Math-123: Splitting field and algebraic closure

Sebastien Vasey

Harvard University

March 25, 2020

Administrivia

- New office hours have been announced (see course website).

Administrivia

- New office hours have been announced (see course website).
- Assignment 7 is due Friday, midnight, and assignment 8 is due next Tuesday, midnight.

Administrivia

- New office hours have been announced (see course website).
- Assignment 7 is due Friday, midnight, and assignment 8 is due next Tuesday, midnight.
- Recordings: please do *not* share them.

Administrivia

- New office hours have been announced (see course website).
- Assignment 7 is due Friday, midnight, and assignment 8 is due next Tuesday, midnight.
- Recordings: please do *not* share them.
- Recordings: you may use a pseudonym (let me know what it is!) or turn off your webcam if you are concerned about privacy.

A question from last class

Asked last time: can we prove that these geometric constructions are impossible without using field theory?

A question from last class

Asked last time: can we prove that these geometric constructions are impossible without using field theory?

At least for trisecting the angle we can! See Terrence Tao's proof linked on the course website.

Splitting fields

Last time, we started talking about the splitting field:

Definition

An extension K of a field F is called a *splitting field* for a polynomial $p(x) \in F[x]$ if $p(x)$ factors into linear factors in $K[x]$ (we say that $p(x)$ *splits completely in* $K[x]$), and does not split completely over any proper subfield of K containing F.

Splitting fields

Last time, we started talking about the splitting field:

Definition

An extension K of a field F is called a *splitting field* for a polynomial $p(x) \in F[x]$ if $p(x)$ factors into linear factors in $K[x]$ (we say that $p(x)$ *splits completely in* $K[x]$), and does not split completely over any proper subfield of K containing F.

Essentially, the splitting field of a polynomial is the smallest field extension containing *all* the roots of that polynomial.

Splitting fields

Last time, we started talking about the splitting field:

Definition

An extension K of a field F is called a *splitting field* for a polynomial $p(x) \in F[x]$ if $p(x)$ factors into linear factors in $K[x]$ (we say that $p(x)$ *splits completely in* $K[x]$), and does not split completely over any proper subfield of K containing F.

Essentially, the splitting field of a polynomial is the smallest field extension containing *all* the roots of that polynomial.

We say "the" splitting field because it is unique up to isomorphism.

Uniqueness of splitting fields

Lemma (Uniqueness of simple extensions, 13.1.8 in DF)

Let $\phi : F \cong F'$ be an isomorphism. Let $p(x) \in F[x]$ be an irreducible polynomial and let $p'(x) \in F'[x]$ be the polynomial obtained by applying ϕ to the coefficients of p.

Let α be a root of $p(x)$ (in some extension of F) and let α' be a root of $p'(x)$ (in some extension of F'). Then there exists an isomorphism $\sigma : F(\alpha) \cong F'(\alpha')$ such that $\sigma \restriction F = \phi$.

$$\begin{array}{ccc} F(\alpha) & \xrightarrow[\sigma]{\cong} & F'(\alpha') \\ | & & | \\ F & \xrightarrow[\phi]{\cong} & F' \end{array}$$

Theorem (Uniqueness of splitting field, 13.1.27 in DF)

Let $\phi : F \cong F'$ be an isomorphism. Let $p(x) \in F[x]$ be a polynomial and let $p'(x) \in F'[x]$ be the corresponding polynomial. Let K be a splitting field for $p(x)$ over F, and let K' be a splitting field for $p'(x)$ over F'. Then ϕ extends to $\sigma : K \cong K'$.

$$\begin{array}{ccc} K & \xrightarrow[\sigma]{\cong} & K' \\ \Big| & & \Big| \\ F & \xrightarrow[\phi]{\cong} & F' \end{array}$$

Theorem (Uniqueness of splitting field, 13.1.27 in DF)

Let $\phi : F \cong F'$ be an isomorphism. Let $p(x) \in F[x]$ be a polynomial and let $p'(x) \in F'[x]$ be the corresponding polynomial. Let K be a splitting field for $p(x)$ over F, and let K' be a splitting field for $p'(x)$ over F'. Then ϕ extends to $\sigma : K \cong K'$.

$$\begin{array}{ccc} K & \xrightarrow[\sigma]{\cong} & K' \\ | & & | \\ F & \xrightarrow[\phi]{\cong} & F' \end{array}$$

Proof.

