Math-123: separability and finite fields

Sebastien Vasey

Harvard University

March 27, 2020

Last time

Define a polynomial to be *separable* if it has no multiple roots.

Last time

Define a polynomial to be *separable* if it has no multiple roots.

Theorem

A root α of $f(x)$ is multiple if and only if it is also a root of the derivative $f'(x)$.

Last time

Define a polynomial to be *separable* if it has no multiple roots.

Theorem

A root α of $f(x)$ is multiple if and only if it is also a root of the derivative $f'(x)$. In particular, a polynomial is separable if and only if it is coprime to its derivative.

Last time

Define a polynomial to be *separable* if it has no multiple roots.

Theorem

A root α of $f(x)$ is multiple if and only if it is also a root of the derivative $f'(x)$. In particular, a polynomial is separable if and only if it is coprime to its derivative.

Corollary

In characteristic zero, irreducible implies separable.

Proof.

If $f(x)$ is irreducible of degree $n \geq 1$, its derivative $f'(x)$ has degree $n - 1$, *hence is not zero*. Since f is irreducible, f' must be coprime to f. □

Where did we use that the underlying field had characteristic zero?

Where did we use that the underlying field had characteristic zero?

Precisely to prove that the derivative of a nonconstant polynomial is not zero!

Where did we use that the underlying field had characteristic zero?

Precisely to prove that the derivative of a nonconstant polynomial is not zero!

Example

Let F be a field of prime characteristic p. Let $f(x) = x^n - 1$.

- The derivative is nx^{n-1}.

Where did we use that the underlying field had characteristic zero?

Precisely to prove that the derivative of a nonconstant polynomial is not zero!

Example

Let F be a field of prime characteristic p. Let $f(x) = x^n - 1$.

- The derivative is nx^{n-1}.
- If n divides p, this is zero!

Where did we use that the underlying field had characteristic zero?

Precisely to prove that the derivative of a nonconstant polynomial is not zero!

Example

Let F be a field of prime characteristic p. Let $f(x) = x^n - 1$.

- The derivative is nx^{n-1}.
- If n divides p, this is zero! In particular, any pth root of unity is multiple.

Where did we use that the underlying field had characteristic zero?

Precisely to prove that the derivative of a nonconstant polynomial is not zero!

Example

Let F be a field of prime characteristic p. Let $f(x) = x^n - 1$.

- The derivative is nx^{n-1}.
- If n divides p, this is zero! In particular, any pth root of unity is multiple.
- If n does not divide p, this is nonzero, and the only roots of the derivative are zero. Thus f is separable: the roots of unity are all distinct.

Where did we use that the underlying field had characteristic zero?

Precisely to prove that the derivative of a nonconstant polynomial is not zero!

Example

Let F be a field of prime characteristic p. Let $f(x) = x^n - 1$.

- The derivative is nx^{n-1}.
- If n divides p, this is zero! In particular, any pth root of unity is multiple.
- If n does not divide p, this is nonzero, and the only roots of the derivative are zero. Thus f is separable: the roots of unity are all distinct.

We can fix the previous corollary to work for all characteristics:

Corollary

An irreducible polynomial *with nonzero derivative* is separable.

When is the derivative zero?

Let F be a field of characteristic $p \neq 0$, let $f(x) = a_n x^n + \ldots + a_0 \in F[x]$. If the derivative of f is zero, then $a_i \neq 0$ implies p must divide i.

When is the derivative zero?

Let F be a field of characteristic $p \neq 0$, let $f(x) = a_n x^n + \ldots + a_0 \in F[x]$. If the derivative of f is zero, then $a_i \neq 0$ implies p must divide i.

The converse is true as well, so a polynomial has zero derivative if and only if its only nonzero coefficients are coefficients of x raised to a multiple of p.

When is the derivative zero?

Let F be a field of characteristic $p \neq 0$, let $f(x) = a_n x^n + \ldots + a_0 \in F[x]$. If the derivative of f is zero, then $a_i \neq 0$ implies p must divide i.

The converse is true as well, so a polynomial has zero derivative if and only if its only nonzero coefficients are coefficients of x raised to a multiple of p.

So we can write $f(x) = b_m x^{pm} + b_{m-1} x^{p(m-1)} + \ldots + b_0$. Thus $f(x) = f_1(x^p)$, where $f_1(x) = b_m x^m + \ldots + b_0$.

When is the derivative zero?

Let F be a field of characteristic $p \neq 0$, let $f(x) = a_n x^n + \ldots + a_0 \in F[x]$. If the derivative of f is zero, then $a_i \neq 0$ implies p must divide i.

The converse is true as well, so a polynomial has zero derivative if and only if its only nonzero coefficients are coefficients of x raised to a multiple of p.

So we can write $f(x) = b_m x^{pm} + b_{m-1} x^{p(m-1)} + \ldots + b_0$. Thus $f(x) = f_1(x^p)$, where $f_1(x) = b_m x^m + \ldots + b_0$.

In words, if $f'(x) = 0$, then $f(x)$ is a polynomial in x^p.

Separable and inseparable degree

Let F be a field of characteristic $p \neq 0$. Let $f(x)$ be an *irreducible* polynomial.

Separable and inseparable degree

Let F be a field of characteristic $p \neq 0$. Let $f(x)$ be an *irreducible* polynomial.

If its derivative is nonzero, f is separable. If not, it is of the form $f(x) = f_1(x^p)$, for some $f_1 \in F[x]$. f_1 is itself irreducible.

Separable and inseparable degree

Let F be a field of characteristic $p \neq 0$. Let $f(x)$ be an *irreducible* polynomial.

If its derivative is nonzero, f is separable. If not, it is of the form $f(x) = f_1(x^p)$, for some $f_1 \in F[x]$. f_1 is itself irreducible.

