M7210 Lectures 31 Friday November 2, 2012

Factorization in Commutative Rings II

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

Greatest common divisors in UFDs

Let A be a UFD. In A, very non-zero non-unit is a finite product of irreducible elements in a way that is unique up to rearrangement of the factors and multiplication by units. Let us picture what this means. Choose a representative from each equivalence class of the associate relationship, and choose a total order on the set of all chosen representatives. (In general, this means using the Axiom of Choice twice.) Then, each element of A can be written uniquely as a unit times a finite product of chosen representatives, listed in ascending order. This is in exact analogy with what we commonly do with $\mathbb{Z}$—selecting the positive primes as the set of representatives and giving them the natural order, then writing each non-zero integer in the form $(\pm 1)(2^{n_2})(3^{n_3})(5^{n_5})\cdots$. The exponents are in $\mathbb{N}$, and all but finitely many are 0. In a similar way, in any UFD, we may represent each element as a "vector of exponents."

In $\mathbb{Z}$, we define $\gcd(a,b)$, the *greatest common divisor* of integers a and b, to be the largest integer (with respect to the linear order on $\mathbb{Z}$) that divides both a and b. As a consequence, $\gcd(a,b)$ is always positive. Every integer that divides both a and b also divides $\gcd(a,b)$, but it is also the case that every integer that divides both a and b also divides $-\gcd(a,b)$.

In any ring R, we have the divisibility relation—$a|b \;\Leftrightarrow\; \exists x\; b = ax$. It may or may not be the case that for any $a,b \in R$, there is some $g \in R$ such that g divides both a and b and every element that divides both a and b also divides g. If there is such an element, it is called a gcd of a and b. In general, it is not unique, since multiplying g by a unit other than 1_R produces another element of R with the same property.

In a UFD, we can find the gcd of two elements by considering their exponent vectors. The exponent vector of any gcd of a and b is the component wise minimum of the exponent vectors of a and b. Just as in $\mathbb{Z}$, we may find gcds in any UFD by examining factorizations. But in the general setting, gcds are defined only up to multiplication by units.

We can restore uniqueness of gcds by factoring out the units. This leads to an interesting construction called "the divisibility group" of a domain. Let A be a domain with group of units U. Let F be the fraction field of A and let F^* be the multiplicative group of non-zero elements of F. Then U is a subgroup of F^*, and we may form the quotient group F^*/U.

Exercise. Show that we may define a partial order $\leq$ on F^*/U by

$$\frac{a}{b} + U \leq \frac{c}{d} + U \;\Leftrightarrow\; \exists x \in A,\; xad = bc.$$

Show that $p \leq q \;\Rightarrow xp \leq xq$ for all $p,q,x \in F^*/U$. Show that if every pair of non-zero elements of A has a gcd, then any pair p,q of elements of F^*/U has a greatest lower bound—denoted $p \wedge q$—and for all $p,q \in F^*/U$ and $a \in A^*/U$, $ap \wedge aq = a(p \wedge q)$. (A partially-ordered abelian group equipped with a greatest-lower-bound operation $\wedge$ over which the group operation distributes is called and abelian ℓ-group. The "ℓ" stands for "lattice".)

Gauss's Lemma and factorization in the ring of polynomials over a UFD

Let A be a UFD. A polynomial $f \in A[x]$ is said to be **primitive** if the greatest common divisor of its coefficients is a unit.

Lemma. *(Gauss.) A product of primitive polynomials in $A[x]$ is primitive.*

Proof. It suffices to show that for any prime $p \in A$, if p does *not* divide all the coefficients of $f(x)$ and does *not* divide all the coefficients of $g(x)$, then it does *not* divide all the coefficients of $f(x)g(x)$. So, let $p \in A$ be any prime.
Argument 1. Suppose $f(x) = a_m x^m + \cdots + a_0$ and $g(x) = b_n x^n + \cdots b_0$. Suppose p does not divide all the coefficients of $f(x)$ nor all the coefficients of $g(x)$. Pick k and ℓ as small as possible so that p does not divide a_k and p does not divide b_ℓ. Then, $p|a_i$ for all $i < k$ and $p|b_j$ for all $j < \ell$. Now, consider the coefficient of $x^{k+\ell}$ in $f(x)g(x)$:

$$p \,|\, a_0 b_{k+\ell} + a_1 b_{k+\ell-1} + \cdots + a_k b_\ell + \cdots + a_{k+\ell} b_0.$$

Since p divides all the terms in this sum other than $a_k b_\ell$, and it does *not* divide this term, p does not divide the coefficient of $x^{k+\ell}$ in $f(x)g(x)$. Thus, p does *not* divide all the coefficients of $f(x)g(x)$.

Argument 2. The ideal $(p) \subseteq A$ is prime, and we have a natural ring morphism $f \mapsto \overline{f} : A[x] \to \big(A/(p)\big)[x]$ sending x to x. The kernel of this homomorphism is (p), since if some coefficient of f is not divisible by p, then the corresponding coefficient of $\overline{f}$ is non-zero. Thus, $\big(A/(p)\big)[x] \equiv A[x]/(p)$. Moreover, since $A/(p)$ is a domain, $A/(p)[x]$ is also a domain. Therefore if $\overline{f}$ and $\overline{g}$ are non-zero, then their product in $(\overline{f})(\overline{g}) = \overline{fg} \in A[x]/(p)$ is non-zero. This is what we needed to prove. /////

These two arguments are essentially the same. Both are simply dressed-up versions of the main idea in the proof of the fact that if A is a domain, then so is $A[x]$. Recall that this fact hinges on the identity:

$$(a_k x_k + \cdots a_m x^m)(b_\ell + \cdots + b_n) = a_k b_\ell x^{k+\ell} + \cdots + a_m b_m x^{m+n},$$

where the terms of the polynomials are written in order of ascending degree. If the coefficients a_i and b_j come from a domain, then the product has at least one non-zero term, namely the term of lowest a degree. (Of course, if it has *two* non-zero terms—the lowest- and highest-degree terms—if it has more then one term—i.e., if at least on of the factors has more than one term.)