Chapter 10.3 part 2

$R = \mathbb{Z}[\sqrt{-5}] = \{ s + t\sqrt{-5} \mid s, t \in \mathbb{Z} \} \subset \mathbb{C}$

(Ex 4) In R, we have

$$\underline{6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})}$$

- two substantially diferent decompositions of 6 into products of irreducibles

Recall $N(s + t\sqrt{-5}) = s^2 + 5t^2 \geq 0$

Th 10.19 In $\mathbb{Z}[\sqrt{d}]$

(1) $N(a) = 0$ iff $a = 0$

(2) $N(ab) = N(a)N(b)$

Th 10.20 $u \in \mathbb{Z}[\sqrt{d}]$ is a unit iff $N(u) = \pm 1$

Prop $\mathbb{Z}[\sqrt{-5}]$ has no elements a such that $N(a) = 2$ or $N(a) = 3$.

(Ex 3) Pf $N(s + t\sqrt{-5}) = s^2 + 5t^2 \begin{cases} \geq 5 \text{ if } t \neq 0 \\ 1, 4, \text{ or } \geq 9 \text{ if } t = 0 \end{cases}$.

Prop $2, 3, 1 \pm \sqrt{5} \in \mathbb{Z}[\sqrt{-5}]$ are irreducibles

Pf Let $2 = ab$ $a, b \in \mathbb{Z}[\sqrt{-5}]$

$N(2) = N(a)N(b)$

$4 = N(a)N(b)$ either $(2, 2)$ - cannot happen as 2 is a norm of no element

or $(1, 4)$ - one of the factors (a or b)

has norm 1, thus it is a unit.

Thus 2 is irreducible.

Similarly with 3 - also irreducible

Let $1 \pm \sqrt{5} = ab$

$N(1 \pm \sqrt{5}) = N(a)N(b)$

$6 = N(a)N(b)$ either $(2,3)$ - cannot happen: there are no elements of norm 2 or 3

or $(1,6)$ - one of the factors has norm 1, therefore a unit.

Thus $1 \pm \sqrt{5}$ are both irreducibles

Prop 2 and 3 are associates to neither $1+\sqrt{-5}$ nor $1-\sqrt{-5}$

Pf <u>If a and b are associates</u>, $a = bu$, and u is a unit $(N(u) = 1)$

$N(a) = N(b)N(u)$

<u>then $N(a) = N(b)$</u>

$N(2) = 4$

$N(3) = 9$

$N(1 \pm \sqrt{-5}) = 6$

The reason for the existence of the two different factorizations.

Although $2 \in \mathbb{Z}[\sqrt{-5}]$ is irreducible, the principal ideal $\underline{(2) \text{ is not prime}}$.

Prop $\underline{1 \pm \sqrt{-5} \notin (2)}$ while $(1+\sqrt{-5})(1-\sqrt{-5}) = 6 \in (2)$

Pf $(2) = \{2(s+t\sqrt{-5}) \mid s,t \in \mathbb{Z}\}$

To check: for no integers s and t $\quad 1 \pm \sqrt{5} = 2s + 2t\sqrt{-5}$

Same is true about the principal ideals (3), $\underline{(1+\sqrt{-5})}$, $(1-\sqrt{-5})$

– these ideals are not prime.

Prop $\begin{array}{l} 2 \notin (1+\sqrt{-5}) \\ 3 \notin (1+\sqrt{-5}) \end{array}$ while $2 \cdot 3 = 6 \in (1+\sqrt{-5})$

Pf $2 \notin (1+\sqrt{-5})$

$2 \neq (1+\sqrt{-5})c$ for any $c \in \mathbb{Z}[\sqrt{-5}]$

because

$N(2) \neq N(1+\sqrt{-5})N(c)$ for any $c \in \mathbb{Z}[\sqrt{-5}]$

$4 \neq 6N(c)$ – indeed, because $N(c)$ is an integer for any $c \in \mathbb{Z}[\sqrt{-5}]$

How the Fundamental Theorem of Arithmetic can be fixed in way such that the corrected version is true in $\mathbb{Z}[\sqrt{-5}]$?

Think about the factorization for $a \in R$

$$a = p_1 p_2 \dots p_n$$

as a factorization of ideal (a) into a product of ideals

$$(a) = (p_1)(p_2)\dots(p_n)$$

Drop the condition that all ideals are principal, and impose the condition that all ideals are prime ideals.

<u>Def</u> Let I, J be ideals in R

Set

$$IJ = \{ a_1 b_1 + a_2 b_2 + \dots + a_n b_n \mid n \geq 1,\ a_k \in I,\ b_k \in J \}$$

To check: IJ is an ideal

If $I = (x)$ and $J = (y)$ - principal ideals, then so is $IJ = (xy)$

A corrected version of the conclusion of the Fundamental Theorem of Arithmetic:

"every ideal can be written as a product of prime ideals in a unique (up to a permutation of the factors) way"

Back to the example with $\mathbb{Z}[\sqrt{-5}]$.

(Ex 5) The three ideals

$Q_1 = (3, 1+\sqrt{-5})$

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

$Q_2 = (3, 1-\sqrt{-5})$

are all prime ideals, and the unique factorization becomes

$$(6) = \underline{P^2 Q_1 Q_2}$$

$P^2 = (2)$

$PQ_1 = (1+\sqrt{-5})$

$PQ_2 = (1-\sqrt{-5})$

$Q_1 Q_2 = (3)$

$$(6) = \underline{(2)(3)} = P^2 \quad Q_1 Q_2 = PQ_1 \; PQ_2 = \underline{((1+\sqrt{-5}))((1-\sqrt{-5}))}$$

Exercises 14 - 20