

Proposition: (Irreducible decomposition)

Let $p(x) \in K[x]$. If the degree of $p(x)$ is greater than 0, $p(x)$ may be expressed as either a product of irreducible polynomials in $K[x]$ or $p(x)$ is irreducible.

Proof: Induct on the degree of $p(x)$.

If the degree is one, $p(x)$ is irreducible. Now

Suppose the degree of $p(x)$ is $n > 1$ and that

any polynomial of smaller degree factors into irreducibles.

If $p(x)$ is not irreducible,

$$\exists q(x), r(x) \in K[x]$$

of smaller degree such that

$$p(x) = q(x) \cdot r(x)$$

But then by induction,

$q(x)$ and $r(x)$ factor into

irreducibles, so $p(x)$

factors into irreducibles.



Proposition: (infinity of irreducibles)

For any field K , there are infinitely many monic irreducible polynomials in $K[x]$.

Proof: If K is infinite, then

$x-a \in K[x]$ is irreducible

$\forall a \in K$. Since K is infinite,

there are infinitely many such polynomials.

If K is finite, the

proof proceeds exactly like

the proof that there are infinitely many prime numbers.

Using contradiction, suppose

$\exists n$ irreducible monic
polynomials

$$P_1(x), P_2(x), \dots, P_n(x) \in K[x].$$

$$\text{Let } q(x) = (P_1(x) \cdot P_2(x) \cdots P_n(x)) + 1$$

where "1" is the multiplicative identity of K . Then we could
like to say that the remainder
upon division of $q(x)$ by
 $P_1(x), P_2(x), \dots, P_n(x)$ is 1.

Since we know any polynomial
is a product of irreducibles,

This means either

1) $q(x)$ is irreducible and monic,

the degree of $q(x)$ is the sum of the degrees of

$p_1(x), p_2(x), \dots, p_n(x)$,

and so the degree of $q(x)$ is strictly larger than that of $p_i(x) \forall 1 \leq i \leq n$.

In particular, $q(x) \neq p_i(x)$ $\forall 1 \leq i \leq n$, contradiction.

2) \exists an irreducible polynomial

$P_{n+1}(x) \in K[x]$ such that

$$q(x) = P_{n+1}(x) \cdot r(x) \text{ with}$$

$r(x) \in K[x]$. By multiplying

by the inverse of the constant

coefficient of the leading term

of $P_{n+1}(x)$, we can take

$P_{n+1}(x)$ to be monic. Since

none of $p_1(x), p_2(x), \dots, p_n(x)$

are factors of $q(x)$, we get

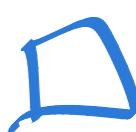
that $P_{n+1}(x) \nmid p_i(x) \forall i \in \{1, \dots, n\}$,

contradiction.

Therefore, \exists infinitely many monic
irreducible polynomials in $K[x]$

if $|K| < \infty$. (modulo

divisibility results)



Proposition: (division) Let $\underline{p(x), q(x)}$ be polynomials in $K[x]$.

If the degree of $q(x)$ is

not $-\infty$, then \exists

polynomials $f(x), r(x)$

in $K[x]$ such that

$$p(x) = q(x) \cdot f(x) + r(x)$$

and the degree of $r(x)$ is smaller than the degree of $q(x)$.

Proof: If the degree of $q(x)$ is greater than the degree of $p(x)$, set

$$f(x) = 0, \quad r(x) = p(x).$$

If the degree of $q(x)$ is less than or equal to that of $p(x)$, we induct on the degree of $p(x)$.

degree 0: Then $p(x)$ is a constant polynomial $p(x) = a$ where $a \neq 0$. Since we assume the degree of $q(x)$ is not $-\infty$, our degree assumption regarding $p(x)$ and $q(x)$ forces $q(x) = b$ where $b \neq 0$. But K is a field, so we can take $r(x) = 0$ and $f(x) = b^{-1} \cdot a$. Then $q(x) \cdot f(x) = b \cdot (b^{-1} \cdot a) = a = p(x)$, by associativity.

Now suppose that

degree = n for some $n \in \mathbb{N}$.

