Math135 - November 26, 2015

Reducible Polynomials - FTA

Proof: Prove that a polynomial over any field $\mathbb{F}$ of degree $n \geq 1$ has, at most, n distinct roots.

Proof by induction.
Base case: When $n = 1$, $f(x) = ax + c$, which has the sole root, $x = -\frac{c}{a}$. The polynomial is degree one, and has at most, one root.

Inductive Hypothesis: Assume that a polynomial of degree k has at most k roots for some $k \in \mathbb{N}$.

Inductive Conclusion: Need to show: A polynomial of degree $k+1$ has at most $k+1$ distinct roots.
Let $f(x)$ be a polynomial of degree $k+1$.
Assume $x = c_1$ is a root of f.
We know $(x - c_1)$ is a factor of $f(x)$. (FT)
$f(x) = (x - c_1)q(x)$ where $q(x)$ is a polynomial of degree k.
$q(x)$ is a polynomial of degree k, which, by the inductive hypothesis, has at most k roots. Combined with our root $(x - c_1)$, we have at most $k+1$ roots.

$\therefore$ by POMI, the statement holds $\forall n \in \mathbb{N}$

Note: Its important to note that $\mathbb{F}$ is a field. This propery does not apply in $\mathbb{Z}_n$ with a non-prime n, or $\mathbb{Z}$.

Reducible / Irreducible

Let $\mathbb{F}$ be a field. A polynomial in $\mathbb{F}[x]$ positive degree is reducible in $\mathbb{F}[x]$ if it can be written as the product of two polynomials in $\mathbb{F}[x]$ of positive degree. Otherwise, the polynomial is irreducible in $\mathbb{F}[x]$

Ex. Write $f(x) = x^4 + x^2 + 1$ as a product of irreducible factors in$\mathbb{Z}_3[x]$

In $\mathbb{Z}_3$, we only have 3 numbers to check so we can just plug them in and see which produce 0.
$f(0) = 1, f(1) = 0, f(2) = 0$
$\therefore x = 1, 2$ are roots.
So, the polynomial is divisible by $(x-1)(x-2) = (x+2)(x+1) = x^2 + 2$.

$(x^2+2)(x^2+2) = x^4 + x^2 + 1$ (By inspection)
$= (x+2)^2(x+1)^2$
$x = 1, 2$ are repeated roots.

Multiplicity of a Root

The multiplicity of a root c of a polynomial $f(x)$ is the largest positive integer k such that $(x-c)^k$ is a factor of $f(x)$.

Ex. $f(x) = x^2 + 1$ in $\mathbb{R}[x]$
This is irreducible.

Note: $(x^2+1)^2 = x^4 + 2x^2 + 1$ has no roots in $\mathbb{R}[x]$, but is still reducible. Roots and reducible-ness are related, but don't have an absolute 1-1 relationship.

What if we use $\mathbb{C}$?
$x^2 + 1 = (x - i)(x + i)$
So, $x^4 + 2x^2 + 1 = (x-i)^2(x+i)^2$
$x = \pm i$ are roots with multiplicity of 2.

Fundamental Theorem of algebra

For all complex polynomials $f(z)$ with $\deg(f(z)) \geq 1$, there exists a $z_0 \in \mathbb{C}$ such that $f(z_0) = 0$

Ex. Solve $x^3 0x^2 + x - 1 = 0$ in $\mathbb{C}$

$x^2(x-1) + (x-1) = 0$
$(x-1)(x^2+1) = 0$
$x = 1, \pm i$

Complex Polynomials of Degree n Have n Roots (CPN)

If $f(z)$ is a complex polynomial of degree $n \geq 1$, then $f(z)$ has n roots, $c_1, c_2, \ldots, c_n \in \mathbb{C}$ and can be written as:

$$c(z-c_1)(z-c_2)\ldots(z-c_n) \text{ for some } c \in \mathbb{C}$$