Is f_1 separable? If not, it can be written $f_1(x) = f_2(x^p)$, so $f(x) = f_2(x^{p^2})$.

Separable and inseparable degree

Let F be a field of characteristic $p \neq 0$. Let $f(x)$ be an *irreducible* polynomial.

If its derivative is nonzero, f is separable. If not, it is of the form $f(x) = f_1(x^p)$, for some $f_1 \in F[x]$. f_1 is itself irreducible.

Is f_1 separable? If not, it can be written $f_1(x) = f_2(x^p)$, so $f(x) = f_2(x^{p^2})$.

Continuing in this way, we see there is a unique $k \geq 0$ and a separable $f_{\text{sep}}(x)$ such that $f(x) = f_{\text{sep}}(x^{p^k})$.

Definition

The degree of f_{sep} is called the *separable degree* of $f(x)$, denoted $\deg_s f(x)$. The integer p^k is called the *inseparability degree* of $f(x)$, denoted $\deg_i f(x)$.

We have that $\deg f(x) = \deg_s f(x) \deg_i f(x)$.

Separable and inseparable degree: examples

Let p be a prime.

- $f(x) = x^p - t$ (as a polynomial with coefficients from the field $\mathbb{F}_p(t)$) is irreducible (seen last time), but its derivative is zero.

Separable and inseparable degree: examples

Let p be a prime.

- $f(x) = x^p - t$ (as a polynomial with coefficients from the field $\mathbb{F}_p(t)$) is irreducible (seen last time), but its derivative is zero. So $f_{\mathrm{sep}}(x) = x - t$, the separable degree of f is 1, its inseparability degree is p. Exercise: check that $f(x)$ has a single root of multiplicity p.

Separable and inseparable degree: examples

Let p be a prime.

- $f(x) = x^p - t$ (as a polynomial with coefficients from the field $\mathbb{F}_p(t)$) is irreducible (seen last time), but its derivative is zero. So $f_{\text{sep}}(x) = x - t$, the separable degree of f is 1, its inseparability degree is p. Exercise: check that $f(x)$ has a single root of multiplicity p.
- More generally, $f(x) = x^{p^n} - t$ has $f_{\text{sep}}(x) = x - t$ and inseparability degree p^n.

pth power: the Frobenius map

Theorem

Let F be a field of characteristic $p \neq 0$. For any $a, b \in F$, $(a+b)^p = a^p + b^p$ and $(ab)^p = a^p b^p$.

pth power: the Frobenius map

Theorem

Let F be a field of characteristic $p \neq 0$. For any $a, b \in F$, $(a+b)^p = a^p + b^p$ and $(ab)^p = a^p b^p$. In fact the map $a \mapsto a^p$ is an injective homomorphism from F to F (called the *Frobenius map*).

pth power: the Frobenius map

Theorem

Let F be a field of characteristic $p \neq 0$. For any $a, b \in F$, $(a+b)^p = a^p + b^p$ and $(ab)^p = a^p b^p$. In fact the map $a \mapsto a^p$ is an injective homomorphism from F to F (called the *Frobenius map*).

Proof.

$(ab)^p = a^p b^p$ is straightforward to see.

pth power: the Frobenius map

Theorem

Let F be a field of characteristic $p \neq 0$. For any $a, b \in F$, $(a+b)^p = a^p + b^p$ and $(ab)^p = a^p b^p$. In fact the map $a \mapsto a^p$ is an injective homomorphism from F to F (called the *Frobenius map*).

Proof.

$(ab)^p = a^p b^p$ is straightforward to see. For the other equation, use the binomial theorem (where $\binom{p}{k} = \frac{p!}{k!(p-k)!}$):

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$$

pth power: the Frobenius map

Theorem

Let F be a field of characteristic $p \neq 0$. For any $a, b \in F$, $(a+b)^p = a^p + b^p$ and $(ab)^p = a^p b^p$. In fact the map $a \mapsto a^p$ is an injective homomorphism from F to F (called the *Frobenius map*).

Proof.

$(ab)^p = a^p b^p$ is straightforward to see. For the other equation, use the binomial theorem (where $\binom{p}{k} = \frac{p!}{k!(p-k)!}$):

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$$

Note p divides $\binom{p}{k}$ if $0 < k < p$, so we are left with just $a^p + b^p$.

pth power: the Frobenius map

Theorem

Let F be a field of characteristic $p \neq 0$. For any $a, b \in F$, $(a+b)^p = a^p + b^p$ and $(ab)^p = a^p b^p$. In fact the map $a \mapsto a^p$ is an injective homomorphism from F to F (called the *Frobenius map*).

Proof.

$(ab)^p = a^p b^p$ is straightforward to see. For the other equation, use the binomial theorem (where $\binom{p}{k} = \frac{p!}{k!(p-k)!}$):

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$$

Note p divides $\binom{p}{k}$ if $0 < k < p$, so we are left with just $a^p + b^p$. For injectivity, check that the kernel of the Frobenius map is $\{0\}$. □

It is natural to ask whether the Frobenius map is *surjective*.

It is natural to ask whether the Frobenius map is *surjective*. Fields like this are called *perfect*:

Definition

A field F of characteristic p is *perfect* if either $p = 0$, or if any element is a pth power: for every $a \in F$, $a = b^p$ for some $b \in F$.

It is natural to ask whether the Frobenius map is *surjective*. Fields like this are called *perfect*:

Definition

A field F of characteristic p is *perfect* if either $p = 0$, or if any element is a pth power: for every $a \in F$, $a = b^p$ for some $b \in F$.

Example

Any finite field F is perfect: the Frobenius map is injective, hence since F is finite must also be surjective!

It is natural to ask whether the Frobenius map is *surjective*. Fields like this are called *perfect*:

Definition

A field F of characteristic p is *perfect* if either $p = 0$, or if any element is a pth power: for every $a \in F$, $a = b^p$ for some $b \in F$.

