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. $\square$

Proposition: (infinitude 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

$p_1(x), p_2(x), \ldots, p_n(x) \in K[x]$.

Let $q(x) = (p_1(x) \cdot p_2(x) \cdot \ldots \cdot p_n(x)) + 1$

where "1" is the multiplicative

identity of K. Then we coould

like to say that the remainder

upon division of $q(x)$ by

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

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

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

2) $\exists$ an irreducible polynomial

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

$q(x) = P_{n+1}(x) \cdot r(x)$ 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 $P_{n+1}(x) \neq P_i(x)$ $\forall\, 1 \leq i \leq n$,

contradiction.

Therefore, $\exists$ infinitely many monic irreducible polynomials in $K[x]$ if $|K| < \infty$. (modulo divisibility results)

$\square$

Proposition: (division) Let $p(x), q(x)$ 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

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

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

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 $a_0, a_1, \ldots, a_n \in K$, $a_n \neq 0$.

We know

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

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

$m \leq n$. (degree assumption)

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

Then

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

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

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

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

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

Then

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

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

We apply our inductive hypothesis to $s(x)$ to obtain $g(x), r(x) \in K[x]$ 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

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

we get that

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

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

Setting $f(x) = g(x) + \ell(x)$, we have the result.

$\square$

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,

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

$$\underbrace{0}_{\text{degree } -\infty} = \underbrace{q(x)}_{\text{degree } \geq 0}\left(f_1(x) - f_2(x)\right) + \left(r_1(x) - r_2(x)\right)$$

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 $q(x) \cdot (f_1(x) - f_2(x))$ is greater than the degree of $q(x)$. Since we assumed the degrees of $r_1(x), r_2(x)$ were strictly smaller than the degree of $q(x)$,

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

This contradicts the fact that

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

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

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

by a^{-1}, we get

$$0 = q(x) + a^{-1}(\underbrace{r_1(x) - r_2(x)}_{\text{Strictly smaller degree than } q(x)})$$

This sum cannot be zero.

We conclude that

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