Algebraic Theory I

Thomas Fleming

November 1, 2021

Contents

Lecture 28: Ring Theory (3)

Fri 29 Oct 2021 11:31

Recall R will be a commutative ring unless otherwise noted.

Definition 0.1 (Prime Ideal)**.** Recall an ideal $P \subseteq R$ is a **prime ideal** when $xy \in P$ implies one of $x \in P$ or $y \in P$. This is equivalent to the statement that R/P is an integral domain.

Definition 0.2 (Maximal Ideals)**.** A proper ideal $M \subseteq R$ is maximal if it is not strictly contained in any other proper ideal. That is, the only ideals containing M are M and R. Equivalently, an ideal I is maximal if and only if R/I is a field.

We prove these two definitions to be equivalent.

Proof. First, assume I maximal. Then, note that an ideal in R/I has the form J/I with $I \subseteq J \subseteq R$ and J being an ideal in R. Hence, as I is maximal, we find $J = I$ or $J = R$. Hence, R/I is a field by prior characterization.
Now assume R/I is a field for some ideal I. Then, the only ideals of R/I are $\{0\}$ and R/I. Suppose I nonmaximal, then we find a $I \subset J \subset R$ corresponding to a proper nontrivial ideal $J/I \subseteq R/I$, $\lightning$ as R/I is a field. $\square$

Proposition 0.1. In a commutative ring R any maximal ideal is prime.

Proof. Since $M \subset R$ and R/M is a field (hence integral domain), we find M to be a prime ideal by the quotient characterization. $\square$

Example. If $R = \mathbb{Z}$, then (0) is a prime ideal, but it is obviously not maximal. $\diamond$

In order to prove some theorems concerning maximal ideals, we need to state some results from basic set theory.

Definition 0.3. If $(X, \preceq)$ is a poset (partially ordered set), with a totally ordered subset $Y \subseteq X$, then an **upper bound** of Y is an element $x \in X$ so that $y \leq x$ for all $y \in Y$. A **maximal element** of X is a $x \in X$ so that for all $y \in X$, $x \leq y$ implies $x = y$.

Law 1 (Zorn's Lemma)**.** If $(X, \preceq)$ is a nonempty poset, with every totally ordered subset having an upper bound, then we find a maximal element $x \in X$.

Of course, this is equivalent to axiom of choice, so we must take it as an axiom. Using Zorn's lemma, we find that every ideal is contained in a maximal ideal (as with subgroups).

Theorem 0.1. If R is a commutative ring with $I \subset R$ being a proper ideal. Then there is a maximal ideal $M \subset R$ with $I \subseteq M$.

Proof. Let $(X, \subseteq)$ be the set of all proper ideals of R which contain I partially ordered by inclusion. As I is proper, we see $I \subseteq I$ hence $I \in X$, so $X \neq \varnothing$. Any maximal element $m \in X$ will be a maximal ideal of R containing I. Hence, we need only show the existence of a maximal element.
Let $(I_\alpha)_{\alpha \in \Omega}$ by a nonempty totally ordered subset of X. Hence, each I_α is a proper ideal containing I with either $I \subseteq I_\alpha \subseteq I_\beta$ or $I \subseteq I_\beta \subseteq I_\alpha$ for all $\alpha, \beta \in \Omega$. Let $J = \bigcup_{\alpha \in \Omega} I_\alpha$, clearly, $I_\alpha \subseteq J$ for all $\alpha \in \Omega$, so we need only show $J \in X$. Clearly, $I \subseteq I_\alpha \subseteq J$, so J is nonempty and contains I. Now, let $x, y \in J$ with $x \in I_\alpha$, $y \in I_\beta$. By total ordering WLOG, let $I_\alpha \subseteq I_\beta$. Hence, $x, y \in I_\beta$. Hence, $x - y \in I_\beta \subseteq J$ as this is an ideal and $rx \in I_\beta \subseteq J$ for all $r \in R$, hence J is an ideal. Finally, suppose $J = R$, then $1 \in J$, so $1 \in I_\alpha$ for some $\alpha \in \Omega$ ↯, as I_α is assumed proper. Hence, $J \in X$ is an upper bound of $(I_\alpha)_{\alpha \in \Omega}$, so there is a maximal element $M \in X$ which is clearly a maximal ideal. ☐

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 0.2. 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 $y \mid x$. ☐

Proposition 0.3. 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 $(x) = (y)$. □

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

Definition 0.5 (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 $|x|$. ◇

Proposition 0.4. 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 $I = (x)$. □

Definition 0.6 (Factorization)**.** 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 0.5. $p \in R$ 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. □

Proposition 0.6. 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 0.7. 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. $\square$