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 $b \mid a$.
- 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 $d \mid a$ and $d \mid b$, and
  - any common divisor of a and b also divides d, meaning if $c \mid a$ and $c \mid b$, then $c \mid d$.
- 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 $b \mid a$.

If $(a) \subseteq (b)$, then $a \in (b)$, so $a = bx$ for some x, and hence $b \mid a$. Conversely, if $b \mid a$, then $a = bx$ for some x, so $a \in (b)$, and by definition of generates, since (b) is an ideal, we must have $(a) \subseteq (b)$.

(b) Show that $(a) = (b)$ if and only if $a \mid b$ and $b \mid a$.

This follows from the previous part since $(a) = (b)$ if and only if $(a) \subseteq (b)$ and $(b) \subseteq (a)$.

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

If a, b are associates, write $a = ub$, so $b \mid a$, and $b = u^{-1}a$, so $a \mid b$, and thus $(a) = (b)$ by the previous part. Conversely, if $(a) = (b)$, then by the previous part $a = bx$ and $b = ay$ for some $x, y \in R$, so $a = xya$. Since R is a domain, $xy = 1$, so x is a unit, and from $a = bx$ we conclude a, b are associates.

(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.

Since e is a common divisor, and d is GCD, we have $e \mid d$. Switching roles, $d \mid e$ as well, so d and e are associates by the previous part.

(b) If $(a, b) = (d)$, show that d is a GCD of a and b.

First, $a \in (a,b) = (d)$ implies $d \mid a$, and likewise for b, so d is a common divisor. Now, if e is any common divisor of a and b, then $a \in (e)$ and $b \in (e)$ implies $(a,b) \subseteq (e)$ by definition of generates, so $(d) \subseteq (e)$ and $e \mid d$, as required.

(c) Use the previous to fill in the blanks:
If R is a ________ then GCDs are unique __________________.
If R is a _______ then GCDs exist.

If R is a DOMAIN then GCDs are unique UP TO ASSOCIATES.
If R is a PID 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 $r \mid ab$ implies $r \mid a$ or $r \mid b$.

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) Show[1] that 5 is not irreducible in $\mathbb{Z}[i]$.

We have $5 = (2+i)(2-i)$. We claim that neither $2+i$ nor $2-i$ is a unit. To see it, consider $N : \mathbb{Z}[i] \smallsetminus \{0\} \to \mathbb{Z}_{\geq 0}$. This is multiplicative, so if $\alpha\beta = 1$ in $\mathbb{Z}[i]$, then $N(\alpha)N(\beta) = 1$ in $\mathbb{Z}_{\geq 0}$ so $N(\alpha) = 1$, but $N(2 \pm i) = 5$.

(b) Show[2] that $f = x^2 + [1]$ is irreducible in $\mathbb{Z}/3[x]$.

[1] Hint: $5 = 2^2 + 1^2$.

[2] Hint: 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.

If $f = gh$, then $2 = \deg(f) = \deg(g) + \deg(h)$. A polynomial of degree 0 is a nonzero constant, which is a unit in $\mathbb{Z}/3$ since it is a field. Thus, if f is reducible, we have $\deg(g) = 1$, and dividing through by the leading coefficient and moving that over to h, we can take $g = x - [n]$. But then $[n]$ would be a root of f in $\mathbb{Z}/3$. Plugging in $[n] = [0], [1], [2]$ we see that there are no roots, so this is impossible. We conclude that f is irreducible.

(c) Use the Theorem to deduce that $\dfrac{\mathbb{Z}[i]}{(5)}$ is *not* an integral domain, and $\dfrac{\mathbb{Z}/3[x]}{(x^2+[1])}$ *is* a field.

Since prime elements are irreducible and 5 is reducible, it is not a prime element in $\mathbb{Z}[i]$. Thus (5) is not a prime ideal, so $\dfrac{\mathbb{Z}[i]}{(5)}$ is not an integral domain.

Now, $\mathbb{Z}/3[x]$ is a PID, and $x^2 + [1]$ is an irreducible element, so by the theorem, $(x^2 + [1])$ is a maximal ideal. Thus $\dfrac{\mathbb{Z}/3[x]}{(x^2+[1])}$ is a field.

(5) Proof of Theorem:

(a) Prove part (i) of the Theorem.

Suppose that r is prime and $r = ab$. Then $r \mid ab$ implies, without loss of generality, that $r \mid a$, so there is some x such that $a = abx$. Then $bx = 1$ so b is a unit. This show that r is irreducible.

(b) Let R be a PID and $r \in R$ irreducible. Explain why[3] there exists some element $s \in R$ such that (s) is a maximal ideal and $(r) \subseteq (s)$.

Following the hint, we have that (r) is contained in some maximal ideal I. Since R is a PID, $I = (s)$ for some s.

(c) Show that $(r) = (s)$, and conclude the proof of part (ii).

Note that s must be nonzero since $0 \neq r \in I$, and not a unit since $I \neq R$. Then $s \mid r$, so $r = sx$ for some x. But r is irreducible and s is not a unit, so x is a unit. Thus from the above, $(r) = (s)$, and hence (r) is maximal.

(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 irreducible[4] in $\mathbb{Z}[i]$.

[3]Hint: 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.

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