

PRINCIPAL IDEAL DOMAINS

FROM LAST TIME:

- A **principal ideal domain (PID)** is an integral domain in which every ideal is principal.
- Every Euclidean domain is a PID, but the converse is false.

DEFINITION: Let R be a commutative ring, and $a, b \in R$.

- If there is some $c \in R$ such that $a = bc$, then we say b **divides** a , or b is a **divisor** of a , or a is a **multiple** of b , and write $b | a$.
- We say a and b are **associates** if $a = ub$ for some unit u . Note that this relation is symmetric, since $b = u^{-1}a$ in this case.
- A **greatest common divisor** or **gcd** of a and b is an element $d \in R$ such that
 - d is a common divisor of a and b , meaning $d | a$ and $d | b$, and
 - any common divisor of a and b also divides d , meaning if $c | a$ and $c | b$, then $c | d$.
- A **least common multiple** or **lcm** of a and b is a common multiple of a and b that divides any common multiple of a and b .

(1) Divisibility and principal ideals: Let R be a commutative ring, and $a, b \in R$.

- (a) Show that $(a) \subseteq (b)$ if and only if $b | a$.
- (b) Show that $(a) = (b)$ if and only if $a | b$ and $b | a$.
- (c) If R is an integral domain, show that a and b are associates if and only if $(a) = (b)$.

(2) GCDs: Let R be an integral domain, and $a, b \in R$.

- (a) If R is an integral domain, and d and e are two GCDs of a and b , show that d and e are associates.
- (b) If $(a, b) = (d)$, show that d is a GCD of a and b .
- (c) Use the previous to fill in the blanks:
 If R is a _____ then GCDs are unique _____.
 If R is a _____ then GCDs exist.

(3) Euclidean algorithm: Let R be an integral domain.

- (a) What is $\gcd(x, 0)$ for $x \neq 0$?
- (b) If $a = bq + r$, show that $\gcd(a, b) = \gcd(b, r)$.
- (c) If R is a Euclidean domain, use the previous two steps to give an algorithm to compute a GCD of two elements.
- (d) Use this to find a single generator for the ideal $(x^6 - 1, x^5 - x^4 - 1)$ in $\mathbb{Q}[x]$.
- (e) Use this to find a single generator for the ideal $(13, 12 - 5i)$ in $\mathbb{Z}[i]$.

DEFINITION: Let R be a domain and $r \in R$.

- (i) We say that r is **irreducible** if $r \neq 0$, r is not a unit, and $r = ab$ implies either a or b is a unit.
- (ii) We say that r is **prime** if $r \neq 0$, r is not a unit, and $r | ab$ implies $r | a$ or $r | b$.

REMARK: An element r of a domain R is prime if and only if (r) is a prime ideal.

THEOREM: Let R be an integral domain and $r \in R$.

- (i) If r is prime, then r is irreducible.
- (ii) If R is a PID, and r is irreducible, then r is prime. Moreover, in this case (r) is a maximal ideal.

(4) Examples of irreducible elements:

- (a) Show¹ that 5 is not irreducible in $\mathbb{Z}[i]$.
- (b) Show² that $f = x^2 + [1]$ is irreducible in $\mathbb{Z}/3[x]$.
- (c) Use the Theorem to deduce that $\frac{\mathbb{Z}[i]}{(5)}$ is *not* an integral domain, and $\frac{\mathbb{Z}/3[x]}{(x^2 + [1])}$ is a field.

(5) Proof of Theorem:

- (a) Prove part (i) of the Theorem.
- (b) Let R be a PID and $r \in R$ irreducible. Explain why³ there exists some element $s \in R$ such that (s) is a maximal ideal and $(r) \subseteq (s)$.
- (c) Show that $(r) = (s)$, and conclude the proof of part (ii).

(6) More irreducible elements:

- (a) Let F be a field. Show that any polynomial $f \in F[x]$ of degree at least two that has a root is reducible.
- (b) Give an example of a reducible polynomial over a field with no root.
- (c) Show that 11 is irreducible⁴ in $\mathbb{Z}[i]$.

¹Hint: $5 = 2^2 + 1^2$.

²Hint: If $f = gh$ with g, h nonunits, argue that without loss of generality we can take $g = x - [n]$ for some n , and show that this is impossible.

³Hint: We showed that every ring contains a maximal ideal. It follows from this fact and the Lattice Isomorphism theorem that every proper ideal is contained in a maximal ideal.

⁴Hint: You can use the fact that the norm function $N(a + bi) = a^2 + b^2$ is multiplicative.