Example

Any finite field F is perfect: the Frobenius map is injective, hence since F is finite must also be surjective!

Theorem

Irreducible polynomials over a perfect field are separable.

It is natural to ask whether the Frobenius map is *surjective*. Fields like this are called *perfect*:

Definition

A field F of characteristic p is *perfect* if either $p = 0$, or if any element is a pth power: for every $a \in F$, $a = b^p$ for some $b \in F$.

Example

Any finite field F is perfect: the Frobenius map is injective, hence since F is finite must also be surjective!

Theorem

Irreducible polynomials over a perfect field are separable.

This shows for example that any irreducible polynomial over $\mathbb{F}_p[x]$ is separable. This is why we had to look at $\mathbb{F}_p(t)[x]$ to find counterexamples.

Theorem

Irreducible polynomials over a perfect field F are separable.

Proof.

Let $f(x) \in F[x]$ be irreducible. If its derivative is zero, then $f(x) = g(x^p)$, for some $g(x) = a_m x^m + \ldots + a_0$.

Theorem

Irreducible polynomials over a perfect field F are separable.

Proof.

Let $f(x) \in F[x]$ be irreducible. If its derivative is zero, then $f(x) = g(x^p)$, for some $g(x) = a_m x^m + \ldots + a_0$.

For each i, we know that $a_i = b_i^p$ for some b_i, since the field is perfect.

Theorem

Irreducible polynomials over a perfect field F are separable.

Proof.

Let $f(x) \in F[x]$ be irreducible. If its derivative is zero, then $f(x) = g(x^p)$, for some $g(x) = a_m x^m + \ldots + a_0$.

For each i, we know that $a_i = b_i^p$ for some b_i, since the field is perfect.

Thus $f(x) = b_m^p x^{pm} + b_{m-1}^p x^{p(m-1)} + \ldots + b_0^p$, so $f(x) = (b_m x^m + \ldots + b_0)^p$, contradicting irreducibility. □

Finite fields

What we know so far about finite fields:

Finite fields

What we know so far about finite fields:

1. For any prime p, $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ is a field with p elements.

Finite fields

What we know so far about finite fields:

1. For any prime p, $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ is a field with p elements.
2. Any finite field has characteristic a prime p.

Finite fields

What we know so far about finite fields:

1. For any prime p, $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ is a field with p elements.
2. Any finite field has characteristic a prime p.
3. If F is a finite field with characteristic p, then $|F| = p^n$ for some $n \geq 1$ (assignment 6).

Finite fields

What we know so far about finite fields:

1. For any prime p, $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ is a field with p elements.
2. Any finite field has characteristic a prime p.
3. If F is a finite field with characteristic p, then $|F| = p^n$ for some $n \geq 1$ (assignment 6).
4. Finite fields are perfect.

Finite fields

What we know so far about finite fields:

1. For any prime p, $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ is a field with p elements.
2. Any finite field has characteristic a prime p.
3. If F is a finite field with characteristic p, then $|F| = p^n$ for some $n \geq 1$ (assignment 6).
4. Finite fields are perfect.

You also constructed some other fields, for example with cardinality 9 or 8. In general, the problem was to find appropriate irreducibile polynomials.

Finite fields

What we know so far about finite fields:

1. For any prime p, $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ is a field with p elements.
2. Any finite field has characteristic a prime p.
3. If F is a finite field with characteristic p, then $|F| = p^n$ for some $n \geq 1$ (assignment 6).
4. Finite fields are perfect.

You also constructed some other fields, for example with cardinality 9 or 8. In general, the problem was to find appropriate irreducibile polynomials.

We can now avoid this issue and construct finite fields of all possible sizes.

Finite fields: existence

Let $n \geq 1$ and let p be a prime. Let $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$. The derivative is -1, so f is separable: it has p^n distinct roots in its splitting field.

Finite fields: existence

Let $n \geq 1$ and let p be a prime. Let $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$. The derivative is -1, so f is separable: it has p^n distinct roots in its splitting field.

Let F be the set of all these distinct roots (so $|F| = p^n$). We can check that F is a subfield of the splitting field!

Finite fields: existence

Let $n \geq 1$ and let p be a prime. Let $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$. The derivative is -1, so f is separable: it has p^n distinct roots in its splitting field.

Let F be the set of all these distinct roots (so $|F| = p^n$). We can check that F is a subfield of the splitting field! If $\alpha, \beta \in F$ then $\alpha^{p^n} = \alpha$, $\beta^{p^n} = \beta$, so $f(\alpha + \beta) = \alpha + \beta - \alpha - \beta = 0$. Similarly, $f(\alpha\beta) = 0$. Thus $\alpha + \beta, \alpha\beta \in F$. Also, $0 \in F$, $1 \in F$, and $\alpha^{-1} \in F$.

Finite fields: existence

Let $n \geq 1$ and let p be a prime. Let $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$. The derivative is -1, so f is separable: it has p^n distinct roots in its splitting field.

Let F be the set of all these distinct roots (so $|F| = p^n$). We can check that F is a subfield of the splitting field! If $\alpha, \beta \in F$ then $\alpha^{p^n} = \alpha$, $\beta^{p^n} = \beta$, so $f(\alpha + \beta) = \alpha + \beta - \alpha - \beta = 0$. Similarly, $f(\alpha\beta) = 0$. Thus $\alpha + \beta, \alpha\beta \in F$. Also, $0 \in F$, $1 \in F$, and $\alpha^{-1} \in F$.

Thus F is a finite field with p^n elements. It has degree n over $\mathbb{F}_p$. By construction, it is the splitting field of f.