By induction on the degree, n, of $p(x)$. If $n = 1$, $F = K$ and $F' = K'$, so we can take $\sigma = \phi$.

Theorem (Uniqueness of splitting field, 13.1.27 in DF)

Let $\phi : F \cong F'$ be an isomorphism. Let $p(x) \in F[x]$ be a polynomial and let $p'(x) \in F'[x]$ be the corresponding polynomial. Let K be a splitting field for $p(x)$ over F, and let K' be a splitting field for $p'(x)$ over F'. Then ϕ extends to $\sigma : K \cong K'$.

$$\begin{array}{ccc} K & \xrightarrow[\sigma]{\cong} & K' \\ \Big| & & \Big| \\ F & \xrightarrow[\phi]{\cong} & F' \end{array}$$

Proof.

By induction on the degree, n, of $p(x)$. If $n = 1$, $F = K$ and $F' = K'$, so we can take $\sigma = \phi$. If $n \geq 2$, let $f(x)$ be an irreducible factor of $p(x)$. Add a root $\alpha \in K$ for f, $\alpha' \in K'$ for f'. Get $\phi' : F(\alpha) \cong F(\alpha')$. Apply the IH to $p(x)/(x - \alpha)$. □

That is, apply the induction hypothesis to the top part of this diagram and the polynomial $p(x)/(x-\alpha)$, of degree $n-1$.

$$
\begin{array}{ccc}
K & \xrightarrow[\sigma]{\cong} & K' \\
\Big| & & \Big| \\
F(\alpha) & \xrightarrow[\phi']{\cong} & F'(\alpha') \\
\Big| & & \Big| \\
F & \xrightarrow[\phi]{\cong} & F'
\end{array}
$$

That is, apply the induction hypothesis to the top part of this diagram and the polynomial $p(x)/(x-\alpha)$, of degree $n-1$.

$$\begin{array}{ccc}
K & \xrightarrow[\sigma]{\cong} & K' \\
\Big| & & \Big| \\
F(\alpha) & \xrightarrow[\phi']{\cong} & F'(\alpha') \\
\Big| & & \Big| \\
F & \xrightarrow[\phi]{\cong} & F'
\end{array}$$

Note the special case where $F = F'$ and ϕ is the identity. Then we get that any two splitting fields of $p(x)$ over F are isomorphic (and the isomorphism fixes the elements of F).

Splitting field of $x^n - 1$

The roots of the polynomial $x^n - 1 \in \mathbb{Q}[x]$ are called the *nth roots of unity*.

Splitting field of $x^n - 1$

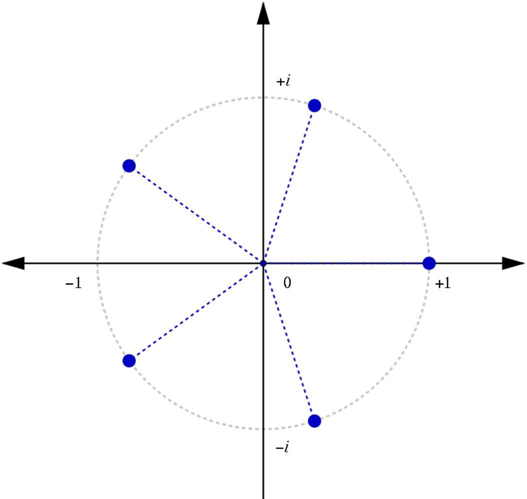
The roots of the polynomial $x^n - 1 \in \mathbb{Q}[x]$ are called the *nth roots of unity*.

They are of the form $e^{2\pi ik/n}$, $k = 1, 2, \ldots, n$.

Splitting field of $x^n - 1$

The roots of the polynomial $x^n - 1 \in \mathbb{Q}[x]$ are called the *nth roots of unity*.

They are of the form $e^{2\pi ik/n}$, $k = 1, 2, \ldots, n$. Drawing for $n = 5$:



Roots of unity

We usually consider the roots of unity inside $\mathbb{C}$, but we can more generally look at them inside *any* field F.