Then $p(x) = \sum_{i=0}^n a_i x^i$

for $a_0, a_1, \dots, a_n \in K$, $a_n \neq 0$.

We know

$$q(x) = \sum_{i=0}^m b_i x^i$$

for $b_0, b_1, \dots, b_m \in K$, $b_m \neq 0$

$m \leq n$. (degree assumption)

Let $\ell(x) = a_n b_m^{-1} x^{n-m}$

Then

$$\ell(x) \cdot q(x)$$

$$= \sum_{i=0}^m a_n b_m^{-1} b_i x^{n-m+i}$$

$$= a_n b_m^{-1} b_m x^n$$

$$+ \sum_{i=0}^{m-1} a_n b_m^{-1} b_i x^{n-m+i}$$

$$= a_n x^n + \sum_{i=0}^{m-1} a_n b_m^{-1} b_i x^{n-m+i}$$

Then

$$p(x) - (l(x) \cdot q(x)) = s(x)$$

where the degree of $s(x)$ is strictly less than the degree of $p(x)$ since $p(x)$ and $l(x) \cdot q(x)$ have the same leading term.

We apply our inductive hypothesis

to $s(x)$ to obtain $g(x), r(x) \in V[x]$

such that

$$s(x) = q(x) \cdot g(x) + r(x)$$

where the degree of $r(x)$ is smaller than that of $q(x)$.

But since

$$p(x) - l(x) \cdot q(x) = s(x) = q(x) \cdot g(x) + r(x),$$

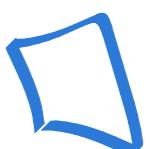
we get that

$$p(x) = q(x) \cdot g(x) + l(x) \cdot q(x) + r(x)$$

$$p(x) = q(x) \cdot \underbrace{(g(x) + l(x))}_{f(x)} + r(x)$$

Setting $f(x) = g(x) + l(x)$, we

have the result.



Comments on Uniqueness of the
previous result:

Suppose $p(x), q(x)$ are as given

in the statement and suppose \exists

$$f_1(x), f_2(x), r_1(x), r_2(x) \in K[x]$$

with the degree of $r_1(x), r_2(x)$ less

than the degree of $q(x)$ such that

$$p(x) = q(x) f_1(x) + r_1(x)$$

$$p(x) = q(x) f_2(x) + r_2(x) .$$

Then subtracting,

$$0 = q(x)f_1(x) + r_1(x) - (q(x)f_2(x) + r_2(x))$$

0 = $q(x)$ $(f_1(x) - f_2(x)) + (r_1(x) - r_2(x))$

degree ≥ 0

- ∞

Either

1) $f_1(x) = f_2(x)$, in which

(case $r_1(x) = r_2(x)$)

- or -

2) $f_1(x) \neq f_2(x)$.

Without loss of generality,
assume that the degree of $f_1(x)$
is greater than or equal to that
of $f_2(x)$.

If the degree of $f_1(x) - f_2(x)$

is positive, then the

degree of $g(x) \cdot (f_1(x) - f_2(x))$

is greater than the degree

of $g(x)$. Since we

assumed the degrees of $r_1(x), r_2(x)$

were strictly smaller than the

degree of $g(x)$,

$$0 \neq g(x) \cdot (f_1(x) - f_2(x)) + \underbrace{(r_1(x) - r_2(x))}_{\text{degree smaller than } g(x)}$$

degree larger than
 $g(x)$

degree smaller
than $g(x)$

This contradicts the fact that

$$0 = g(x) \cdot (f_1(x) - f_2(x)) + (r_1(x) - r_2(x))$$

Now suppose that the degree of $f_1(x) - f_2(x)$ is zero. Then $f_1(x) - f_2(x) = a$ for $a \in K$, $a \neq 0$.

Multiplying both sides of $0 = q(x) \cdot (f_1(x) - f_2(x)) + (f_1(x) - f_2(x))$ by a^{-1} , we get

$$0 = q(x) + \underbrace{a^{-1}(f_1(x) - f_2(x))}_{\text{strictly smaller degree than } q(x)}$$

This sum cannot be zero.

We conclude that

$$f_1(x) = f_2(x), \quad r_1(x) = r_2(x).$$