Lecture 18: Irreducibility criterion for deg 2 and 3

Monday, May 14, 2018 11:10 AM

In the previous lecture we proved:

Lemma. Suppose F is a field and $f(x) \in F[x]$ has degree ≥ 2.

If $f(x)$ has a zero in F, then f is not irreducible.

Then we pointed out the converse is true if $\deg f \leq 3$.

Proposition. Suppose F is a field, $f(x) \in F[x]$, and

$$2 \leq \deg f \leq 3.$$

Then f is irreducible in $F[x]$ $\Leftrightarrow$ f has no zero in F.

Pf. We need to show

$$f \text{ is not irred.} \Leftrightarrow f \text{ has a zero in } F.$$

($\Leftarrow$) we have already proved.

($\Rightarrow$) f is not irreducible in $F[x]$ $\Rightarrow$

$f(x) = g(x)\, h(x)$ and $\deg g, \deg h \geq 1$. Hence

$\deg g + \deg h = \deg f \leq 3$. Therefore either $\deg g = 1$

or $\deg h = 1$. A degree 1 poly. in $F[x]$ has a zero in

F; and so f has a zero in F. ■

Lecture 18: Degree 3 polynomials

Monday, May 14, 2018 11:27 AM

Ex. Suppose $f(x) = x^3 + 3x^2 + 2x + 5$. Prove that $f(x)$ is reducible in $\mathbb{R}[x]$.

Pf. It is enough to show f has a zero in $\mathbb{R}$. We use calculus: $\lim_{x \to +\infty} f(x) = +\infty$, $\lim_{x \to -\infty} f(x) = -\infty$.

And so if a is large enough, $f(a) > 0$; and if b is small enough $f(b) < 0$. Since f is continuous,

$\exists\, b < c < a$, s.t. $f(c) = 0$; and claim follows. ∎

Over $\mathbb{Q}$ we need to use arithmetic, and calculus (over $\mathbb{R}$) is less effective.

Ex. Is $x^3 - x + 2$ irreducible in $\mathbb{Q}[x]$?

Solution. By the previous proposition, if $x^3 - x + 2$ is not irreducible, then it has a rational zero. Any rational number can be written as $\frac{b}{c}$ such that $\gcd(b,c) = 1$ and $c > 0$. So by the contrary assumption, $\exists\, b, c \in \mathbb{Z}$, $\gcd(b,c) = 1$, and $c > 0$, and

$(b/c)^3 - (b/c) + 2 = 0$; and so $b^3 - bc^2 + 2c^3 = 0$. Hence

Lecture 18: Rational root criterion

Monday, May 14, 2018 11:33 AM

$$b^3 - bc^2 = -2c^3 \Rightarrow b\underbrace{(b^2-c^2)}_{\text{in } \mathbb{Z}} = -2c^3 \Rightarrow \left.\begin{array}{l} b \mid 2c^3 \\ \gcd(b,c)=1 \end{array}\right\} \Rightarrow b \mid 2.$$

Similarly $-bc^2 + 2c^3 = -b^3 \Rightarrow c(-bc+2c^2) = -b^3$

$$\left.\begin{array}{l} \Rightarrow c \mid b^3 \\ \gcd(b,c)=1 \end{array}\right\} \Rightarrow \left.\begin{array}{l} c \mid 1 \\ c>0 \end{array}\right\} \Rightarrow c=1.$$

Hence $b/c \in \{2,-2\}$.

x	2	-2
x^3-x+2	8	-4

; and so ± 2 are not zeros of x^3-x+2 which is a contradiction. ∎

This idea can be generalized; and we get the following rational zero criterion:

<u>Proposition</u>. Suppose $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, $a_0 \neq 0$, $a_n \neq 0$. If $f(\frac{b}{c}) = 0$ for $b, c \in \mathbb{Z}$, $c \neq 0$, and $\gcd(b,c)=1$, then $b \mid a_0$ and $c \mid a_n$.

<u>Pf.</u> $f(\frac{b}{c}) = 0$ implies $a_n (\frac{b}{c})^n + a_{n-1}(\frac{b}{c})^{n-1} + \cdots + a_1(\frac{b}{c}) + a_0 = 0$.

Hence $a_n b^n + a_{n-1} b^{n-1} c + \cdots + a_1 b c^{n-1} + a_0 c^n = 0$; and so

$$-a_n b^n = a_{n-1} b^{n-1} c + \cdots + a_1 b c^{n-1} + a_0 c^n = c\underbrace{(a_{n-1} b^{n-1} + \cdots + a_1 b c^{n-2} + a_0 c^{n-1})}_{\text{in } \mathbb{Z}}$$

Lecture 18: Rational root criterion

Monday, May 14, 2018 11:36 AM

and so $\left.\begin{array}{l} c \mid a_n b^n \\ \gcd(b,c)=1 \end{array}\right\} \xRightarrow[\text{lemma}]{\text{Euclid's}} c \mid a_n.$

Similarly, $-a_0 c^n = a_n b^n + a_{n-1} b^{n-1} c + \dots + a_1 b c^{n-1}$

$$= b\underbrace{(a_n b^{n-1} + a_{n-1} b^{n-2} c + \dots + a_1 c^{n-1})}_{\text{in } \mathbb{Z}}$$

Hence $\left.\begin{array}{l} b \mid a_0 c^n \\ \gcd(b, c)=1 \end{array}\right\} \Rightarrow b \mid a_0.$ ∎

Cor (1). Suppose $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in \mathbb{Z}[x]$. Then if $a \in \mathbb{Q}$ is a zero of f, then $a \in \mathbb{Z}$.

(2) Suppose $g(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + 1 \in \mathbb{Z}[x]$. Then if $a \in \mathbb{Q}$ is a zero of f, then $a = \pm 1$.

Pf. (1) $\exists\, b, c \in \mathbb{Z}$, $\gcd(b,c)=1$, $c>0$ s.t. $a = \frac{b}{c}$. So by the rational root criterion, $c \mid$ the leading coeff. of f; this means $c \mid 1$. As $c>0$, we get $c=1$; and so $a = b \in \mathbb{Z}$.

(2) As in part (1), $a \in \mathbb{Z}$ and $a \mid$ the constant term of f; this means $a \mid 1$; and so $a = \pm 1$. ∎

Lecture 18: Having zero in Q and modular numbers

Monday, May 14, 2018 11:38 AM

Another important technique is using $\mathbb{Z}_n$'s.

<u>Proposition.</u> If $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ has a zero in $\mathbb{Q}$, then $f(x)$ has a zero in $\mathbb{Z}_m$ for any $m \in \mathbb{Z}^{\geq 2}$.

(Of course here we mean $c_m(f)$ has a zero in $\mathbb{Z}_m$).

<u>Pf.</u> If f has a zero in $\mathbb{Q}$, then, by the previous corollary, $\exists\, b \in \mathbb{Z}$ s.t. $f(b) = 0$. Since $c_m : \mathbb{Z} \to \mathbb{Z}_m$ is a ring hom., $c_m(f(b)) = 0$; and so $(c_m(f))(c_m(b)) = 0$. Thus $c_m(f)$ has a zero in $\mathbb{Z}_m$.

(It is the same as saying $f(b) \equiv 0 \pmod{m}$.) ∎