Observation: for a fixed n, the nth roots of unity form a group under multiplication (if $\alpha^n = 1$ and $\beta^n = 1$, then $(\alpha\beta)^n = 1$).

Roots of unity

We usually consider the roots of unity inside $\mathbb{C}$, but we can more generally look at them inside *any* field F.

Observation: for a fixed n, the nth roots of unity form a group under multiplication (if $\alpha^n = 1$ and $\beta^n = 1$, then $(\alpha\beta)^n = 1$).

In fact it is a cyclic group (inside any field, not just $\mathbb{C}$). This follows from the more general:

Roots of unity

We usually consider the roots of unity inside $\mathbb{C}$, but we can more generally look at them inside *any* field F.

Observation: for a fixed n, the nth roots of unity form a group under multiplication (if $\alpha^n = 1$ and $\beta^n = 1$, then $(\alpha\beta)^n = 1$).

In fact it is a cyclic group (inside any field, not just $\mathbb{C}$). This follows from the more general:

Lemma

If F is a field and $F^\times$ is its group of units, then any finite subgroup G of $F^\times$ is cyclic.

Lemma

If F is a field and $F^\times$ is its group of units, then any finite subgroup G of $F^\times$ is cyclic.

Proof.

$F^\times$ is abelian, so G is also abelian. By the structure theorem for finitely generated $\mathbb{Z}$-modules, G is isomorphic to $Z_{n_1} \times Z_{n_2} \times Z_{n_3} \times \ldots \times Z_{n_k}$, where $2 \leq n_1 | n_2 | \ldots | n_k$, and we have written $Z_\ell = \mathbb{Z}/\ell\mathbb{Z}$.

Lemma

If F is a field and $F^\times$ is its group of units, then any finite subgroup G of $F^\times$ is cyclic.

Proof.

$F^\times$ is abelian, so G is also abelian. By the structure theorem for finitely generated $\mathbb{Z}$-modules, G is isomorphic to $Z_{n_1} \times Z_{n_2} \times Z_{n_3} \times \ldots \times Z_{n_k}$, where $2 \leq n_1 | n_2 | \ldots | n_k$, and we have written $Z_\ell = \mathbb{Z}/\ell\mathbb{Z}$.

In particular, any member of G is a root of the polynomial $x^{n_k} - 1$. Thus $n_1 \cdot n_2 \cdot \ldots \cdot n_k = |G| \leq n_k$, so $k = 1$, so G is cyclic. □

Roots of unity, continued

The group of nth roots of unity is cyclic. A generator is called a *primitive* nth root of unity.

Roots of unity, continued

The group of nth roots of unity is cyclic. A generator is called a *primitive* nth root of unity.

$1 = e^{2\pi in/n}$ is not a primitive root of unity (for $n \geq 2$), but $e^{2\pi i/n}$ is a primitive nth root of unity.

Roots of unity, continued

The group of nth roots of unity is cyclic. A generator is called a *primitive* nth root of unity.

$1 = e^{2\pi in/n}$ is not a primitive root of unity (for $n \geq 2$), but $e^{2\pi i/n}$ is a primitive nth root of unity.

In general, $e^{2\pi ik/n}$ is a primitive root of unity if and only if k is coprime to n.

Roots of unity, continued

The group of nth roots of unity is cyclic. A generator is called a *primitive* nth root of unity.

$1 = e^{2\pi in/n}$ is not a primitive root of unity (for $n \geq 2$), but $e^{2\pi i/n}$ is a primitive nth root of unity.

In general, $e^{2\pi ik/n}$ is a primitive root of unity if and only if k is coprime to n. Thus there are exactly $\phi(n)$ primitive roots of unity (ϕ is Euler's Totient function: it gives the number of k coprime to n with $1 \leq k \leq n$).

Roots of unity, continued

The group of nth roots of unity is cyclic. A generator is called a *primitive* nth root of unity.

$1 = e^{2\pi in/n}$ is not a primitive root of unity (for $n \geq 2$), but $e^{2\pi i/n}$ is a primitive nth root of unity.

In general, $e^{2\pi ik/n}$ is a primitive root of unity if and only if k is coprime to n. Thus there are exactly $\phi(n)$ primitive roots of unity (ϕ is Euler's Totient function: it gives the number of k coprime to n with $1 \leq k \leq n$).

