2016/17 Exam Paper

3(a) $a \in R$ is a <u>unit</u> if

$\exists b \in R$ s.t. $ab = 1 = ba$.

A non-zero non-unit $p \in R$ is

- prime if $\forall a, b \in R$,

  $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

- irreducible if $\forall a, b \in R$,

  $p = ab \Rightarrow a$ or b is a unit.

(b)(i) R is a UFD if

- every non-zero non-unit can be written as a product of finitely many irreducibles in R, and
- given two such decompositions

  $r_1 \cdots r_s = r_1' \cdots r_t'$,

$s = t$, and (after renumbering)

$Rr_i = Rr_i'$ $\forall\ 1 \leq i \leq s$.

(ii) Let R be a UFD. Then

$p \in R$ prime $\iff p \in R$ irreducible.

($\Rightarrow$) If $p = ab$, then $p \mid ab$,

so p prime gives (say) $p \mid a$,

ie. $a = pc$ for some $c \in R$.

Sub. this into $p = ab$, and cancel p's (since R is a integral domain) to see that b is a unit.

($\Leftarrow$) Suppose $p \mid ab$. If either a or b is a unit, we're done. If not, take irreducible factorisations of both, so

$$ab = (p_1 \cdots p_s)(p_1' \cdots p_t')$$

with each p_i, p_j' irreducible. Since p is irreducible, it is (up to a unit) one of these factors, i.e.

$\exists$ unit $u \in R$ s.t.

- $p = up_i$, so $p \mid a$, or
- $p = up_j'$, so $p \mid b$,

as required. □.

(c)(i) Let $\alpha = a + ib$.

($\Rightarrow$) Suppose $\exists \beta \in \mathbb{Z}[i]$ s.t. $\alpha\beta = 1$. Then

$$N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1.$$

Since $N(\alpha), N(\beta) \in \mathbb{Z}_{\geq 0}$, we have $N(\alpha) = 1$.

($\Leftarrow$) Suppose

$$1 = N(\alpha) = a^2 + b^2 = (a+ib)(a-ib)$$
$$= \alpha(a-ib).$$

Then α is a unit, since $a-ib \in \mathbb{Z}[i]$. □.

(ii) Let $N(\alpha) \in \mathbb{Z}$ be prime. Suppose $\alpha = a+ib$ is not prime. Using the fact that $\mathbb{Z}[i]$ is a UFD, by (b)(ii), α is not irreducible, so $\exists \alpha_1, \alpha_2 \in \mathbb{Z}[i]$ non-zero non-units s.t. $\alpha = \alpha_1\alpha_2$, so $N(\alpha) = N(\alpha_1\alpha_2) = N(\alpha_1)N(\alpha_2)$. Each $N(\alpha_i)$ is non-zero, and a non-unit by (c)(i), so $N(\alpha)$ is not irreducible. Using the fact that $\mathbb{Z}$ is a UFD, by (b)(ii), $N(\alpha)$ is not prime. □

(d) $2+i = i(1-2i)$, and $i \in \mathbb{Z}[i]$ is a unit $(i \cdot (-i) = 1)$.

Hence $\mathbb{Z}[i](2+i) = \mathbb{Z}[i](1-2i)$.

Similarly, $2-i = (-i)(1+2i)$,

so $\mathbb{Z}[i](2-i) = \mathbb{Z}[i](1+2i)$.

This is consistent with $\mathbb{Z}[i]$ being a UFD.

2(d) For a ring homomorphism $\varphi : R \longrightarrow S$, there is an isomorphism

$$R/\ker(\varphi) \cong \mathrm{Im}(\varphi).$$

Sketch proof:

- Consider $\bar{\varphi} : R/\ker(\varphi) \longrightarrow \mathrm{Im}(\varphi)$ defined by

$$\bar{\varphi}([a]) = \varphi(a),$$

which is well-defined because for $a, b \in R$,

$$[a] = [b] \iff a - b \in \ker(\varphi)$$
$$\iff \varphi(a-b) = 0$$
$$\iff \varphi(a) = \varphi(b). \quad (*)$$

- $\bar{\varphi}$ is a ring homomorphism:

$$\bar{\varphi}([a]+[b]) = \bar{\varphi}([a+b])$$
$$= \varphi(a) + \varphi(b) = \bar{\varphi}([a]) + \bar{\varphi}([b]),$$
$$\bar{\varphi}([a]\cdot[b]) = \bar{\varphi}([a\cdot b])$$
$$= \varphi(a)\varphi(b) = \bar{\varphi}(a)\bar{\varphi}(b).$$

- It's clearly surjective. It's injective by $\Leftarrow$ implication in $(*)$. So $\bar{\varphi}$ is a bijection.
- A ring homomorphism that is bijective is an isomorphism, so $\bar{\varphi}$ is an isomorphism.