M7210 Lectures 32 Monday, November 5, 2012

Factorization in Commutative Rings III

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

Content of a polynomial

Let F be the field of fractions of A, where A is a UFD. Every element of F can be written in the form b/c with $b, c \in A$. We can always cancel common irreducible factors from the numerator and denominator, and if this has been done then b and c have no irreducible factors in common. We can extend to F the idea of the "vector of exponents" discussed previously in connection with gcds to F. Assume a set of representatives $\{p, p', \dots\}$ for the irreducibles of A has been chosen. If $b/c \in F$, we define $L(b/c) := L(b) - L(c)$. Thus, $L(b/c)_p$ is the integer (positive or negative) denoting the power to which p appears in the expression for b/c as a unit times a product of powers of irreducibles of A. If $L(b/c)_p$ is negative, then its value is the negative of the exponent of p in the expansion of c, assuming b and c have no common irreducible factors.

Proposition. (Knapp 8.19.) *Every $f \in F[x]$ can be written as $c_f f_0$, with $c_f \in F$ and $f_0 \in A[x]$ primitive. c_f and f_0 are unique up to multiplication by units.*

Proof. Let $f = a_0 + \cdots + a_n x^n$. Let M be the exponent vector such that

$$M_p = \min\{\, L(a_i)_p \mid i = 0, \dots, n\}.$$

Let c_f be any element of F whose exponent vector is M and let $f_0 := c_f^{-1} f$.

> *Example*. Suppose $f = (225/8) + (20/9)x$. Then, $L(a_0)_2 = -3$, $L(a_0)_3 = 2$, $L(a_0)_5 = 2$ and $L(a_0)_p = 0$ if $p \neq 2, 3, 5$. Also, $L(a_1)_2 = 2$, $L(a_1)_3 = -2$, $L(a_1)_5 = 1$ and $L(a_1)_p = 0$ if $p \neq 2, 3, 5$. In this case, $M_2 = -3$, $M_3 = -2$ and $M_5 = 1$, $c_f = (5/72)$ and $f_0 = 45 + 32x$.

Suppose $f_0 = b_0 + \cdots + b_n x^n$. Note that $L(b_i) = L(a_i) - M$. Thus, for each prime p, there is some b_i such that $L(b_i)_p = 0$. Moreover, for all i and all p, $0 \le L(b_i)_p$, and M is the only exponent vector with these properties. /////

We call c_f the *content of f*. Of course, it is only determined up to a unit. In the following, we will write $a \sim b$ if $a = ub$ for some unit $u \in A$, where a and b are any elements of F. In other words, $a \sim b$ is synonymous with $L(a) = L(b)$.

Corollary 1. $(fg)_0 \sim f_0 g_0$ *and* $c_{fg} \sim c_f c_g$.

Proof. By Gauss's Lemma, $f_0 g_0$ is primitive, so $f_0 g_0 \sim (fg)_0$ by the uniqueness clause of 8.19. The second assertion follows from the first. /////

Corollary 2. *Suppose $f \in A[x]$. Then f is irreducible in $A[x]$ if and only if either*
a) f has degree 0 and is irreducible in A or
b) f has degree > 0 and is primitive (in $A[x]$) and irreducible in $F[x]$.

Proof. It is clear that a polynomial of degree 0—i.e., a constant—is irreducible in $A[x]$ if and only if it is irreducible in A. Suppose f has degree > 0 and f is irreducible in $A[x]$.

Observe, first, that f is primitive in $A[x]$. Now, if $f = gh$, with $g, h \in F[x]$, we may write $g = c_g g_0$ and $h = c_h h_0$ with $g_0, h_0 \in A[x]$ primitive. By Corollary 1, $f \sim g_0 h_0$ in $A[x]$. Therefore, either g_0 or h_0 is a unit. Thus, either g or h is a constant—hence a unit—in $F[x]$. Accordingly, f is irreducible in $F[x]$. Suppose f has degree > 0 and is primitive in $A[x]$ and irreducible in $F[x]$. If $f = gh$ with $g, h \in A[x]$, then either g or h must be a unit in $F[x]$, hence an element of A. Say $g \in A$. Since f is primitive, g must be a unit in A. Thus, f is irreducible in $A[x]$. /////

Theorem. (Knapp 8.21.) *If A is a UFD, so is $A[x]$.*

Proof. UFD1: We need to show that $f \in A[x]$ factors into irreducibles. If f is a constant, this is obvious by Corollary 2.a), so assume f is not constant. In this case, it suffices to show that f_0 factors into irreducibles. If f_0 itself is irreducible in $A[x]$, we are done. If f_0 is not irreducible in $A[x]$, then it is a non-zero non-unit in $F[x]$, and it has a factor $g \in F[x]$ of lower degree than f_0. Moreover, if $f_0 = gh$ in $F[x]$, then $f_0 \sim g_0 h_0$ in $A[x]$. Now g_0 and h_0 have lower degree than f, so the result follows by induction.

UFD2′: Suppose $f \in A[x]$ is irreducible. Since $f = c_f f_0$, either f_0 is a unit and $f \sim c_f$ is an irreducible element of A, or c_f is a unit and $f \sim f_0$ is primitive of degree > 0 and is irreducible—hence prime—in $F[x]$. Now we show that in either case, f is prime in $A[x]$. Suppose $g, h \in A[x]$. If a is an irreducible in A and $a|gh$, then $a|c_g c_h$, so $a|c_g$ or $a|c_h$, so $a|g$ or $a|h$. This takes care of the first case. In the second case, if $f|gh$ in $F[x]$, then in $F[x]$ either $f|g$ or $f|h$. Altering notation, if necessary, we may assume $f|g$ in $F[x]$. That is, $g = fk$ in $F[x]$. Now, $c_g \sim c_k$ because f is primitive. Therefore $c_k \in A$ and consequently $k \in A[x]$. Thus $f|g$ in $A[x]$. /////