We will write ζ_n instead of $e^{2\pi i/n}$. Any other root of unity is of the form ζ_n^k, and it is primitive if and only if k is coprime to n.

Roots of unity, continued

The group of nth roots of unity is cyclic. A generator is called a *primitive* nth root of unity.

$1 = e^{2\pi in/n}$ is not a primitive root of unity (for $n \geq 2$), but $e^{2\pi i/n}$ is a primitive nth root of unity.

In general, $e^{2\pi ik/n}$ is a primitive root of unity if and only if k is coprime to n. Thus there are exactly $\phi(n)$ primitive roots of unity (ϕ is Euler's Totient function: it gives the number of k coprime to n with $1 \leq k \leq n$).

We will write ζ_n instead of $e^{2\pi i/n}$. Any other root of unity is of the form ζ_n^k, and it is primitive if and only if k is coprime to n.

We have shown in particular $\mathbb{Q}(\zeta_n)$ is the splitting field of $x^n - 1$.

Roots of unity, continued

The group of nth roots of unity is cyclic. A generator is called a *primitive* nth root of unity.

$1 = e^{2\pi i n/n}$ is not a primitive root of unity (for $n \geq 2$), but $e^{2\pi i/n}$ is a primitive nth root of unity.

In general, $e^{2\pi i k/n}$ is a primitive root of unity if and only if k is coprime to n. Thus there are exactly $\phi(n)$ primitive roots of unity (ϕ is Euler's Totient function: it gives the number of k coprime to n with $1 \leq k \leq n$).

We will write ζ_n instead of $e^{2\pi i/n}$. Any other root of unity is of the form ζ_n^k, and it is primitive if and only if k is coprime to n.

We have shown in particular $\mathbb{Q}(\zeta_n)$ is the splitting field of $x^n - 1$.

Definition

The field $\mathbb{Q}(\zeta_n)$ is called the *cyclotomic field of nth roots of unity*.

Degree of the cyclotomic field

We will see later that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$.

Degree of the cyclotomic field

We will see later that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$.

We can prove it now for $n = p$ a prime. First factor:

$$x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \ldots + 1)$$

Since $\zeta_p \neq 1$, it is a root of $f(x) = x^{p-1} + x^{p-2} + \ldots + 1$. This polynomial is irreducible, so ζ_p has degree $p - 1 = \phi(p)$.

Degree of the cyclotomic field

We will see later that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$.

We can prove it now for $n = p$ a prime. First factor:

$$x^p - 1 = (x - 1)(x^{p-1} + x^{p-2} + \ldots + 1)$$

Since $\zeta_p \neq 1$, it is a root of $f(x) = x^{p-1} + x^{p-2} + \ldots + 1$. This polynomial is irreducible, so ζ_p has degree $p - 1 = \phi(p)$.

Why is $f(x)$ irreducible? Observe $f(x) = \frac{x^p - 1}{x - 1}$. Replace x by $x + 1$, and write $\binom{p}{k} := \frac{p!}{k!(p-k)!}$. By the binomial theorem, get:

$$\frac{1}{x}\left(\binom{p}{0}x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \ldots + \binom{p}{p-1}x\right)$$
$$= x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \ldots + \binom{p}{p-1}$$

Note p divides all the non-leading coefficients, but the last coefficient is p. Apply Eisenstein's criterion.

Splitting field of $x^p - 2$, p a prime

We considered the case $p = 3$ before. We proceed similarly.

Splitting field of $x^p - 2$, p a prime

We considered the case $p = 3$ before. We proceed similarly.

The roots of $x^p - 2$ are $\zeta \sqrt[p]{2}$, for ζ any pth root of unity.

Splitting field of $x^p - 2$, p a prime

We considered the case $p = 3$ before. We proceed similarly.

The roots of $x^p - 2$ are $\zeta \sqrt[p]{2}$, for ζ any pth root of unity.

Note $\zeta_p = (\zeta_p \sqrt[p]{2})/(\sqrt[p]{2})$, so $\mathbb{Q}(\sqrt[p]{2}, \zeta_p)$ is contained in the splitting field.

Splitting field of $x^p - 2$, p a prime

We considered the case $p = 3$ before. We proceed similarly.