Finite fields: uniqueness

Let F be *any* finite field. Let p be its characteristic. The prime subfield is then $\mathbb{F}_p$. Let n be the degree of F over $\mathbb{F}_p$ (as F is finite, n exists). By basic counting, F has p^n elements.

Finite fields: uniqueness

Let F be *any* finite field. Let p be its characteristic. The prime subfield is then $\mathbb{F}_p$. Let n be the degree of F over $\mathbb{F}_p$ (as F is finite, n exists). By basic counting, F has p^n elements.

Consider the group $F^\times$ of units of F. It has $p^n - 1$ elements, hence by Lagrange's theorem $a^{p^n-1} = 1$ for all $a \in F^\times$.

Finite fields: uniqueness

Let F be *any* finite field. Let p be its characteristic. The prime subfield is then $\mathbb{F}_p$. Let n be the degree of F over $\mathbb{F}_p$ (as F is finite, n exists). By basic counting, F has p^n elements.

Consider the group $F^\times$ of units of F. It has $p^n - 1$ elements, hence by Lagrange's theorem $a^{p^n-1} = 1$ for all $a \in F^\times$.

Multiply both sides by a to get $a^{p^n} = a$. Thus every element of $F^\times$ is a root of $f(x) = x^{p^n} - x$ (and of course 0 also is a root).

Finite fields: uniqueness

Let F be *any* finite field. Let p be its characteristic. The prime subfield is then $\mathbb{F}_p$. Let n be the degree of F over $\mathbb{F}_p$ (as F is finite, n exists). By basic counting, F has p^n elements.

Consider the group $F^\times$ of units of F. It has $p^n - 1$ elements, hence by Lagrange's theorem $a^{p^n-1} = 1$ for all $a \in F^\times$.

Multiply both sides by a to get $a^{p^n} = a$. Thus every element of $F^\times$ is a root of $f(x) = x^{p^n} - x$ (and of course 0 also is a root).

This shows that F must be the splitting field of $f(x)$ over $\mathbb{F}_p$.

Finite fields: uniqueness

Let F be *any* finite field. Let p be its characteristic. The prime subfield is then $\mathbb{F}_p$. Let n be the degree of F over $\mathbb{F}_p$ (as F is finite, n exists). By basic counting, F has p^n elements.

Consider the group $F^\times$ of units of F. It has $p^n - 1$ elements, hence by Lagrange's theorem $a^{p^n-1} = 1$ for all $a \in F^\times$.

Multiply both sides by a to get $a^{p^n} = a$. Thus every element of $F^\times$ is a root of $f(x) = x^{p^n} - x$ (and of course 0 also is a root).

This shows that F must be the splitting field of $f(x)$ over $\mathbb{F}_p$. Since splitting fields are unique, we get that any two finite fields with p^n elements are isomorphic.

Finite fields: uniqueness

Let F be *any* finite field. Let p be its characteristic. The prime subfield is then $\mathbb{F}_p$. Let n be the degree of F over $\mathbb{F}_p$ (as F is finite, n exists). By basic counting, F has p^n elements.

Consider the group $F^\times$ of units of F. It has $p^n - 1$ elements, hence by Lagrange's theorem $a^{p^n-1} = 1$ for all $a \in F^\times$.

Multiply both sides by a to get $a^{p^n} = a$. Thus every element of $F^\times$ is a root of $f(x) = x^{p^n} - x$ (and of course 0 also is a root).

This shows that F must be the splitting field of $f(x)$ over $\mathbb{F}_p$. Since splitting fields are unique, we get that any two finite fields with p^n elements are isomorphic. We have just proven:

Theorem

For any prime p and any natural number $n \geq 1$, there exists a unique (up to isomorphism) field with p^n elements.

We write $\mathbb{F}_{p^n}$ for this field.

And now for something completely different...

Back to cyclotomic extensions: recall if $\zeta_n := e^{2\pi i/n}$, we call the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ the *cyclotomic extension of nth root of unity*. It is the splitting field of $x^n - 1$.

And now for something completely different...

Back to cyclotomic extensions: recall if $\zeta_n := e^{2\pi i/n}$, we call the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ the *cyclotomic extension of nth root of unity*. It is the splitting field of $x^n - 1$.

Theorem

The degree of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is $\phi(n)$.

And now for something completely different...

Back to cyclotomic extensions: recall if $\zeta_n := e^{2\pi i/n}$, we call the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ the *cyclotomic extension of nth root of unity*. It is the splitting field of $x^n - 1$.

Theorem

The degree of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is $\phi(n)$.

Here, $\phi(n)$ is the number of elements $k \in \{1, 2, \ldots, n\}$ such that k is coprime to n.

Groups of roots of unity

Recall: the roots of $x^n - 1$ (in $\mathbb{C}$) are called *nth roots of unity*.
They are of the form ζ_n^k, $1 \leq k \leq n$.

Groups of roots of unity

Recall: the roots of $x^n - 1$ (in $\mathbb{C}$) are called *nth roots of unity*. They are of the form ζ_n^k, $1 \leq k \leq n$.

For each n, the nth roots of unity form a group under multiplication. It is a cylic group, generated by ζ_n. Let μ_n denote that group.

Groups of roots of unity

Recall: the roots of $x^n - 1$ (in $\mathbb{C}$) are called *nth roots of unity*. They are of the form ζ_n^k, $1 \leq k \leq n$.

For each n, the nth roots of unity form a group under multiplication. It is a cylic group, generated by ζ_n. Let μ_n denote that group.

Lemma

d divides n if and only if μ_d is a subgroup of μ_n.

Groups of roots of unity

Recall: the roots of $x^n - 1$ (in $\mathbb{C}$) are called *nth roots of unity*. They are of the form ζ_n^k, $1 \leq k \leq n$.

For each n, the nth roots of unity form a group under multiplication. It is a cylic group, generated by ζ_n. Let μ_n denote that group.

