Math 320 April 9, 2020

Last: roots, reducibility

Factor Theorem: $f(x) \in F[x]$, $a \in F$.
Then, $a$ is a root of $f(x)$
iff $(x-a) \mid f(x)$.

Cor 4.17: $f(x) \in F[x]$ be nonzero
poly of degree $n$. Then $f(x)$
has at most $n$ roots in $F$.

Pf: By the Factor theorem, if
$f(x)$ has a root $a_1 \in F$, then

$$f(x) = (x-a_1)\, g_1(x)$$

f.s. $g_1(x) \in F[x]$.

If $f(x)$ has another root $a_2 \in F$,
then

$$f(x) = (x-a_1)(x-a_2)\, g_2(x).$$

If $f(x)$ has more roots $a_3, \dots, a_k$, we have

$$f(x) = (x-a_1)(x-a_2)\cdots(x-a_k)\,g_k(x)$$

where $g_k(x) \in F[x]$.

We'll consider two cases:

(1) $k = n$

(2) $k \neq n$, and $g_k(x)$ has no roots in $F$.

Our goal: show $f(x)$ has $\leq n$ roots, which means we want $\boxed{k \leq n.}$

Case 1: $k = n$. We have

$$f(x) = (x-a_1)(x-a_2)\cdots(x-a_n)\,g_n(x)$$

Just need to make sure $g_n(x)$ doesn't have any roots.

Let's look at degrees:

$$n = \deg f(x) = \deg \left[ (x-a_1)(x-a_2)\cdots(x-a_n)\, g_n(x) \right]$$

$$n = \deg(x-a_1) + \deg(x-a_2) + \cdots + \deg(x-a_n) + \deg g_n(x)$$

$$n = \sum_{i=1}^{n} \underbrace{\deg(x-a_i)}_{\text{degree } 1} + \deg g_n(x)$$

$$n = \sum_{i=1}^{n} 1 + \deg g_n(x) = n + \deg g_n(x)$$

$$\Rightarrow n = n + \deg g_n(x)$$

$$\Rightarrow \deg g_n(x) = 0$$

So, $g_n(x)$ is constant, so it has no roots.

This shows $f(x)$ has exactly $n$ roots in this case.

(2) $k \neq n$, and $g_k(x)$ has no roots in $F$.

Similar to above,

$$n = \deg f(x) = \deg\left[(x-a_1)\cdots(x-a_k)\,g_k(x)\right]$$

$$n = \sum_{i=1}^{k} \deg(x-a_i) + \deg g_k(x)$$

$$n = \sum_{i=1}^{k} 1 + \deg g_k(x)$$

$$n = k + \deg g_k(x)$$

degrees are nonnegative, so

$$k < k + \deg g_k(x) = n$$

$$\Rightarrow \boxed{k < n}$$

This shows that $f(x)$ has $k < n$ roots in this case.

In either case, $f(x)$ has $\leq n$ roots. ∎

Cor 4.18: $f(x) \in F[x]$ with $\deg f \geq 2$. If $f(x)$ is irreducible in $F[x]$, then $f(x)$ has no roots in $F$.

Pf: Short contrapositive proof.

Proposition: "If f is irreducible, then f has no roots."

Contrapositive:

"If f has a root, then f is reducible."

If f has a root $a \in F$, then by the Factor Theorem,

$$\underset{\deg \geq 2}{f(x)} = \underset{\deg 1}{(x-a)}\, g(x).$$

Since $\deg f(x) \geq 2$ and $\deg(x-a) = 1$,

$$1 \leq \deg g(x) < \deg f(x).$$

So, $f(x)$ is reducible. This proves the contrapositive, which proves the original statement. $\blacksquare$

Question: Is it true that if $f(x)$ has no roots, then $f$ is irreducible?

That is, is the converse of Cor 4.18 true?

Answer: Sometimes

Cor 4.19: Let $f(x) \in F[x]$ of degree 2 or 3. Then, $f(x)$ is irreducible in $F[x]$ if and only if $f(x)$ has no roots in $F$.

So, if a poly has degree 2 or 3, we can see if it's irreducible by checking for roots.

Ex: $x^2 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$.

Why? it no roots:

$0^2 + 0 + 1 = 1$

$1^2 + 1 + 1 = 1$

no roots

We'll prove this next time.

Note/warning: this <u>only</u> works for polynomials of degree 2 or 3.

You can find plenty of reducible polynomials of higher degree w/ no roots.

Ex: $x^4 - 4$ has no roots in $\mathbb{Q}$.
However, it's reducible, since

$$x^4 - 4 = (x^2 - 2)(x^2 + 2).$$

how to show $(x-2) \mid x^7 - x$ ?

Factor Thm: $a$ is a root of $f(x)$ if and only if $(x-a) \mid f(x)$

$2$ $\qquad x^7 - x$

$$x^7 - x = x(x^6 - 1)$$

also $x = x - 0$

remember, $6 = -1$, $5 = -2$