Abstract Algebra
Lecture 13
Wednesday, 10/20/2010

1 Ideals, continued

Recall: Ideals generated by subsets $A \subseteq R$. If R has an identity,

$$(A) = \{r_1 a_1 s_1 + \cdots + r_n a_n s_n | r_i, s_i \in R, a_i \in A\}.$$

Note that this is only for rings with identity. It is close to correct for other rings, but not quite. We don't really care for rings without identity, though, because they are boring.

Ex: Let $R = \mathbb{Z}[x]$, $A = \{2, x\}$. Note that $(x) = \{\text{polynomials with 0 constant term}\}$. Therefore,

$$(2, x) = \{\text{polynomials with even constant term}\}.$$

Contrast this with $(2) = \{\text{polynomials with even coefficients}\}$.

Claim: $(2, x)$ cannot be generated by a single element.
Suppose that $(f) = (2, x) = \{rf \mid r \in R\}$. Then $2 = rf$ for some r, so the degree of f is 0. But $x = rf$ for some r as well, so $f = \pm 1$. But $(1) = (-1) = R$, a contradiction.
Note that this means that $(2, x)$ is therefore **not** a principal ideal.

Theorem: Let I be an ideal of a ring with identity R. Then

- $I = R$ if and only if I contains a unit
- If R is commutative, then R is a field if and only if the only ideals of R are 0 and R.

Proof:

- If $I = R$, then $1 \in I$. Say $u \in I$ is a unit. Let $r \in R$. Then $ru^{-1} \cdot u = r$, so $r \in I$ since ideals absorb multiplication.
- If R is a field and has an ideal that contains anything other than 0, that element is a unit, so the ideal is all of R. Suppose the only ideals of R are 0 and R. Let $r \in R$, $r \neq 0$. Then $(r) = R, 1 \in (r)$. But $(r) = \{rs \mid s \in R\}$, so we can write $1 = rs$ for some s, so r is a unit, so R is a field.

■

Defn: Let R be a ring. A **maximal ideal** of R is a proper ideal I such that $I \subset J \subseteq R$ implies $J = R$.

Ex: $2\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$. If we add any element to it, that element must be odd, and then we can generate all of the odd numbers as well as all of the even numbers, which seems an awful lot like all of $\mathbb{Z}$.
$3\mathbb{Z}$ is also a maximal ideeal of $\mathbb{Z}$.
In fact, $n\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$ if and only if n is prime. If n is prime and we throw in some element that is not a multiple of n, then $(n, m) = 1$, so we can generate everything. If n is composite, then we can throw in a factor of n and not generate all of $\mathbb{R}$. (x) is a maximal ideal of $\mathbb{R}[x]$.

Theorem: Let M be an ideal of a commutative ring R with identity. Then

$$M \text{ is maximal} \iff R/M \text{ is a field.}$$

Proof: (This can be proved by the 4th isomorphism theorem rather intuitively.)
Assume M is maximal. Pick $r + M \in R/M$, $r + M \neq 0$ (which means $r \notin M$). Consider the ideal generated by $(M \cup \{r\}) = I$. Then $I \supset M$ since $r \notin M$. Since M is maximal, $I = R$. This means $1 \in I = \{mr_1 + rr_1 \mid r_1, r_2 \in R, m \in M\}$, so $1 = mr_1 + rr_2$, or $1 - mr_1 = rr_2$. Specifically, $(r + M)(r_2 + M) = (1 - mr_1) + M = 1 + M$, so $r + M$ is a unit in R/M.
Assume R/M is a field. We want to show that $x \notin M$ implies that $(M \cup \{x\}) = R$. Let $x \notin M$. Then $x + M \neq 0$, so $x + M$ is a unit in R/M. So $(x + M)(y + M) = 1 + M$ for some $y \in R$. Thus, $xy = 1 + m$ for some $m \in M$, so $xy - m = 1$, but $xy - m$ lives in $(M \cup \{x\})$, so $1 \in (M \cup \{x\}) = R$. ∎

Defn: An ideal is a commutative ring is **prime** if $ab \in I$ implies $a \in I$ or $b \in I$.

Theorem: Let P be an ideal of a commutative ring with identity. Then

$$P \text{ is prime} \iff R/P \text{ is an integral domain.}$$

Proof: Assume that P is prime. Assume $(a + P)(b + P) = 0$ in R/P. Then $(a + P)(b + P) = P$, so $ab + P = P$, so $ab \in P$. Then either $a \in P$ or $b \in P$, so either $(a + P) = 0$ or $(b + P) = 0$.
Assume that R/P has no zero divisors. Let $ab \in P$. Then $(ab + P) = 0$ in R/P. This gives us $(a + P)(b + P) = 0$. But we have no zero divisors, so either $(a + P) = P$ or $(b + P) = P$, so either $a \in P$ or $b \in P$, so P is prime. ∎

Corollary: In commutative rings with identity, maximal ideals are prime.

Proof: M is maximal, so R/M is a field, so it is also an integral domain, so M is prime. ∎

Note: The converse is not true.