

A root of $p(x) \in \mathbb{F}[x]$ is an element $a \in \mathbb{F}$ such that $p(a) = 0$.

Root-Factor Theorem

a is a root of $p(x)$ if and only if $(x - a)$ divides $p(x)$.

Consequence:

If $p(x)$ is a nonzero polynomial in $\mathbb{F}[x]$ of degree k , then $p(x)$ has at most k roots.

Proof:

$p(x)$ has roots $a_1, \dots, a_\ell \Rightarrow$

$p(x) = (x - a_1)(x - a_2) \cdots (x - a_\ell)m(x)$ for some nonzero polynomial $m(x)$.

Thus, $\deg(p(x)) \geq \ell$. ■

So, if \mathbb{F} is an infinite field, and the polynomial $f(x)$ has $f(a) = 0$ for all $a \in \mathbb{F}$, then $f(x)$ is the zero polynomial.

Not every polynomial has a root; e.g. $f(x) = x^2 + 1$ over \mathbb{R} , or $g(x) = x^2 + x + 1$ over \mathbb{Z}_2 .

However, one can always extend the field to make a given polynomial have a root.

And can always extend the field to make a given nonconstant polynomial be a product of linear factors.

Example: $f(x) = x^2 + 1$ over \mathbb{R} .

Extend the field to \mathbb{C} . Over \mathbb{C} , i is a root of $f(x)$.

Note $\mathbb{C} = \{a + bi : a, b, \in \mathbb{R}\}$ and $i^2 = -1$.

Can mimic this for any irreducible polynomial
 $p(x) = c_0 + c_1x + c_2x^2 + \dots + x^n$ over a field \mathbb{F} .

Elements of new field

$$\mathbb{E} = \{a_0 + a_1j + a_2j^2 + \dots + a_{n-1}j^{n-1} : a_k \in \mathbb{F}\}.$$

Addition—add like terms

Multiplication: use distributivity and whenever we have a j^n
replace it by $-c_0 - c_1j - c_2j^2 - \dots - c_{n-1}j^{n-1}$.

These operations make \mathbb{E} into a field that contains \mathbb{F}

And $p(x)$ has the root j in \mathbb{E} .

Consider $f(x) = x^2 + x + 1$ over \mathbb{Z}_2 .

f is irreducible.

$E = \{a + bj : a, b \in \mathbb{Z}_2\} = \{0 + 0j, 0 + 1j, 1 + 0j, 1 + 1\}$, where
 $j^2 = -j - 1 = j + 1$.

$+$	0	1	j	$1+j$	$*$	0	1	j	$1+j$
0	0	1	j	$1+j$	0	0	0	0	0
1	1	0	$1+j$	j	1	0	1	j	$1+j$
j	j	$1+j$	0	1	j	0	j	$j+1$	1
$1+j$	$1+j$	j	1	0	$j+1$	0	$j+1$	1	j

Note over E , $f(x) = x^2 + x + 1 = (x + j)(x + j + 1)$.

Let's look at another example: $g(x) = x^3 + x + 1$ over \mathbb{Z}_2 .
 $g(x)$ is irreducible.

Set $E = \{a + bj + cj^2 : a, b, c \in \mathbb{Z}_{\neq}\}$, where $j^3 = j + 1$.

+	0	1	j	$1+j$	j^2	j^2+1	j^2+j	j^2+j+1
0	0	1	j	$1+j$	j^2	j^2+1	j^2+j	j^2+j+1
1	1	0	$1+j$	j	j^2+1	j^2	j^2+j+1	j^2+j
j	j	$1+j$	0	1	j^2+j	j^2+j+1	j^2	j^2+1
$j+1$	$j+1$	j	1	0	j^2+j+1	j^2+j	j^2+1	j^2
j^2	j^2	j^2+1	j^2+j	j^2+j+1	0	1	j	$j+1$
j^2+1	j^2+1	j^2	j^2+j+1	j^2+j	1	0	$j+1$	j
j^2+j	j^2+j	j^2+j+1	j^2	j^2+1	j	$j+1$	0	1
j^2+j+1	j^2+j+1	j^2+j	j^2+1	j^2	$j+1$	j	1	0

*	0	1	j	$1+j$	j^2	j^2+1	j^2+j	j^2+j+1
0	0	0	0	0	0	0	0	0
1	0	1	j	$1+j$	j^2	$1+j^2$	j^2+j	j^2+j+1
j	0	j	j^2	j^2+j	$j+1$	1	j^2+j+1	j^2+1
$j+1$	0	$j+1$	j^2+j	j^2+1	j^2+j+1	j^2	1	j
j^2	0	j^2	$j+1$	j^2+j+1	j^2+j	j	j^2+1	1
j^2+1	0	j^2+1	1	j^2	j	j^2+j+1	$j+1$	j^2+j
j^2+j	0	j^2+j	j^2+j+1	1	j^2+1	$j+1$	j	j^2
j^2+j+1	0	j^2+j+1	j^2+1	j	1	j^2+1	j^2	$j+1$

Over E , $f(x) = x^3 + x + 1$ factors as
 $x^3 + x + 1 = (x + j)(x^2 + jx + (j^2 + 1))$.

This is a pain!

Question: Isn't there a field in which every nonconstant polynomial has a root?

Fundamental Theorem of Algebra

Every nonconstant complex polynomial has a complex root.

Consequences of the Fundamental Theorem of Algebra

- The irreducibles in $\mathbb{C}[x]$ are the linear polynomials $x - a$
- Every nonconstant complex polynomial of degree n is the product of n linear polynomials.
- Every nonconstant complex polynomial of degree n has n complex roots (if we count multiplicity).

Consequences for $\mathbb{R}[x]$:

- $p(x) \in \mathbb{R}[x] \Rightarrow \lambda$ root of $p(x)$ if and only if $\bar{\lambda}$ is.
- The irreducibles in $\mathbb{R}[x]$ are the linear polynomials, $x - a$, and the irreducible quadratics $x^2 + ax + b$ where $b^2 - 4ac < 0$.
- Every nonconstant real polynomial is a product of linear and quadratic polynomials, where the quadratic polynomials have no real roots.

Can also show that for every prime p there is a (infinite field) E that contains \mathbb{Z}_p such that every nonconstant polynomial in $E[x]$ has a root in E .

Note that over \mathbb{Z}_2 we have that

$$(x + y)^2 = x^2 + 2xy + y^2 = x^2 + y^2.$$

More generally, over \mathbb{Z}_p we have that

$$(x + y)^p = x^p + y^p.$$

Why? By the binomial theorem, the coefficient of $x^k y^{p-k}$ in $(x + y)^p$ is

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}.$$

This is 0 mod p , unless $k = 0$ or p , and in this case we have 1.

Consequence: Over \mathbb{Z}_p we have:

$$1^p = 1$$

$$(2)^p = (1 + 1)^p = 1^p + 1^p = 1 + 1 = 2$$

$$(3)^p = (1 + 2)^p = 1^p + 2^p = 1 + 2 = 3$$

and so forth.

Fermat's Little Theorem

Let p be a prime. Then $x^p \equiv x \pmod{p}$

Use in modern day cryptography.