The roots of $x^p - 2$ are $\zeta \sqrt[p]{2}$, for ζ any pth root of unity.

Note $\zeta_p = (\zeta_p \sqrt[p]{2})/(\sqrt[p]{2})$, so $\mathbb{Q}(\sqrt[p]{2}, \zeta_p)$ is contained in the splitting field.

On the other hand if ζ is a pth root of unity, $\zeta \sqrt[p]{2} = \zeta_p^k \sqrt[p]{2}$ for some k, so $\zeta \sqrt[p]{2} \in \mathbb{Q}(\sqrt[p]{2}, \zeta_p)$, so $\mathbb{Q}(\sqrt[p]{2}, \zeta_p)$ *is* the splitting field.

Splitting field of $x^p - 2$, p a prime

We considered the case $p = 3$ before. We proceed similarly.

The roots of $x^p - 2$ are $\zeta\sqrt[p]{2}$, for ζ any pth root of unity.

Note $\zeta_p = (\zeta_p\sqrt[p]{2})/(\sqrt[p]{2})$, so $\mathbb{Q}(\sqrt[p]{2}, \zeta_p)$ is contained in the splitting field.

On the other hand if ζ is a pth root of unity, $\zeta\sqrt[p]{2} = \zeta_p^k\sqrt[p]{2}$ for some k, so $\zeta\sqrt[p]{2} \in \mathbb{Q}(\sqrt[p]{2}, \zeta_p)$, so $\mathbb{Q}(\sqrt[p]{2}, \zeta_p)$ *is* the splitting field.

What is the degree of the splitting field? Well $\mathbb{Q}(\sqrt[p]{2}, \zeta_p)$ is the composite of $\mathbb{Q}(\sqrt[p]{2})$ and $\mathbb{Q}(\zeta_p)$. The first has degree p, the second degree $p - 1$. Since p and $p - 1$ are relatively prime, the degree of the splitting field is $p(p - 1)$.

Algebraic closure

A simple algebraic extension adds *one* root of *one* polynomial.

Algebraic closure

A simple algebraic extension adds *one* root of *one* polynomial.

The splitting field adds *all* roots of *one* polynomial.

Algebraic closure

A simple algebraic extension adds *one* root of *one* polynomial.

The splitting field adds *all* roots of *one* polynomial.

Why not add *all* roots of *all* polynomials?

Algebraic closure

A simple algebraic extension adds *one* root of *one* polynomial.

The splitting field adds *all* roots of *one* polynomial.

Why not add *all* roots of *all* polynomials?

Definition

The field $\bar{F}$ is called an *algebraic closure* of F if $\bar{F}$ is an algebraic extension of F and *every* polynomial $p(x) \in F[x]$ splits completely over $\bar{F}$ *[recall this means that p has only linear factors in $\bar{F}[x]$]*.

Algebraic closure

A simple algebraic extension adds *one* root of *one* polynomial.

The splitting field adds *all* roots of *one* polynomial.

Why not add *all* roots of *all* polynomials?

Definition

The field $\bar{F}$ is called an *algebraic closure* of F if $\bar{F}$ is an algebraic extension of F and *every* polynomial $p(x) \in F[x]$ splits completely over $\bar{F}$ *[recall this means that p has only linear factors in $\bar{F}[x]$]*.

We can go even further:

Definition

A field K is *algebraically closed* if every polynomial in $K[x]$ has a root in K.

Algebraic closure

A simple algebraic extension adds *one* root of *one* polynomial.

The splitting field adds *all* roots of *one* polynomial.

Why not add *all* roots of *all* polynomials?

Definition

The field $\bar{F}$ is called an *algebraic closure* of F if $\bar{F}$ is an algebraic extension of F and *every* polynomial $p(x) \in F[x]$ splits completely over $\bar{F}$ *[recall this means that p has only linear factors in $\bar{F}[x]$]*.

We can go even further:

Definition

A field K is *algebraically closed* if every polynomial in $K[x]$ has a root in K.

Note that if K is algebraically closed, then every $p(x) \in K[x]$ has *all* its roots in K: use repeated division.

Properties of the algebraic closure

- K is algebraically closed if and only if $\bar{K} = K$ (K is its own algebraic closure).

