Chapter 10.1 part 2

Chapter 10 Arithmetic in Integral Domains

In Chapters 1 & 4, The Fundamental Theorem of Arithmetic was proved for $\mathbb{Z}$ & $F[x]$ (F is a field)

Every non-zero non-unit element of the ring can be written as a product of irreducibles/primes in an essentially unique way.

"Essentially unique" - up to units and permutations

units - the ring must have identity

permutations - the ring is commutative

exception of zero hints that we possibly want to consider rings without zero divisors.

$ab = 0_R$ while $a \neq 0_R$, $b \neq 0_R$

$\boxed{R \text{ - ring - is an integral domain.}}$

Examples

$\mathbb{Z}$ - the ring of integers (Chapter 1)

$F[x]$ (F is a field) (Chapter 4)

$\mathbb{Z}[x]$

$\{a+bi \mid a,b \in \mathbb{Z}\} \subset \mathbb{C}$

$\{a+b\sqrt{7} \mid a,b \in \mathbb{Z}\} \subset \mathbb{R} \subset \mathbb{C}$

Divisibility $a|b$ means there exist $c \in R$ such that $b = ac$

Units - divisors of $1_R \in R$ $\quad (uv = 1_R, \ u, v \in R)$
$v = u^{-1}$

| $\{-1, 1\}$ in $\mathbb{Z}$
| $\{a \in F \mid a \neq 0_F\}$ in $F[x]$
polynomials of degree zero

Associates a and b are associates means
$a \neq 0_R$ $b \neq 0_R$ $\quad a = bu$, u is a unit

Every non-zero element of R is divisible by all units and all associates of the element.

Irreducible $p \in R$ is called irreducible if p is divisible by
$p \neq 0_R$ nothing besides units and associates of p.
p - not a unit

Th 10.1 Let $p \in R$, $p \neq 0_R$. Then p is irreducible iff whenever $p = rs$, then r or s is a unit (not both).

Section 10.1 Euclidean Domains

Integral domains where The Fundamental Theorem of Arithmetic can be proved by the same argument as in Chapters 1 & 4.

Argument - Euclid's Lemma - assumes a way of measurement.

Def An integral domain R is a <u>Euclidean domain</u> if there is a function

$$\delta : R \setminus \{0_R\} \longrightarrow \{n \in \mathbb{Z} \mid n \geq 0\}$$

which satisfies the following requirements

(i) If $a, b \in R$, both non-zero, then

$$\delta(a) \leq \delta(ab)$$

(ii) If $a, b \in R$, $b \neq 0_R$, then there exist $q, r \in R$ such that

$$a = bq + r \quad \text{and} \quad \text{either } r = 0_R \text{ or } \delta(r) < \delta(b)$$

Examples $\mathbb{Z}$ $\delta(a) = |a|$

$F[x]$ $\delta(f) = \deg f$

Remark Only existence of q and r are required. Uniqueness may be not true and does not matter

$\{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ - the ring of Gaussian integers

$$\delta(a + bi) = a^2 + b^2$$

Th 10.7 The Fundamental Theorem of Arithmetic holds in every Euclidean domain.

The description of units in a Euclidean domain

Th 10.2 Let R be a Euclidean domain. Let $u \in R$, $u \neq 0_R$.

The following three conditions are equivalent

(1) u is a unit in R

(2) $\delta(u) = \delta(1_R)$

(3) $\delta(c) = \delta(cu)$ for some $c \in R$

Pf (1) implies (2)

We use nothing but $\delta(a) \leq \delta(ab)$ } (i) in the definition

$a = 1_R$ $b = u$: $\quad \delta(1_R) \leq \delta(1_R \cdot u) = \delta(u)$ $\quad \delta(1_R) \leq \delta(u)$

$a = u$ $b = u^{-1}$: $\quad \delta(u) \leq \delta(u u^{-1}) = \delta(1_R)$ $\quad \delta(u) \leq \delta(1_R)$

(2) implies (3)

pick $c = 1_R$ and just write (2) down.

(3) implies (1)

We use $a = bq + r$, either $r = 0_R$ or $\delta(r) < \delta(b)$

with $a = c$ $b = uc$:

$$c = ucq + r, \quad \text{either } r = 0_R \text{ or } \delta(r) < \delta(uc)$$

It suffices to prove that $r = 0_R$, because this implies $c = ucq$ implies $1_R = uq$, so u is a unit.

Assume $r \neq 0_R$ to find a contradiction

$c = ucq + r$ $\quad \underline{\delta(r) < \delta(uc) = \delta(c)}$ by assumption (3)

$r = c - ucq = c(1_R - uq)$ implies by (i) in the definition of Euclidean domain

$$\underline{\delta(r) \geq \delta(c)}$$

The inequalities contradict each other proving that the assumption $r \neq 0_R$ was wrong.

Remark $\delta(c) = \delta(cu)$ for some $c \in R$ implies that u is a unit in R. That implies $\delta(c) = \delta(cu)$ for any non-zero $c \in R$

From this point on, the way to the Fundamental Theorem of Arithmetic – Th 10.7 – in an arbitrary Euclidean domain follows the lines of Chapters 1 & 4.

One defines gcd (non-unique - up to a multiplication by a unit),

finds an alternative description of gcd (by the measurement δ).

Th 10.5 $a \mid bc$, $(a, b) = 1_R$ (1_R is among them) imply $a \mid c$.
relatively prime

Cor 10.6 p is irreducible $p \in R$, $p \mid bc$ implies $p \mid b$ or $p \mid c$ (or both)

The presence of δ also helps with the existence clause in Th 10.7 (the argument is similar to those for $\mathbb{Z}$ and $F[x]$).

New example - Gaussian integers - $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}] = \{a+bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$

$$\delta(a+ib) = a^2 + b^2$$

Not in general, though:

$$\mathbb{Z}[\sqrt{-15}] = \{a + b\sqrt{-15} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

A similar $\delta(a+b\sqrt{-15}) = a^2 + 15b^2$ will not make an Euclidean domain out of $\mathbb{Z}[\sqrt{-15}]$.