Lemma

d divides n if and only if μ_d is a subgroup of μ_n.

Proof.

If d divides n, say $n = kd$, and ζ is a dth root of unity, then $\zeta^n = \zeta^{kd} = \left(\zeta^d\right)^k = 1$. Thus ζ is an nth root of unity.

Groups of roots of unity

Recall: the roots of $x^n - 1$ (in $\mathbb{C}$) are called *nth roots of unity*. They are of the form ζ_n^k, $1 \leq k \leq n$.

For each n, the nth roots of unity form a group under multiplication. It is a cylic group, generated by ζ_n. Let μ_n denote that group.

Lemma

d divides n if and only if μ_d is a subgroup of μ_n.

Proof.

If d divides n, say $n = kd$, and ζ is a dth root of unity, then $\zeta^n = \zeta^{kd} = \left(\zeta^d\right)^k = 1$. Thus ζ is an nth root of unity.

If $\mu_d \subseteq \mu_n$, then $\zeta_d \in \mu_n$ and it has order d. By Lagrange's theorem, the order of any element of μ_n must divide the order n of μ_n. □

Cyclotomic polynomials

Recall that an nth root of unity is *primitive* if it generates μ_n. We have that ζ_n^k is primitive if and only if k and n are coprime.

Cyclotomic polynomials

Recall that an nth root of unity is *primitive* if it generates μ_n. We have that ζ_n^k is primitive if and only if k and n are coprime.

Definition

The *nth cyclotomic polynomial*, $\Phi_n(x)$ is the polynomial whose roots are the *primitive* nth roots of unity:

$$\Phi_n(x) := \prod_{1 \leq k \leq n, (k,n)=1} (x - \zeta_n^k)$$

Cyclotomic polynomials

Recall that an nth root of unity is *primitive* if it generates μ_n. We have that ζ_n^k is primitive if and only if k and n are coprime.

Definition

The *nth cyclotomic polynomial*, $\Phi_n(x)$ is the polynomial whose roots are the *primitive* nth roots of unity:

$$\Phi_n(x) := \prod_{1 \leq k \leq n, (k,n)=1} (x - \zeta_n^k)$$

Note Φ_n is a monic polynomial of degree $\phi(n)$, which has ζ_n as a root.

Cyclotomic polynomials

Recall that an nth root of unity is *primitive* if it generates μ_n. We have that ζ_n^k is primitive if and only if k and n are coprime.

Definition

The *nth cyclotomic polynomial,* $\Phi_n(x)$ is the polynomial whose roots are the *primitive* nth roots of unity:

$$\Phi_n(x) := \prod_{1 \leq k \leq n, (k,n)=1} (x - \zeta_n^k)$$

Note Φ_n is a monic polynomial of degree $\phi(n)$, which has ζ_n as a root.

We aim eventually to show it is the minimal polynomial of ζ_n over $\mathbb{Q}$.

Note that:

$$x^n - 1 = \prod_{1 \leq k \leq n} (x - \zeta_n^k)$$

Note that:

$$x^n - 1 = \prod_{1 \le k \le n} (x - \zeta_n^k)$$

To go further, observe: if ζ is an element of order d in μ_n, then it is a *primitive dth root of unity*, so:

$$\begin{aligned} x^n - 1 &= \prod_{d \mid n} \left(\prod_{\zeta \in \mu_d,\ \zeta \text{ primitive}} (x - \zeta) \right) \\ &= \prod_{d \mid n} \Phi_d(x) \end{aligned}$$

Note that:

$$x^n - 1 = \prod_{1 \leq k \leq n} (x - \zeta_n^k)$$

To go further, observe: if ζ is an element of order d in μ_n, then it is a *primitive dth root of unity*, so:

$$\begin{aligned} x^n - 1 &= \prod_{d|n} \left(\prod_{\zeta \in \mu_d,\ \zeta \text{ primitive}} (x - \zeta) \right) \\ &= \prod_{d|n} \Phi_d(x) \end{aligned}$$

In particular, looking at degrees, we recover a cute formula from number theory: $n = \sum_{d|n} \phi(d)$.

Some examples of cyclotomic polynomials

Just for fun, let's use the formula $x^n - 1 = \prod_{d|n} \Phi_d(x)$ to compute some cyclotomic polynomials.

Some examples of cyclotomic polynomials

Just for fun, let's use the formula $x^n - 1 = \prod_{d|n} \Phi_d(x)$ to compute some cyclotomic polynomials.

- $\Phi_1(x) = x - 1$.

Some examples of cyclotomic polynomials

Just for fun, let's use the formula $x^n - 1 = \prod_{d|n} \Phi_d(x)$ to compute some cyclotomic polynomials.

- $\Phi_1(x) = x - 1$.
- $\Phi_2(x) = x - (-1) = x + 1$.

Some examples of cyclotomic polynomials

Just for fun, let's use the formula $x^n - 1 = \prod_{d|n} \Phi_d(x)$ to compute some cyclotomic polynomials.

- $\Phi_1(x) = x - 1$.
- $\Phi_2(x) = x - (-1) = x + 1$.
- Observe $x^3 - 1 = \Phi_1(x)\Phi_3(x)$, so $\Phi_3(x) = \frac{x^3-1}{x-1} = x^2 + x + 1$.

Some examples of cyclotomic polynomials

Just for fun, let's use the formula $x^n - 1 = \prod_{d|n} \Phi_d(x)$ to compute some cyclotomic polynomials.

- $\Phi_1(x) = x - 1$.
- $\Phi_2(x) = x - (-1) = x + 1$.
- Observe $x^3 - 1 = \Phi_1(x)\Phi_3(x)$, so $\Phi_3(x) = \frac{x^3-1}{x-1} = x^2 + x + 1$.
- $x^4 - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x)$, so $\Phi_4(x) = \frac{x^4-1}{(x-1)(x+1)} = x^2 + 1$.

