

8. FACTORIZATION

Definition 8.1. Let R be a commutative ring with unity.

- 1) a divides b if $b = ac$ for some $c \in R$, denote by $a|b$.
- 2) u is a *unit* if u divides 1.
- 3) a and b are *associates* in R if $a = bu$ for some unit u .
- 4) A nonzero element a in an integral domain D is an *irreducible* of D if $a = bc$ in D implies either b or c is a unit.
- 5) A nonzero nonunit element p of an integral domain D is a *prime* if, for all $a, b \in D$, $p|ab$ implies either $p|a$ or $p|b$.
- 6) An integral domain D is a *unique factorization domain (UFD)* if
 - Every non-zero non-unit element of D can be factored into a product of a finite number of irreducibles.
 - The above factorization is unique up to the order of irreducible factors and associates.
- 7) An integral domain D is a *principal ideal domain (PID)* if every ideal in D is a principal ideal.

We need several lemmas:

- Lemma 8.1.**
- 1) Let R be a commutative ring and let $N_1 \subset N_2 \subset \dots$ be an ascending chain of ideals N_i in R . Then $N = \cup_i N_i$ is an ideal of R .
 - 2) **Ascending Chain Condition (ACC) for a PID** Let D be a PID. If $N_1 \subset N_2 \subset \dots$ is an ascending chain of ideals N_i , then there exists a positive integer r such that $N_r = N_s$ for all $s \geq r$. Equivalently, every strictly ascending chain of ideals (all inclusions proper) in a PID is of finite length. We express this by saying that the **ascending chain condition (ACC)** holds for ideals in a PID.

Theorem 8.1.

- 1) Let D be a PID. Every element that is neither 0 nor a unit in D is a product of irreducibles
- 2) An ideal $\langle p \rangle$ in a PID is maximal if and only if p is an irreducible.
- 3) In a PID, if an irreducible p divides ab , then either $p|a$ or $p|b$.
- 4) If p is an irreducible in a PID and p divides the product $a_1 a_2 \cdots a_n$ for $a_i \in D$, then $p|a_i$ for at least one i .
- 5) Every PID is a UFD.
- 6) **Fundamental Theorem of Arithmetic.** The integral domain \mathbb{Z} is a UFD.

Now we show that a polynomial ring over a UFD is still a UFD.

Definition 8.2. Let D be a UFD.

- 1) A *greatest common divisor (gcd)* of all the a_i 's in D is an element $d \in D$, unique up to a unit factor, such that $d|a_i$ for all i and any other with this property divides d .
- 2) A nonconstant polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n \in D[x]$ is *primitive* if the gcd of the a_i 's is 1.

It is clear that any non-constant polynomial $f(x) \in D[x]$ can be written as $f(x) = cg(x)$ where $g(x)$ is primitive and $c \in D$. The decomposition is unique up to a unit factor and c is called the *content* of $f(x)$. A less trivial observation is

- Lemma 8.2.**
- 1) **Gauss' Lemma.** *If D is a UFD, then a product of two primitive polynomials in $D[x]$ is again primitive.*
 - 2) *If D is a UFD, then a finite product of primitive polynomials in $D[x]$ is again primitive.*
 - 3) *Let D be a UFD and let F be a field of quotients of D . Let $f(x) \in D[x]$ of positive degree. If $f(x)$ is an irreducible in $D[x]$, then $f(x)$ is also an irreducible in $F[x]$. Also, if $f(x)$ is primitive in $D[x]$ and irreducible in $F[x]$, then $f(x)$ is irreducible in $D[x]$.*
 - 4) *Let D be a UFD and F its quotient field. Then $f(x) \in D[x]$ admits a factorization if and only if it admits a factorization in $F[x]$.*

Summarizing the above results, we finally can prove

Theorem 8.2. *If D is a UFD, then $D[x]$ is a UFD. Consequently, if $F[x_1, \dots, x_n]$ is a UFD for a field F .*