M7210 Lecture 30 Wednesday October 31, 2012

Factorization in Commutative Rings

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

This lecture is about factorization—i.e., about the multiplicative structure of a ring. Ring addition plays no role in basic parts of the theory, so we introduce an abstraction that enables us to focus on just what we need:

Definition. A *monoid* is a set equipped with an associative operation and an identity element for this operation.

Thus, a monoid is like a group, but we do not assume that elements have inverses—though some might. If A is a (commutative) ring, then the elements of A with the operation of multiplication form a commutative monoid. If A is a *domain*, then $A^* := A \setminus \{0\}$ is also a monoid. If A is a field, then A^* is a group. Thus, if A is a domain, then A^* is a commutative submonoid of a commutative group.

Exercise (not to hand in). Let M be a commutative monoid. We say that M is cancellative if $ab = ab'$ implies $b = b'$ for all $a, b, b' \in M$. A commutative group is cancellative by virtue of the presence of inverses, and thus every submonoid of a commutative group is cancellative. Here is the task. Suppose that M is cancellative. Show that there is a commutative group that contains M and is generated by M, and that any two groups that contain M and are generated by M are isomorphic by an isomorphism that restricts to the identity on M. (Hint: Copy the construction of the field of fractions.)

Throughout the following, we let M be a cancellative commutative monoid. The elements of M that have inverses will be called *units*. Clearly, the units of M form a group.

Definition. Suppose a and b are elements of M.

i) If $a = ub$ for some unit u, we call a and b *associates*.
ii) We say a *divides* b—in symbols, $a|b$—if there is $c \in M$ such that $b = ac$.
iii) We say b is *irreducible* if b is not a unit and for any relation of the form $b = ac$, either a or c is a unit.
iv) We say b is *prime* if b is not a unit and whenever $b|ac$, either $b|a$ or $b|c$.

The same definitions may be made for the non-zero elements of an integral domain. Indeed, one could complain that introducing the language of monoids is just extra baggage. But I would counter that the extra baggage is all the structure in an integral domain that is unused in developing the theory of factorization. Monoids help us focus attention where it is needed.

Fact. Any prime element of M is irreducible. (Reminder: M is cancellative.) *Proof.* Suppose b is prime and $x, y \in M$. If $b = xy$, then $b|x$ or $b|y$. Without loss of generality, we may assume $b|x$. Then, $x = bz$ for some $z \in M$. Then $b = bzy$, so $1 = zy$, so y is a unit. /////

Unique Factorization

Definition. Let M be a cancellative commutative monoid. We say M has *unique factorization* if the following two conditions hold:

UF1: Every non-unit of M is a finite product of irreducible elements.

UF2: If a non-unit of M is factored into irreducibles in two ways, then by rearrangement and multiplication of the factors by units, the two factorizations may be made the same.

Proposition. *Suppose M satisfies UF1. Then M satisfies UF2 if and only if it satisfies:*

UF2′: Every irreducible element of M is prime.

Proof. UF2 $\Rightarrow$ UF2′: Suppose p is irreducible. If $p|ab$ ($ab \neq 0$) then $ab = px$ for some $x \in M$. Factoring a, b and x into irreducibles:

$$(a_1 \cdots a_k)(b_1 \cdots b_\ell) = p(x_1 \cdots x_m).$$

By $UF2$, p is an associate of one of the a_i or b_j, so either $p|a$ or $p|b$.

UF2′ $\Rightarrow$ UF2: Suppose we have two products of irreducibles $p_1 \cdots p_m = q_1 \cdots q_n$. We need to show that $m = n$ and after rearrangement p_i is an associate of q_i. By UF2′, p_1 is prime, so $p_1|q_i$ for some i. Rearranging, we may assume $i = 1$. Then $q_1 = x_1 p_1$ for some x_1. Since q_i is irreducible, x_1 is a unit. The result follows by induction. (But mind the details! What does the $m = 1$ case look like?)

Comment. This all translates directly to domains. If A is a domain, we call A a *unique factorization domain* (or UFD for short) if the monoid A^* satisfies UF1 and UF2. We call these ring-theoretic conditions UFD1 and UFD2.

Principal Ideal Domains

An ideal I of a ring A is said to be *principal* if it is generated by a single element.

Proposition. *Let A be an integral domain. A principal ideal $(p) \subseteq A$ is prime (as an ideal) if and only if p is prime (as an element).*

Proof. If p is a unit, then (p) is not prime as an ideal and p is not prime as an element. Confining attention to no-zero non-units p: (p) is prime $\Leftrightarrow$ for all $a, b \in A$, $ab \in (p)$ implies $a \in (p)$ or $b \in (p)$ $\Leftrightarrow$ for all $a, b \in A$, $p \mid ab$ implies $p \mid a$ or $p \mid b$.

An integral domain, such as $\mathbb{Z}$ or $\mathbb{F}[x]$ ($\mathbb{F}$ a field), in which every ideal is principal is called a *principal ideal domain*, or PID for short.

Proposition. *Every PID is a UFD.*

Proof. (PID $\Rightarrow$ UFD1.) Suppose A is a domain that fails to satisfy UF1. Then A contains a non-zero non-unit a that does not have a finite factorization into irreducibles. Then, we may write $a = b_1 a_1$ where b_1 and a_1 are non-zero non-units. Moreover, at least one of these must fail to have a finite factorization into irreducibles, and choosing notation appropriately, we may assume that a_1 fails. Then $a_1 = b_2 a_2$, where b_2 and a_2 are non-zero non-units and a_2 does not have a finite factorization into irreducibles. We can continue in this fashion indefinitely. Then the ideals

$$(a_1) \subset (a_2) \subset \cdots$$

form an ascending chain in which every containment is proper. The union of this chain is an ideal, but it cannot be principal because if it were, the generator would have to lie in some (a_i) and from this point on the containments would not be proper. Thus A is not a PID.

Proof. (PID $\Rightarrow$ UF2′.) Suppose A is a PID and $a \in A$ is irreducible. We show (a) is maximal, so (a) is prime, so a is prime. Let I be an ideal properly larger than (a). Since A is a PID, $I = (c)$ for some $c \in A$. Then, $a = bc$, so either b or c is a unit. But if b is a unit, $(a) = (c)$. Thus $I = A$.

Homework (due Monday, 11/6) Page 441-3: 12, 16, 18, 27, 28.