

On the other hand, if $\alpha = a + b\sqrt{-26} \in \ker\phi$ then $a - b \equiv 0 \mod 3$, say $a = b + 3t$, with $t \in \mathbb{Z}$.

So $\alpha = 3t + b(1+\sqrt{-26}) \in (3, 1+\sqrt{-26})_R = J$.

Hence $\ker\phi \subseteq J$ and so $\ker\phi = J$.

Now ϕ is clearly surjective with image $\mathbb{Z}_3$. So, by the first isomorphism theorem for rings, $R/J \cong \mathbb{Z}_3$, a field. And hence J is maximal, as required.