M7210 Lecture 29 Monday October 29, 2012

Ideals in Commutative Rings

We assume all rings are commutative and have multiplicative identity (different from 0).

Ideals

Suppose A is a ring.

Fact. Then for all $a \in A$, $a0_A = 0_A$.

Definition. A subgroup of the additive group of A with the property that

$$\text{for all } a \in A, \text{ and all } y \in I,\ ay \in I \tag{1}$$

is called an *ideal*.[1]

Fact. The kernel of any ring homomorphism is an ideal.

Fact. If $I \subseteq A$ is an ideal, the set of (additive) cosets of I has a multiplication defined unambiguously by $(a+I)(b+I) = ab + I$, and with this operation A/I is a ring and $q : A \to A/I; a \mapsto a + I$ is a ring homomorphism.

Exercise. Let $\{ I_b \mid b \in B \}$ be a collection of ideals indexed by a set B. For each $b \in B$, let $q_B : A \to A/I_b$ be the canonical surjection. These homomorphisms induce a ring homomorphism $Q : A \to \prod_{b\in B} A/I_b$. Show that the kernel of Q is the intersection $\bigcap_{b\in B} I_b$.

The largest ideal in A is A itself. The smallest ideal is $\{0\}$. Any intersection of ideals in A is an ideal. Thus, given any subset $S \subseteq A$, there is a smallest ideal containing S. This is called *the ideal generated by* S. The ideal generated by a single element $a \in A$ is often denoted (a) or aA, and the ideal generated by a finite set $\{a_1, \ldots, a_k\}$ may be denoted $(a_1, \ldots, a_k)$ or $a_1A + \cdots + a_kA$.

Fact. $(a) = \{ ax \mid x \in A \}$. *Proof.* The containment $\{ ax \mid x \in A \} \subseteq (a)$ follows from "closure under in-out multiplication". So, it is enough to show that $\{ ax \mid x \in A \}$ is an ideal. Since $0 = a0$, this set is non-empty, and since $ax - ay = a(x - y)$, it is closed under subtraction. So, it's a subgroup of A, and finally since $a'(ax) = a(a'x)$, it's an ideal./////

Exercise. Show that $(a_1, \ldots, a_k) = \{ a_1x_1 + \cdots + a_kx_k \mid x_1, \ldots, x_k \in A \}$.

Exercise. Suppose I and J are ideals of A. Then the ideal generated by $I \cup J$ is

$$I + J := \{ y + z \mid y \in I \,\&\, z \in J \}.$$

Exercise. $(a) = A$ if and only if a is a unit.

[1] If A is not assumed commutative, this is called a *left ideal.* In the non-commutative case, an ideal is required to be closed under both "out-in" and "in-out" multiplication, i.e., it must satisfy (1) and also for all $a \in A$, and all $y \in I$, we must have $ya \in I$.

Prime and Maximal Ideals

Definition. An ideal $I \subset A$ is said to be *maximal* if the ideal generated by I and any element not in I is all of A. If S is a subset of A, an ideal $I \subset A$ is said to be *maximal disjoint from* S if the ideal generated by I and any element not in I contains some element of S.

Definition. An ideal $I \subset A$ is said to be *prime* if its complement contains 1 and is closed under multiplication.

Fact. I is maximal if and only if A/I is a field. I is prime if and only if A/I is a domain.

Proposition. *Suppose $S \subseteq A$ contains 1, does not contain 0 and is closed under multiplication. Then,*
a) there is an ideal maximal disjoint from S, and
b) any ideal maximal disjoint from S is prime.

Proof. a) We can approach this two ways: either take it as an axiom, or derive it from Zorn's Lemma. Zorn's Lemma is interesting from the perspective of set theory, but we learn very little of algebraic interest by applying it. Nonetheless, it is important to know how the typical application runs. So, let show this. There is at least one ideal disjoint from S—namely $\{0\}$—and if $C = \{ I \subset I' \subset I'' \subset \cdots \}$ is any ascending chain of ideals each of which is disjoint from S, then $\cup C$ is an ideal disjoint from S—for if $x, y \in \cup C$, then both x and y belong to some ideal in the chain, and hence their difference is in the union of the chain, and also for any $a \in A$, and $x \in \cup C$, $ax \in \cup C$. Now, Zorn's Lemma says that if these conditions are satisfied, then there is an ideal disjoint from S such that no properly larger ideal is disjoint from S.

b) Suppose I is maximal disjoint from S. Let a and a' be any elements of $A \setminus I$. We show $aa' \notin I$. Select elements $y, y' \in I$ and $x, x' \in A$ such that $y + ax \in S$ and $y' + a'x' \in S$. Then $yy' + axy' + a'x'y + axa'x' \in S$. If $aa' \in I$, then $yy' + axy' + a'x'y + axa'x' \in I$. But $I \cap S = \emptyset$. So $aa' \notin I$. /////

Exercise. An element $a \in A$ is said to be *nilpotent* if there is $n \in \mathbb{N}$ such that $a^n = 0$.

a) Show that the difference of two nilpotent elements of A is nilpotent and that any multiple of a nilpotent element is nilpotent. Conclude that the set of all nilpotent elements of A is an ideal. (This is called the *nil radical of* A.)
b) Show that every prime ideal of A contains the nil radical of A. Show that if $a \in A$ is *not* nilpotent, then there is a prime ideal that does *not* contain a. Conclude that the nil radical of A is the intersection of all the prime ideals of A.
c) If $I \subset A$ is an ideal, let

$$\sqrt{I} := \{ a \in A \mid \exists n \in \mathbb{N} \;\; a^n \in I \}.$$

Show that $\sqrt{I}$ is the intersection of all the prime ideals of A that contain I.