Chapter 10.1 part 1

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 divisors that we possibly want to consider rings without zero divisors.

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

R - 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 $1_R \in R$ ($uv = 1_R$, $u, v \in R$)

$v = u^{-1}$

- $\{-1, 1\}$ 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

$a \neq 0_R$ $b \neq 0_R$ $a = bu$, 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

$p \neq 0_R$

p - not a unit

nothing besides units and associates of p.

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 **Euclidean domain** 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.