Abstract II Spring 2010
Factorization of Polynomials over a Field-Section 23

Throughout this section F denotes a field.

Theorem 0.1. *(Division algorithm for $f[x]$) Let*

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

and

$$g(x) = b_m x^m + \cdots + b_1 x + b_0$$

be two elements of $F[x]$, with a_n and $b_m \neq 0$ and $m > 0$. Then there are unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that

$$f(x) = g(x)q(x) + r(x)$$

where either $r(x) = 0$ or the degree of $r(x)$ is less than the degree m of $g(x)$.

Proof:

Example:

Corollary 0.2. *(Factor theorem) An element $a \in F$ is a zero of $f(x) \in F[x]$ iff $x - a$ is a factor of $f(x) \in F[x]$.*

Proof:

Corollary 0.3. *A nonzero polynomial $f(x) \in F(x)$ of degree n has at most n zeros in a field F.*

Proof:

Irreducible polynomials

Definition 0.4. *A nonconstant polynomial $f(x) \in F[x]$ is irreducible over F if $f(x)$ cannot be expressed as a product $g(x)h(x)$ of two polynomials $g(x)$ and $h(x)$ in $F[x]$ both of lower degree than the degree of $f(x)$. Otherwise it is called reducible.*

True or False: If a polynomial $f(x)$ is irreducible over F then it is irreducible over any field that contains F.

Theorem 0.5. *Let $f(x) \in F[x]$, and let $f(x)$ be of degree 2 or 3. Then $f(x)$ is reducible over F if and only if it has a zero in F.*

Proof:

Theorem 0.6. *If $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ is in $\mathbb{Z}[x]$ with $a_0 \neq 0$ and if $f(x)$ has a zero in $\mathbb{Q}$, then it has a zero $m \in \mathbb{Z}$ and m divides a_0.*

Proof:

Theorem 0.7. *(Eisenstein's Criterion) Let $p \in \mathbb{Z}$ be a prime. Suppose that $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ is in $\mathbb{Z}[x]$, and $a_n \cong 0 \mod p$, but $a_i \equiv 0 \mod p$ for all $i < n$, with $a_0 \ncong 0 \mod p^2$. Then $f(x)$ is irreducible over $\mathbb{Q}$.*

Proof:

Uniqueness of Factorization in $F[x]$

Theorem 0.8. *If F is a field, then every nonconstant polynomial $f(x) \in F[x]$ can be factored in $f[x]$ into a product of irreducible polynomials in a unique way up to the order and units.*

Proof: