Irreducible elements

Sunday, August 20, 2017 10:30 PM

Def. Let R be a unital commutative ring. An element $x \in R$ is called irreducible if

① $x \neq 0$, x is not a zero divisor, and $x \notin U(R)$.

② For $a, b \in R$, $x = ab \Rightarrow$ (either $a \in U(R)$ or $b \in U(R)$).

Ex. $x \in \mathbb{Z}$ is irreducible $\Leftrightarrow$ $x \neq 0$, $x \neq \pm 1$, and the only positive divisors of x are 1 and $|x|$.

(You have been calling such number "prime". We use the word "prime" for another type of elements; and we will show $x \in \mathbb{Z}$ is irreducible $\Leftrightarrow$ it is prime.)

Ex. Let F be a field. Then $f(x) \in F[x]$ is irreducible $\Leftrightarrow$ ① $\deg f \geq 1$

② $f(x)$ cannot be written as a product of non-constant polynomials.

Irreducible polynomials

Sunday, August 20, 2017 10:44 PM

<u>Pf.</u> ($\Rightarrow$) Since F is a field, $F[x]$ is an integral domain.

So it does not have a zero divisor. And $U(F[x]) = U(F)$
$= F\setminus\{0\}$.

So $\deg f \geq 1$.

If $f(x) = a(x)\, b(x)$, then either $a(x) \in U(F[x]) = F\setminus\{0\}$

or $b(x) \in U(F[x]) = F\setminus\{0\}$; which implies that

f cannot be written as a product of non-constant

polynomials.

($\Leftarrow$) Since $U(F[x]) = F\setminus\{0\}$ and $F[x]$ is an integral domain,

$\deg f \geq 1$ implies $f \neq 0$, f is not a zero-divisor,

and f is not a unit.

$f(x) = a(x) b(x) \Rightarrow$ (either $\deg a = 0$ or $\deg b = 0$).

$f \neq 0 \Rightarrow (a \neq 0$ and $b \neq 0)$.

So either $a \in F\setminus\{0\} = U(F[x])$ or $b \in F\setminus\{0\} = U(F[x])$ ∎

<u>Ex.</u> $2x$ is irreducible in $\mathbb{Q}[x]$; but it is reducible

(that means not irreducible) in $\mathbb{Z}[x]$. (Either 2 or x

are not units in $\mathbb{Z}[x]$.

Irreducibility of degree 2 and 3 polynomials

Sunday, August 20, 2017 10:59 PM

<u>Lemma</u>. Let F be a field. Suppose $f \in F[x]$ and $2 \leq \deg f \leq 3$. Then f is reducible in $F[x]$ if and only if f has a zero in F.

<u>Pf.</u> ($\Rightarrow$) $\exists\, a, b \in F[x]$, $\deg a, \deg b \geq 1$ and $ab = f$. Since F is a field, we have $\deg a + \deg b = \deg f$. As $\deg a, \deg b \geq 1$ and $\deg f \leq 3$, either $\deg a = 1$ or $\deg b = 1$. Without loss of generality, we can and will assume $\deg a = 1$. So $a(x) = c_0 + c_1 x$ and $c_1 \neq 0$. Therefore $f(-c_0 c_1^{-1}) = a(-c_0 c_1^{-1})\, b(-c_0 c_1^{-1})$

$$= 0.$$

($\Leftarrow$) If f has a zero $\alpha \in F$, then by the factor theorem $\exists\, g(x) \in F[x]$ such that $f(x) = (x - \alpha) g(x)$.

So $\deg g + \deg(x - \alpha) = \deg f \Rightarrow$

$$\deg g = \deg f - 1 \geq 1.$$

Hence f is reducible. $\blacksquare$

Irreducible polynomials

Sunday, August 20, 2017 11:14 PM

Ex. Show that x^2+1 is reducible in $\mathbb{C}[x]$ and irreducible in $\mathbb{R}[x]$.

Solution. • $x^2+1=(x+i)(x-i)$ and $\deg(x\pm i)\geq 1$. So x^2+1 is reducible in $\mathbb{C}[x]$.

• Suppose x^2+1 is reducible in $\mathbb{R}[x]$. Then by the previous lemma, it has a zero in $\mathbb{R}$; which is a contradiction. ■

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

Solution. It is enough to show f has a zero in $\mathbb{R}$. Notice that, since $\lim_{x\to\infty} f(x)=\infty$ and $\lim_{x\to-\infty} f(x)=-\infty$, for large enough a, we have $f(a)>0$ and for small enough b we have $f(b)<0$. Since f is continuous, $\exists\ b<c<a$ such that $f(c)=0$.

Remark. Using a similar argument one can show:

$$\left(f(x)\in\mathbb{R}[x],\ \deg f>1,\ \deg f \text{ odd}\right)\Rightarrow f \text{ has a zero in } \mathbb{R}$$
$$\Rightarrow f \text{ is reducible in } \mathbb{R}[x].$$

Having a zero in Q

Monday, August 21, 2017 1:32 PM

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

Solution. Since $\deg(x^3-x+2)$, by a Lemma, it is irredu. in $\mathbb{Q}[x]$ exactly when it does not have a zero in $\mathbb{Q}$.

So suppose b/c is a zero of x^3-x+2 where $b, c \in \mathbb{Z}$, $c \neq 0$, and $\gcd(b,c) = 1$. Hence $\left(\frac{b}{c}\right)^3 - \left(\frac{b}{c}\right) + 2 = 0$.

After clearing the denominator, we get

$$b^3 - bc^2 + 2c^3 = 0.$$

So $-2c^3 = b(b^2-c^2)$ which implies $b \mid -2c^3$, and $b \neq 0$

Since $\gcd(b,c)=1$ and $b \mid -2c^3$, we deduce $b \mid 2$.

Similarly $-b^3 = c(-bc+2c^2)$ implies $c \mid -b^3$.

Since $\gcd(b,c)=1$ and $c \mid -b^3$, we deduce $c \mid 1$.

Hence $b/c \in \{\pm 1, \pm 2\}$. Since

x	1	-1	2	-2
x^3-x+2	2	2	8	-4

,

we deduce that x^3-x+2 does not have a zero in $\mathbb{Q}$, and so it is irreducible in $\mathbb{Q}[x]$. ∎

The above method is fairly effective in finding out whether

Having a zero in Q

Monday, August 21, 2017 1:44 PM

an integer polynomial has a zero in $\mathbb{Q}$.

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

$$b \mid a_0 \quad \text{and} \quad c \mid a_n .$$

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

implies $a_n b^n + a_{n-1} b^{n-1} c + \cdots + a_1 b c^{n-1} + a_0 c^n = 0$. $\circledast$

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

which implies $b \mid -a_0 c^n$. Since $\gcd(b,c) = 1$ and $b \mid -a_0 c^n$, we deduce that $b \mid a_0$.

By $\circledast$, we also get

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

So $c \mid -a_n b^n$, which, together with $\gcd(c,b) = 1$, implies $c \mid a_n$. ∎

Using the residue maps to study irreducibility

Monday, August 21, 2017 1:52 PM

<u>Ex.</u> Suppose $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + 1 \in \mathbb{Z}[x]$. Then f has a zero in $\mathbb{Q}$ if and only if either $f(1)=0$ or $f(-1)=0$.

<u>Proof.</u> ($\Leftarrow$) is clear as $\pm 1 \in \mathbb{Q}$.

($\Rightarrow$) By the previous lemma, if $f(\frac{b}{c})=0$ for $b,c\in\mathbb{Z}$, $c\neq 0$, $\gcd(b,c)=1$, then $b \mid 1$ and $c \mid 1$. So $\frac{b}{c} \in \{-1,1\}$, which means either $f(1)=0$ or $f(-1)=0$. ∎

Another important technique is using the residue maps: recall that, for any integer n, $c_n : \mathbb{Z} \to \mathbb{Z}_n$, $c_n(a) = a\, 1_{\mathbb{Z}_n}$ is a ring homomorphism. We can extend it to the ring of polynomials.

<u>Lemma</u>. $c_n : \mathbb{Z}[x] \to \mathbb{Z}_n[x]$, $c_n(\sum_{i=0}^{\infty} a_i x^i) = \sum_{i=0}^{\infty} c_n(a_i) x^i$ is a ring homomorphism.

<u>Pf.</u>
$$c_n\left(\sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} b_i x^i\right) \overset{\text{def. of addition in } \mathbb{Z}[x]}{=} c_n\left(\sum_{i=0}^{\infty} (a_i+b_i)\, x^i\right)$$
$$\overset{\text{def. of } c_n}{=} \sum_{i=0}^{\infty} c_n(a_i+b_i)\, x^i$$

Using the residue maps to study Irreducibility

Monday, August 21, 2017 3:57 PM

$c_n : \mathbb{Z} \to \mathbb{Z}_n$ is a ring homomo.

def. of addition in $\mathbb{Z}_n[x]$

$$= \sum_{i=0}^{\infty} (c_n(a_i) + c_n(b_i))\, x^i$$

$$= \sum_{i=0}^{\infty} c_n(a_i)\, x^i + \sum_{i=0}^{\infty} c_n(b_i)\, x^i$$

$$= c_n\Big(\sum_{i=0}^{\infty} a_i x^i\Big) + c_n\Big(\sum_{i=0}^{\infty} b_i x^i\Big).$$

def. of c_n

$$c_n\Big(\Big(\sum_{i=0}^{\infty} a_i x^i\Big)\Big(\sum_{i=0}^{\infty} b_i x^i\Big)\Big) = c_n\Big(\sum_{k=0}^{\infty}\Big(\sum_{l=0}^{k} a_l b_{k-l}\Big) x^k\Big)$$

$$= \sum_{k=0}^{\infty} c_n\Big(\sum_{l=0}^{k} a_l b_{k-l}\Big) x^k$$

$$= \sum_{k=0}^{\infty} \Big(\sum_{l=0}^{k} c_n(a_l)\, c_n(b_{k-l})\Big) x^k$$

$$= \Big(\sum_{i=0}^{\infty} c_n(a_i)\, x^i\Big)\Big(\sum_{i=0}^{\infty} c_n(b_i)\, x^i\Big)$$

$$= c_n\Big(\sum_{i=0}^{\infty} a_i x^i\Big)\, c_n\Big(\sum_{i=0}^{\infty} b_i x^i\Big).$$

(Exercise. Determine the reasoning behind each equality.) ■

Corollary Let $g(x) = a_r x^r + a_{r-1} x^{r-1} + \cdots + a_0$ and $h(x) = b_s x^s + b_{s-1} x^{s-1} + \cdots + b_0$. Suppose $g, h \in \mathbb{Z}[x]$, and p is a prime which does not divide $a_r b_s$.

Then $c_p(gh) = c_p(g)\, c_p(h)$ and $\deg(c_p(g)) = r$ and $\deg(c_p(h)) = s$.

Using the residue maps to study Irreducibility

Monday, August 21, 2017 4:15 PM

Pf. By the previous lemma, $c_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ is a ring homomorphism. So $c_p(gh) = c_p(g)\, c_p(h)$.

Since $c_p(g) = c_p(a_r)\, x^r + c_p(a_{r-1})\, x^{r-1} + \cdots + c_p(a_0)$ and $c_p(a_r) \neq 0$ (notice $p \nmid a_r$), we have

$$\deg c_p(g) = r.$$

Similarly, since $c_p(h) = c_p(b_s)\, x^s + \cdots + c_p(b_0)$ and $c_p(b_s) \neq 0$ (notice $p \nmid b_s$), we have $\deg c_p(h) = s$. ∎

Corollary. 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 it has a zero in $\mathbb{Z}_m$ for any integer $m \geq 2$. (Here it, in fact, refers to $c_m(f)$.)

