MATH 171 FALL 2008: LECTURE 14

DAGAN KARP

1. Properties of Ideals continued

Definition 1. *A proper ideal* M *of a ring* R *is* maximal *if whenever* I *is an ideal of* R *and* $M \subset I \subset R$*, then* $M = I$ *or* $I = R$.

Definition 2. *A proper ideal* P *of a commutative ring* R *is* prime *if* $ab \in P$ *implies* $a \in P$ *or* $b \in P$ *for any* $a, b \in R$.

1.1. **Exercise.**

(1) Show that the ideal $n\mathbb{Z}$ of $\mathbb{Z}$ is prime if and only if n is prime.
(2) Inspect the lattice of subgroups of $\mathbb{Z}/36\mathbb{Z}$ and show that (2) and (3) are maximal ideals.
(3) Show that the ideal $(x^2 + 1)$ is not prime in $\mathbb{Z}_2[x]$.

Date: October 22, 2008.

Theorem 3. *Let R be a commutative ring with unity and let $A \subset R$ be an ideal. Then R/A is an integral domain if and only if A is prime.*

Proof. Suppose that R/A is an integral domain. Let $a, b \in R$ and suppose that $a \cdot b \in A$. We must show that $a \in A$ or $b \in A$.

We compute

$$(a + A)(b + A) = (ab) + A = A = 0 + A,$$

which is the additive identity in R/A. But R/A is an integral domain. Therefore $a + A = A$ or $b + A = A$. Therefore $a \in A$ or $b \in A$.

Conversely, suppose that A is prime, and let $a + A, b + A \in R/A$ be such that $(a + A)(b + A) = ab + A = A$. Then $ab \in A$. But A is prime. Thus $a \in A$ or $b \in A$. Thus $a + A = 0 \in R/A$ or $b + A = 0 \in R/A$. Hence R/A is an integral domain. □

Theorem 4. *Let R be a commutative ring with unity and let A be an ideal of R. Then R/A is a field if and only if A is maximal.*

Proof. Suppose that R/A is a field. Let B be an ideal of R that properly contains A,

$$A \subsetneqq B \subseteq R.$$

We must show that $B = R$.

First, there exists $b \in B$ such that $b \notin A$. Then $b + A$ is a non-zero element of R/A. But R/A is a field, hence $b + A$ must have a multiplicative inverse, i.e. there exists $c \in R$ such that

$$(b + A)(c + A) = bc + A = 1 + A,$$

where the latter is the multiplicative identity of R/A. Therefore $1 - bc \in A \subset B$. But $bc \in B$ since B is an ideal. Thus

$$(1 - bc) + bc = 1 \in B.$$

Therefore $B = R$.

Conversely, suppose that A is maximal. We wish to show that R/A is a field. It is easily seen to be a commutative ring with unity. Our goal is to show that every non zero element has a multiplicative inverse. Every non zero element of R/A is of the form $b + A$ for some $b \in R - A$. Choose and fix such an element b.

Consider the following subset $B \subset R$ given by

$$B = \{br + a : r \in R, a \in A\}.$$

Claim. B is an ideal of R properly containing A. Indeed,

$$br + a - (br' + a') = b(r - r') + (a - a') \in B,$$

so B is a subgroup of $(R, +)$. Further, multiplication is associative in B as it is in R. For any $s \in R$,

$$s \cdot (br + a) = sbr + sa = b(sr) + (sa)$$

because R is commutative. Since A is an ideal, $sa \in A$. Hence

$$b(sr) + (sa) \in B,$$

and B is an ideal of R. Also, for any $a \in A$,

$$a = b \cdot 0 + a \in B,$$

and

$$b = b \cdot 1 + 0 \in B - A.$$

Therefore B is indeed an ideal such that

$$A \subsetneqq B \subseteq R.$$

Corollary 5. *In a commutative ring* R *with unity, every maximal ideal is prime.*

Remark 6. The converse is not true, as we see in the following example.

Exercise. Show that the principal ideal (x) in $\mathbb{Z}[x]$ is prime but not maximal. *Hint: Show that* $(x) = \{f(x) \in \mathbb{Z}[x] : f(0) = 0\}$.