Some examples of cyclotomic polynomials

Just for fun, let's use the formula $x^n - 1 = \prod_{d|n} \Phi_d(x)$ to compute some cyclotomic polynomials.

- $\Phi_1(x) = x - 1$.
- $\Phi_2(x) = x - (-1) = x + 1$.
- Observe $x^3 - 1 = \Phi_1(x)\Phi_3(x)$, so $\Phi_3(x) = \frac{x^3-1}{x-1} = x^2 + x + 1$.
- $x^4 - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x)$, so $\Phi_4(x) = \frac{x^4-1}{(x-1)(x+1)} = x^2 + 1$.
- If p is a prime, $x^p - 1 = \Phi_1(x)\Phi_p(x)$, so $\Phi_p(x) = \frac{x^p-1}{x-1} = 1 + x + \ldots + x^{p-1}$.
- Continuing, get $\Phi_6(x) = x^2 - x + 1$.

Some examples of cyclotomic polynomials

Just for fun, let's use the formula $x^n - 1 = \prod_{d|n} \Phi_d(x)$ to compute some cyclotomic polynomials.

- $\Phi_1(x) = x - 1$.
- $\Phi_2(x) = x - (-1) = x + 1$.
- Observe $x^3 - 1 = \Phi_1(x)\Phi_3(x)$, so $\Phi_3(x) = \frac{x^3-1}{x-1} = x^2 + x + 1$.
- $x^4 - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x)$, so $\Phi_4(x) = \frac{x^4-1}{(x-1)(x+1)} = x^2 + 1$.
- If p is a prime, $x^p - 1 = \Phi_1(x)\Phi_p(x)$, so $\Phi_p(x) = \frac{x^p-1}{x-1} = 1 + x + \ldots + x^{p-1}$.
- Continuing, get $\Phi_6(x) = x^2 - x + 1$.
- A few more are in Dummit and Foote.

Lemma

$\Phi_n(x) \in \mathbb{Z}[x]$. That is, a cyclotomic polynomial has integer coefficients!

Lemma

$\Phi_n(x) \in \mathbb{Z}[x]$. That is, a cyclotomic polynomial has integer coefficients!

Proof.

By induction on n. For $n = 1$, $\Phi_1(x) = x - 1$.

Lemma

$\Phi_n(x) \in \mathbb{Z}[x]$. That is, a cyclotomic polynomial has integer coefficients!

Proof.

By induction on n. For $n = 1$, $\Phi_1(x) = x - 1$.

Assume $n \geq 2$ and the result holds below n. We have $x^n - 1 = f(x)\Phi_n(x)$, where $f(x) = \prod_{d|n, d \neq n} \Phi_d(x)$.

Lemma

$\Phi_n(x) \in \mathbb{Z}[x]$. That is, a cyclotomic polynomial has integer coefficients!

Proof.

By induction on n. For $n = 1$, $\Phi_1(x) = x - 1$.

Assume $n \geq 2$ and the result holds below n. We have $x^n - 1 = f(x)\Phi_n(x)$, where $f(x) = \prod_{d|n, d \neq n} \Phi_d(x)$.

By the induction hypothesis, $f(x) \in \mathbb{Z}[x]$.

Lemma

$\Phi_n(x) \in \mathbb{Z}[x]$. That is, a cyclotomic polynomial has integer coefficients!

Proof.

By induction on n. For $n = 1$, $\Phi_1(x) = x - 1$.

Assume $n \geq 2$ and the result holds below n. We have $x^n - 1 = f(x)\Phi_n(x)$, where $f(x) = \prod_{d|n, d \neq n} \Phi_d(x)$.

By the induction hypothesis, $f(x) \in \mathbb{Z}[x]$.

In $\mathbb{Q}(\zeta_n)[x]$, $f(x)$ divides $x^n - 1$. Both $x^n - 1$ and $f(x)$ have rational coefficients, so the division algorithm must yield a polynomial with rational coefficients. Thus $\Phi_n(x) \in \mathbb{Q}[x]$.

Lemma

$\Phi_n(x) \in \mathbb{Z}[x]$. That is, a cyclotomic polynomial has integer coefficients!

Proof.

By induction on n. For $n = 1$, $\Phi_1(x) = x - 1$.

Assume $n \geq 2$ and the result holds below n. We have $x^n - 1 = f(x)\Phi_n(x)$, where $f(x) = \prod_{d|n, d \neq n} \Phi_d(x)$.

By the induction hypothesis, $f(x) \in \mathbb{Z}[x]$.

In $\mathbb{Q}(\zeta_n)[x]$, $f(x)$ divides $x^n - 1$. Both $x^n - 1$ and $f(x)$ have rational coefficients, so the division algorithm must yield a polynomial with rational coefficients. Thus $\Phi_n(x) \in \mathbb{Q}[x]$.

The factorization of $x^n - 1$ into monic irreducibles in $\mathbb{Q}[x]$ and $\mathbb{Z}[x]$ must be the same (Gauss' lemma). In particular, since $f(x)$ divides $x^n - 1$ in $\mathbb{Q}[x]$, it must divide it in $\mathbb{Z}[x]$. Thus $\Phi_n(x) \in \mathbb{Z}[x]$. □

Theorem

$\Phi_n(x)$ is irreducible in $\mathbb{Z}[x]$. Thus the degree of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is $\phi(n)$.

Theorem

$\Phi_n(x)$ is irreducible in $\mathbb{Z}[x]$. Thus the degree of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is $\phi(n)$.

Proof.

Write $\Phi_n(x) = f(x)g(x)$, for f, g monic in $\mathbb{Z}[x]$, f irreducible with some primitive root of unity ζ as a root.

