Unique Factorization in Z[x]

As a further application of the ideas presented in this chapter, we next prove that Z[x] has an important factorization property. We will study this property in greater depth. The first proof of theorem i.e unique factorization in Z[x] was given by Gauss. In reading this theorem and its proof, keep in mind that the units in Z[x] are precisely f(x)=1 and f(x)=-1, the irreducible polynomials of degree 0 over Z are precisely those of the form f(x)=p and f(x)=-p where p is a prime and every non-constant polynomial from Z[x] that is irreducible over Z is primitive.

Theorem: Every polynomial in $Z[x]$ that is not the zero polynomial or a unit in $Z[x]$ can be written in the form

$b_1 b_2 \cdots b_s P_1(x) P_2(x) \cdots P_m(x)$, where the b_i's are irreducible polynomials of degree 0 and the $P_i(x)$'s are irreducible polynomials of positive degree. Furthermore, if

$b_1 b_2 \cdots b_s P_1(x) P_2(x) \cdots P_m(x) = c_1 c_2 \cdots c_t q_1(x) q_2(x) \cdots q_n(x)$,

where the b_i's and c_i's are irreducible polynomials of degree 0 and the $P_i(x)$'s and $q_i(x)$'s are irreducible polynomials of positive degree, then $s = t$, $m = n$ and, after renumbering the c's and $q(x)$'s, we have

$b_i = \pm c_i$ for $i = 1, \cdots, s$

and $P_i(x) = \pm q_i(x)$ for $i = 1, \cdots, m$

Proof: Let $f(x)$ be a non-zero, non-unit Polynomial from $Z[x]$. If $\deg f(x) = 0$, then $f(x)$ is Constant and the result follows from the Fundamental theorem of Arithmetic. If $\deg f(x) > 0$, let b denote the Content of $f(x)$, and let ~~$b_1 b_2 \cdots b_s$~~ be $b_1 b_2 \cdots b_s$ be the factorization of b as a Product of primes. Then

$f(x) = b_1 b_2 \cdots b_s f_1(x)$, where $f_1(x)$ belongs to $Z[x]$, is primitive and $\deg f_1(x) = \deg f(x)$. Thus to Prove the existence Portion of the theorem, it suffices to show that a Primitive polynomial $f(x)$ of Positive degree. We Proceed by induction on $\deg f(x)$. If $\deg f(x) = 1$, then $f(x)$ is already irreducible and we are done

Now suppose that every primitive polynomial of degree less that deg $f(x)$ can be written as a product of irreducibles of positive degree. If $f(x)$ is irreducible, there is nothing to prove. Otherwise, $f(x) = g(x)h(x)$, where both $g(x)$ and $h(x)$ can be written as a product of irreducibles of positive degree. Clearly, then $f(x)$ is also such a product

TO prove the uniqueness portion of the theorem Suppose that $f(x) = b_1 b_2 \cdots b_s P_1(x) P_2(x) \cdots P_m(x) = c_1 c_2 \cdots c_t q_1(x) q_2(x) \cdots q_n(x)$

Where the b_i's and c_i's are irreducible

17 SUNDAY

polynomials of degree 0 and the $P_i(x)$'s and $q_i(x)$'s are irreducible polynomials of positive degree.

Let $b = b_1 b_2 \cdots b_s$ and $c = c_1 c_2 \cdots c_t$.

Since the $P(x)$'s and $q(x)$'s are primitive, it follows from Gauss's Lemma that $P_1(x) P_2(x) \cdots P_m(x)$ and $q_1(x) q_2(x) \cdots q_n(x)$ are primitive. Hence both b and c must equal plus or minus the content of $f(x)$ and, therefore, are equal in absolute value. It then follows from the Fundamental theorem of Arithmetic that $s = t$ and, after renumbering $b_i = \pm c_i$ for $i = 1, 2, \ldots, s$. Thus by canceling the constant terms in the two factorizations for $f(x)$, we have

$$P_1(x) P_2(x) \cdots P_m(x) = \pm q_1(x) q_2(x) \cdots q_n(x).$$

Now viewing the $P(x)$'s and $q(x)$'s as elements of $Q[x]$ and

noting that $P_1(x)$ divides $q_1(x) \cdots q_n(x)$ it follows that $P_1(x) \mid q_i(x)$ for some i.

by renumbering we say ~~as Some i~~ assume $i=1$. Then, Since $q_1(x)$ is irreducible we have $q_1(x) = (r/s) P_1(x)$ where $r, s \in \mathbb{Z}$.

However because both $q_1(x)$ and $P_1(x)$ are primitive, we must have $r/s = \pm 1$,

So, $q_1(x) = \pm P_1(x)$. Also after ~~Cancelling~~ Canceling, we have $P_2(x) P_3(x) \cdots P_m(x) = \pm q_2(x) \cdots q_n$

Now we may repeat the argument above with $P_2(x)$ in place of $P_1(x)$. If $m < n$, after m such steps we would have 1 on the left and a non-constant polynomial on the right and a non-constant polynomial on the left - another

impossibility. So. $m = n$ and $P_i(x) = \pm q_i(x)$ after suitable renumbering of the $q(x)$'s.