Algebraic Theory I

Thomas Fleming

November 3, 2021

Contents

Lecture 29: Ring Theory (4)

Mon 01 Nov 2021 11:31

We will again denote all rings R to be commutative.

Recall. An ideal I is principal if $I = (x)$, that is I is generated by one element, so $I = Rx$.

Notation. We say $x \mid y$ if $y = rx$ for some $r \in R$, hence $y \in (x)$.

Proposition 0.1. If $x \mid y$ and $y \mid x$, then $(x) = (y)$.

Proof. $x \mid y$ implies $y \in (x)$, so $(y) \subseteq (x)$.
Similarly, $y \mid x$ implies $x \in (y)$, so $(x) \subseteq (y)$.
Conversely, if $(x) = (y)$, then $x = ry$ and $y = sx$ for some $r, s \in R$, hence $x \mid y$ and $y \mid x$. $\square$

Proposition 0.2. If R is an integral domain with $x \neq 0$, then $x \mid y$ and $y \mid x$ if and only if $y = mx$ for a unit $m \in R$.

Proof. If $(x) = (y)$, then $y = rx$ and $x = sy$ for some $r, s \in R$ hence $x = sy = srx$, so $sr = 1$, hence s and r are units. The other direction is immediately clear, if $x = my$, then $x \in (y)$ so $m^{-1}x = y \in (x)$, hence $(x) = (y)$. $\square$

Remark. If $x = my$ for a unit m, then we say x and y are associated if x and y are equal up to multiplication by a unit.

Definition 0.1 (Principal Ideal Domain)**.** A commutative integral domain R in which every ideal is principal is called a **principal ideal domain** (or PID).

Definition 0.2 (Euclidean Domain)**.** Suppose R is an integral domain and there is a size function (sometimes called a norm) $f : \mathbb{R} \setminus \{0\} \to \mathbb{N}_0$ such that for all $a, b \in R$ with $b \neq 0$, there is $q, r \in R$ such that $a = qb + r$ and either $r = 0$ or $f(r) < f(b)$, then R is a **euclidean domain** or ED.

Example. $\mathbb{Z}$ is a PID. $\mathbb{Z}$ is also a euclidean domain under norm $|x|$. $\diamond$

Proposition 0.3. A euclidean domain is a principal ideal domain.

Proof. Let I be a proper nontrivial ideal and let $x \in I$ be a nonzero element with $f(x)$ being minimal (where f is the norm from the definition). We know such an x to exist by the well ordering of $\mathbb{N}_0$. Now, let $y \in I$ and we find by the division algorithm that $y = qx + r$ for some $q, r \in R$ with $f(r) < f(x)$ and $r = 0$. Hence, we find $r = y - qx \in I$ as $x \in I$, $y \in I$. Suppose $f(r) < f(x)$, then $\lightning$ as x is the minimal element of I, hence, we find $r = 0$, so $y = qx$. Hence, we find $y \in (x)$, so $I = (x)$. $\square$

Definition 0.3 (Primality/Irreducibility)**.** Let R be a commutative ring

- A non-zero, non-unit $p \in R$ so that for all $x, y \in R$, we have $p \mid xy$ implies $p \mid x$ or $p \mid y$ is called a **prime element**.
- A non-zero, non-unit such that $x = yz$ with $y, z \in R$ implies either y or z is a unit is called an **irreducible** or an **atom**.

Proposition 0.4. $p \in R$ is prime implies (p) is prime.

Proof. Suppose $xy \in (p)$, so $p \mid xy$. Hence, $p \mid x$ or $p \mid y$ as p is prime. Hence, $x \in (p)$ or $y \in (p)$. As p is not a unit, we see $(p) \neq R$, so (p) is prime. $\square$

Proposition 0.5. If $p \in R$ is irreducible, then (p) is maximal by inclusion among all proper principal ideals of R.

Proof. Suppose $(p) \subset (x) \subset R$, that is x is not a unit. Then, $p \in (p) \subset (x)$, so $p = rx$ for some $r \in R$, but p is irreducible, so either r or x is a unit, but we know x to be a non-unit, so r must be a unit. So, $(p) = (rx) = (x)$, $\lightning$, as the unit will not change the ideal generated and (p) must be properly contained in (x) . $\square$

Corollary 1. If R is a PID, then $p \in R$ being irreducible implies (p) is maximal.

Proposition 0.6. If R is an integral domain with $p \neq 0$ and (p) being maximal among all proper principal ideals, then p is irreducible.

Proof. Suppose $p = xy$, hence $p \in (x)$ and $p \in (y)$. Hence, $(p) \subseteq (y)$ and as (p) is maximal, we have $(y) = (p)$ or $(y) = R$. If $(y) = (p)$, then $p = uy$ for some unit y. But, $p = xy = uy$, hence $x = u$ as we're in an integral domain (with $x, y \neq 0$), so x is a unit. If $(y) = R$, then y is a unit, hence p is irreducible by an earlier lemma. $\square$

Lecture 30: Ring Theory (5)

Wed 03 Nov 2021 11:32

Again, we suppose R to be commutative unless otherwise stated.

Proposition 0.7. If R is an integral domain with $p \in R$ being prime, then p is irreducible.

Proof. We know p is nonzero and a non-unit. Then, suppose $p = xy$ $x, y \in R$. Since p prime, we see $p \mid xy$ implies $p \mid x$ or $p \mid y$. WLOG, suppose $p \mid x$, then $x \in (p)$, so $x = rp$ for an $r \in R$. Then, we see

$$p = xy = (rp)\, y = (ry)\, p.$$

Canceling p yields $1 = ry$, so y is a unit. Hence, p is irreducible. $\square$

Remark. Here are a few basic facts about principal ideals, prime ideals, etc. we have shown, compiled together:

- $x \mid y \Leftrightarrow y \in (x) = Rx$.
- $x \mid y$ and $y \mid x \Leftrightarrow (x) = (y)$.
- If R is an integral domain with $x \neq 0$ then $(x) = (y) \Leftrightarrow ux = y$ for a unit u.
- $(x) = R \Leftrightarrow x$ is a unit.
- $p \in R$ is prime implies (p) is a prime ideal.
- (p) is a prime ideal and $p \neq 0$ implies $p \in R$ is prime.
- $p \in R$ irreducible implies (p) is maximal among all proper principal ideals.
- If R is an integral domain and $p \neq 0$, then $(p) \subset R$ is maximal among principal ideals $\Leftrightarrow p \in R$ is irreducible.
- If R is an integral domain with $p \in R$ being prime then p is also irreducible.