Chapter 10.3 part 1

10.3 Factorization of quadratic integers.

Def An integer $d \in \mathbb{Z}$ is called square-free if $c^2 \mid d$, $c \in \mathbb{Z}$ implies $c = \pm 1$

The integer d is not divisible by squares (of integers) besides 1.

$\boxed{\text{Assume that } d \in \mathbb{Z} \text{ is square-free.}}$

Def $\mathbb{Z}[\sqrt{d}] = \{s + t\sqrt{d} \mid s, t \in \mathbb{Z}\} \subset \mathbb{C}$ - complex numbers

$\mathbb{R}$ (reals if $d > 0$)

Easy to check: $\mathbb{Z}[\sqrt{d}]$ is an integral domain.

Norm - a very useful tool in the study of $\mathbb{Z}[\sqrt{d}]$

Def The function $\mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$ given by

$$N(s+t\sqrt{d}) = (s+t\sqrt{d})(s-t\sqrt{d}) = s^2 - dt^2$$

is called <u>norm</u>

Basic properties of norm:

Th 10.19

(1) For $a \in \mathbb{Z}[\sqrt{d}]$, $N(a) = 0$ iff $a = 0$

(2) $N(ab) = N(a)N(b)$ for any $a, b \in \mathbb{Z}[\sqrt{d}]$ } norm is a multiplicative function

Rem For Gaussian integers $\mathbb{Z}[\sqrt{-1}]$, the norm $N(s+t\sqrt{-1}) = s^2+t^2$ makes it into a Euclidean domain.
That is not the case $\mathbb{Z}[\sqrt{d}]$.

Characterization of units

Th10.20 $u \in \mathbb{Z}[\sqrt{d}]$ is a unit iff $N(u) = \pm 1$ | Pf. from 10.19(2) - in the textbook

Prop In $\mathbb{Z}[\sqrt{d}]$, the ACC condition on principal ideals holds

Remark The existence clause in the Fundamental Theorem of Arithmetic follows from that, as discussed in Section 10.2.

| Alternatively, Th10.23 provides another proof, avoiding ACC

Pf From Th10.19 (2): $N(ab) = N(a)N(b)$
implies $|N(ab)| \geq |N(a)|$
$a|c$ implies $|N(c)| \geq |N(a)|$

Let
$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \dots$
be an ascending chain of principal ideals

We have by Lemma 10.19(1)
$a_2|a_1$, $a_3|a_2$ ...

We thus have

$$|N(a_1)| \geq |N(a_2)| \geq |N(a_3)| \geq \dots$$

A decreasing sequence of non-negative integers must stabilize.

$$|N(a_n)| = |N(a_{n+1})| = |N(a_{n+3})| = \dots$$

$a_{n+1} | a_n$ means $\underline{a_{n+1} = c\, a_n}$

$|N(a_{n+1})| = |N(c)||N(a_n)|$ implies $|N(c)| = 1$

means $N(c) = \pm 1$

We conclude that $\underline{c \text{ is a unit}}$, thus a_n and a_{n+1} are associates.

That implies $\underline{(a_n) = (a_{n+1})}$

Similarly $(a_{n+1}) = (a_{n+2}) = \dots$

Thus the chain of ideals stabilizes from some point on, and therefore ACC on principal ideals holds in $\mathbb{Z}[\sqrt{d}]$.