Theorem

$\Phi_n(x)$ is irreducible in $\mathbb{Z}[x]$. Thus the degree of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is $\phi(n)$.

Proof.

Write $\Phi_n(x) = f(x)g(x)$, for f, g monic in $\mathbb{Z}[x]$, f irreducible with some primitive root of unity ζ as a root.

Let p be a prime not dividing n. Then ζ^p is a primitive root of unity. Either $f(\zeta^p) = 0$ or $g(\zeta^p) = 0$.

Theorem

$\Phi_n(x)$ is irreducible in $\mathbb{Z}[x]$. Thus the degree of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is $\phi(n)$.

Proof.

Write $\Phi_n(x) = f(x)g(x)$, for f, g monic in $\mathbb{Z}[x]$, f irreducible with some primitive root of unity ζ as a root.

Let p be a prime not dividing n. Then ζ^p is a primitive root of unity. Either $f(\zeta^p) = 0$ or $g(\zeta^p) = 0$.

If $g(\zeta^p) = 0$, then ζ is a root of $g(x^p)$, so $f(x)$ divides $g(x^p)$ in $\mathbb{Z}[x]$:

Theorem

$\Phi_n(x)$ is irreducible in $\mathbb{Z}[x]$. Thus the degree of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is $\phi(n)$.

Proof.

Write $\Phi_n(x) = f(x)g(x)$, for f, g monic in $\mathbb{Z}[x]$, f irreducible with some primitive root of unity ζ as a root.

Let p be a prime not dividing n. Then ζ^p is a primitive root of unity. Either $f(\zeta^p) = 0$ or $g(\zeta^p) = 0$.

If $g(\zeta^p) = 0$, then ζ is a root of $g(x^p)$, so $f(x)$ divides $g(x^p)$ in $\mathbb{Z}[x]$:

$$g(x^p) = f(x)h(x)$$

Reducing modulo p, we get $\bar{g}(x^p) = (\bar{g}(x))^p = \bar{f}(x)\bar{g}(x)$.

Theorem

$\Phi_n(x)$ is irreducible in $\mathbb{Z}[x]$. Thus the degree of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is $\phi(n)$.

Proof.

Write $\Phi_n(x) = f(x)g(x)$, for f, g monic in $\mathbb{Z}[x]$, f irreducible with some primitive root of unity ζ as a root.

Let p be a prime not dividing n. Then ζ^p is a primitive root of unity. Either $f(\zeta^p) = 0$ or $g(\zeta^p) = 0$.

If $g(\zeta^p) = 0$, then ζ is a root of $g(x^p)$, so $f(x)$ divides $g(x^p)$ in $\mathbb{Z}[x]$:

$$g(x^p) = f(x)h(x)$$

Reducing modulo p, we get $\bar{g}(x^p) = (\bar{g}(x))^p = \bar{f}(x)\bar{g}(x)$.

So $\bar{f}$ and $\bar{g}$ have an irreducible factor in common in $\mathbb{F}_p[x]$! □

Proof of irreducibility of Φ_n, continued

We know also $\bar{f}\bar{g} = \overline{\Phi_n}(x)$. Since $\bar{f}$ and $\bar{g}$ have a factor in common, $\overline{\Phi_n}(x)$ has a multiple root in $\mathbb{F}_p[x]$.

Proof of irreducibility of Φ_n, continued

We know also $\bar{f}\bar{g} = \overline{\Phi_n}(x)$. Since $\bar{f}$ and $\bar{g}$ have a factor in common, $\overline{\Phi_n}(x)$ has a multiple root in $\mathbb{F}_p[x]$.

Thus $x^n - 1$ also has a multiple root in $\mathbb{F}_p[x]$. We saw before that if p does not divide n, $x^n - 1$ is separable, contradiction.

Proof of irreducibility of Φ_n, continued

We know also $\bar{f}\bar{g} = \overline{\Phi_n}(x)$. Since $\bar{f}$ and $\bar{g}$ have a factor in common, $\overline{\Phi_n}(x)$ has a multiple root in $\mathbb{F}_p[x]$.

Thus $x^n - 1$ also has a multiple root in $\mathbb{F}_p[x]$. We saw before that if p does not divide n, $x^n - 1$ is separable, contradiction.

We had that $\Phi_n(x) = f(x)g(x)$, f irreducible, and we took ζ a root of f. We showed $g(\zeta^p) \neq 0$ for any prime p not dividing n.

Proof of irreducibility of Φ_n, continued

We know also $\bar{f}\bar{g} = \overline{\Phi_n}(x)$. Since $\bar{f}$ and $\bar{g}$ have a factor in common, $\overline{\Phi_n}(x)$ has a multiple root in $\mathbb{F}_p[x]$.

Thus $x^n - 1$ also has a multiple root in $\mathbb{F}_p[x]$. We saw before that if p does not divide n, $x^n - 1$ is separable, contradiction.

We had that $\Phi_n(x) = f(x)g(x)$, f irreducible, and we took ζ a root of f. We showed $g(\zeta^p) \neq 0$ for any prime p not dividing n.

Thus $f(\rho^p) = 0$ for *any* root ρ of f and *any* prime p not dividing n.

Proof of irreducibility of Φ_n, continued

We know also $\bar{f}\bar{g} = \overline{\Phi_n}(x)$. Since $\bar{f}$ and $\bar{g}$ have a factor in common, $\overline{\Phi_n}(x)$ has a multiple root in $\mathbb{F}_p[x]$.

Thus $x^n - 1$ also has a multiple root in $\mathbb{F}_p[x]$. We saw before that if p does not divide n, $x^n - 1$ is separable, contradiction.

We had that $\Phi_n(x) = f(x)g(x)$, f irreducible, and we took ζ a root of f. We showed $g(\zeta^p) \neq 0$ for any prime p not dividing n.