Pf. If $f(\frac{b}{c}) = 0$, $b, c \in \mathbb{Z}$, $c \neq 0$, and $\gcd(b,c) = 1$, then

c divides the leading coefficient, which is 1. So $c = \pm 1$; and this implies f has a zero, say d, in $\mathbb{Z}$. So

$d^n + a_{n-1} d^{n-1} + \cdots + a_0 = 0$, which implies

$c_m(d)^n + c_m(a_{n-1})\, c_m(d)^{n-1} + \cdots + c_m(a_0) = 0$. Hence $c_m(d)$ is a zero of $c_m(f)$. ∎

Using the residue maps and Fermat's theorem

Monday, August 21, 2017 4:29 PM

Let's use the above corollary to give a quick answer to the next question.

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

Solution. Since $\deg(x^3-x+2)=3$, it is irreducible exactly when it has no zero in $\mathbb{Q}$.

If it has a zero in $\mathbb{Q}$, then using the previous corollary x^3-x+2 has a zero in $\mathbb{Z}_3$. But by Fermat's theorem $\forall a\in\mathbb{Z}_3$, $a^3=a$; and so $a^3-a+2=2\neq 0$. Hence x^3-x+2 does not have a zero in $\mathbb{Z}_3$; so it does not have a zero in $\mathbb{Q}$, which implies it is irreducible in $\mathbb{Q}[x]$. ∎

Using Fermat's theorem we can find out whether a polyno. with large degrees has a zero in $\mathbb{Z}_p$ (if p is small).

The key tool is the following:

Lemma. Let p be prime, and $n\in\mathbb{Z}^+$. Then for any $a\in\mathbb{Z}_p$, $a^{(p^n)}=a$.

Finding zeros and Fermat's theorem

Monday, August 21, 2017 4:38 PM

Pf. We proceed by induction on n.

Base of induction ($n=1$). This case is given by Fermat's theorem.

Inductive step. Suppose $a^{(p^k)} = a$ for any $a \in \mathbb{Z}_p$. We'd like to show $a^{(p^{k+1})} = a$.

$$a^{(p^{k+1})} = \left(a^{(p^k)}\right)^p \underset{\text{the induction hypothesis}}{=} a^p \overset{\text{Fermat's theorem}}{=} a. \blacksquare$$

Ex. Does $x^{(5^{10})} - x + 2$ have a zero in $\mathbb{Z}_5$?

Solution. By the previous lemma, for any $a \in \mathbb{Z}_5$, we have $a^{(5^{10})} - a + 2 = a - a + 2 = 2 \neq 0$. So $x^{(5^{10})} - x + 2$ does not have a zero in $\mathbb{Z}_5$. $\blacksquare$

Ex. Does $x^{(5^{10})} - x + 2$ have a zero in $\mathbb{Q}$?

Solution. Since the leading coefficient is 1, if $x^{(5^{10})} - x + 2$ has a zero in $\mathbb{Q}$, it has a zero in $\mathbb{Z}$. So $x^{(5^{10})} - x + 2$ has a zero in $\mathbb{Z}_5$, which contradicts the previous example. $\blacksquare$

Finding zeros and Fermat's theorem

Monday, August 21, 2017 9:52 PM

Ex. Does $x^{50}-x+2$ have a zero in $\mathbb{Z}_5$?

Solution. We write 50 in base-5: $50=(5^2)(2)$.

For any $a\in\mathbb{Z}_5$, $a^{50}-a+2=(a^2)^{(5^2)}-a+2$

$$=a^2-a+2.$$

Now that we have a polynomial with small degree we can evaluate at all the elements of $\mathbb{Z}_5$.

a	0	1	-1	2	-2
a^2-a+2	2	2	4	4	3

So $x^{50}-x+2$ does not have a zero in $\mathbb{Z}_5$. ■