Thus $f(\rho^p) = 0$ for *any* root ρ of f and *any* prime p not dividing n.

If ζ is a root of f, any other primitive root of unity is of the form ζ^k, k coprime to n. Thus $k = p_1 p_2 \ldots p_m$, with the p_i's primes not dividing n.

Proof of irreducibility of Φ_n, continued

We know also $\bar{f}\bar{g} = \overline{\Phi_n}(x)$. Since $\bar{f}$ and $\bar{g}$ have a factor in common, $\overline{\Phi_n}(x)$ has a multiple root in $\mathbb{F}_p[x]$.

Thus $x^n - 1$ also has a multiple root in $\mathbb{F}_p[x]$. We saw before that if p does not divide n, $x^n - 1$ is separable, contradiction.

We had that $\Phi_n(x) = f(x)g(x)$, f irreducible, and we took ζ a root of f. We showed $g(\zeta^p) \neq 0$ for any prime p not dividing n.

Thus $f(\rho^p) = 0$ for *any* root ρ of f and *any* prime p not dividing n.

If ζ is a root of f, any other primitive root of unity is of the form ζ^k, k coprime to n. Thus $k = p_1 p_2 \dots p_m$, with the p_i's primes not dividing n.

We showed $f(\zeta^{p_1}) = 0$. Thus applying the previous observation to $\rho = \zeta^{p_1}$ and $p = p_2$, $f(\zeta^{p_1 p_2}) = 0$.

Proof of irreducibility of Φ_n, continued

We know also $\bar{f}\bar{g} = \overline{\Phi_n}(x)$. Since $\bar{f}$ and $\bar{g}$ have a factor in common, $\overline{\Phi_n}(x)$ has a multiple root in $\mathbb{F}_p[x]$.

Thus $x^n - 1$ also has a multiple root in $\mathbb{F}_p[x]$. We saw before that if p does not divide n, $x^n - 1$ is separable, contradiction.

We had that $\Phi_n(x) = f(x)g(x)$, f irreducible, and we took ζ a root of f. We showed $g(\zeta^p) \neq 0$ for any prime p not dividing n.

Thus $f(\rho^p) = 0$ for *any* root ρ of f and *any* prime p not dividing n.

If ζ is a root of f, any other primitive root of unity is of the form ζ^k, k coprime to n. Thus $k = p_1 p_2 \dots p_m$, with the p_i's primes not dividing n.

We showed $f(\zeta^{p_1}) = 0$. Thus applying the previous observation to $\rho = \zeta^{p_1}$ and $p = p_2$, $f(\zeta^{p_1 p_2}) = 0$.

Continuing in this way, we get that $f(\zeta^{p_1 p_2 \cdots p_m}) = 0$. Thus f has *all* primitive roots of unity as roots, so $f = \Phi_n$, as desired.

Summary

- In any field of characteristic p, raising to the pth power gives an injective homomorphism from the field into itself.

Summary

- In any field of characteristic p, raising to the pth power gives an injective homomorphism from the field into itself.
- A field of characteristic p is called *perfect* if the map is also surjective: any element is a power of p. Fields of characteristic zero are also called perfect.

Summary

- In any field of characteristic p, raising to the pth power gives an injective homomorphism from the field into itself.
- A field of characteristic p is called *perfect* if the map is also surjective: any element is a power of p. Fields of characteristic zero are also called perfect.
- Finite fields are perfect.

Summary

- In any field of characteristic p, raising to the pth power gives an injective homomorphism from the field into itself.
- A field of characteristic p is called *perfect* if the map is also surjective: any element is a power of p. Fields of characteristic zero are also called perfect.
- Finite fields are perfect.
- In any perfect field, irreducible polynomials are separable.

Summary

- In any field of characteristic p, raising to the pth power gives an injective homomorphism from the field into itself.
- A field of characteristic p is called *perfect* if the map is also surjective: any element is a power of p. Fields of characteristic zero are also called perfect.
- Finite fields are perfect.
- In any perfect field, irreducible polynomials are separable.
- In a field of characteristic p, an irreducible polynomial $f(x)$ can always be uniquely written as $f(x) = f_{\text{sep}}(x^{p^n})$, for some irreducible separable $f_{\text{sep}}(x)$.

Summary

- In any field of characteristic p, raising to the pth power gives an injective homomorphism from the field into itself.
- A field of characteristic p is called *perfect* if the map is also surjective: any element is a power of p. Fields of characteristic zero are also called perfect.
- Finite fields are perfect.
- In any perfect field, irreducible polynomials are separable.
- In a field of characteristic p, an irreducible polynomial $f(x)$ can always be uniquely written as $f(x) = f_{\text{sep}}(x^{p^n})$, for some irreducible separable $f_{\text{sep}}(x)$.
- For any prime p and any $n \geq 1$, there is a unique field $\mathbb{F}_{p^n}$ with p^n elements.

Summary

- In any field of characteristic p, raising to the pth power gives an injective homomorphism from the field into itself.
- A field of characteristic p is called *perfect* if the map is also surjective: any element is a power of p. Fields of characteristic zero are also called perfect.
- Finite fields are perfect.
- In any perfect field, irreducible polynomials are separable.
- In a field of characteristic p, an irreducible polynomial $f(x)$ can always be uniquely written as $f(x) = f_{\text{sep}}(x^{p^n})$, for some irreducible separable $f_{\text{sep}}(x)$.
- For any prime p and any $n \geq 1$, there is a unique field $\mathbb{F}_{p^n}$ with p^n elements.
- The *nth cyclotomic polynomial* is the product of $(x - \zeta)$ for ζ ranging over all primitive nth root of unity. It is a monic irreducible polynomial in $\mathbb{Z}[x]$ of degree $\phi(n)$.