Properties of the algebraic closure

- K is algebraically closed if and only if $\bar{K} = K$ (K is its own algebraic closure).
- An algebraic closure $\bar{F}$ of F is algebraically closed.

Properties of the algebraic closure

- K is algebraically closed if and only if $\bar{K} = K$ (K is its own algebraic closure).
- An algebraic closure $\bar{F}$ of F is algebraically closed. *[Why? let $p(x) \in \bar{F}[x]$. Let $\bar{F}(\alpha)$ be an extension with a root α for p. $\bar{F}(\alpha)$ is algebraic over $\bar{F}$, and $\bar{F}$ is algebraic over F, hence $\bar{F}(\alpha)$ is algebraic over F, so α is algebraic over F, but that means $\alpha \in \bar{F}$, as desired.]*

Properties of the algebraic closure

- K is algebraically closed if and only if $\bar{K} = K$ (K is its own algebraic closure).
- An algebraic closure $\bar{F}$ of F is algebraically closed. *[Why? let $p(x) \in \bar{F}[x]$. Let $\bar{F}(\alpha)$ be an extension with a root α for p. $\bar{F}(\alpha)$ is algebraic over $\bar{F}$, and $\bar{F}$ is algebraic over F, hence $\bar{F}(\alpha)$ is algebraic over F, so α is algebraic over F, but that means $\alpha \in \bar{F}$, as desired.]*
- Any field has an algebraic closure

Properties of the algebraic closure

- K is algebraically closed if and only if $\bar{K} = K$ (K is its own algebraic closure).
- An algebraic closure $\bar{F}$ of F is algebraically closed. *[Why? let $p(x) \in \bar{F}[x]$. Let $\bar{F}(\alpha)$ be an extension with a root α for p. $\bar{F}(\alpha)$ is algebraic over $\bar{F}$, and $\bar{F}$ is algebraic over F, hence $\bar{F}(\alpha)$ is algebraic over F, so α is algebraic over F, but that means $\alpha \in \bar{F}$, as desired.]*
- Any field has an algebraic closure *[Proof idea: iterate through all polynomials and keep adding roots. The precise version uses Zorn's lemma. There is another proof in the book.]*

Properties of the algebraic closure

- K is algebraically closed if and only if $\bar{K} = K$ (K is its own algebraic closure).
- An algebraic closure $\bar{F}$ of F is algebraically closed. *[Why? let $p(x) \in \bar{F}[x]$. Let $\bar{F}(\alpha)$ be an extension with a root α for p. $\bar{F}(\alpha)$ is algebraic over $\bar{F}$, and $\bar{F}$ is algebraic over F, hence $\bar{F}(\alpha)$ is algebraic over F, so α is algebraic over F, but that means $\alpha \in \bar{F}$, as desired.]*
- Any field has an algebraic closure *[Proof idea: iterate through all polynomials and keep adding roots. The precise version uses Zorn's lemma. There is another proof in the book.]*
- Any two algebraic closures of a given field are isomorphic (as for the splitting field).

Properties of the algebraic closure

- K is algebraically closed if and only if $\bar{K} = K$ (K is its own algebraic closure).
- An algebraic closure $\bar{F}$ of F is algebraically closed. *[Why? let $p(x) \in \bar{F}[x]$. Let $\bar{F}(\alpha)$ be an extension with a root α for p. $\bar{F}(\alpha)$ is algebraic over $\bar{F}$, and $\bar{F}$ is algebraic over F, hence $\bar{F}(\alpha)$ is algebraic over F, so α is algebraic over F, but that means $\alpha \in \bar{F}$, as desired.]*
- Any field has an algebraic closure *[Proof idea: iterate through all polynomials and keep adding roots. The precise version uses Zorn's lemma. There is another proof in the book.]*
- Any two algebraic closures of a given field are isomorphic (as for the splitting field). *[Proof idea: similar to the proof of uniqueness of splitting field. Build the isomorphism "polynomial by polynomial".]*

Example

The complex numbers $\mathbb{C}$ are an algebraically closed field (fundamental theorem of algebra). We will give a proof later.

Example

The complex numbers $\mathbb{C}$ are an algebraically closed field (fundamental theorem of algebra). We will give a proof later.

However the algebraic closure of $\mathbb{Q}$ is *not* $\mathbb{C}$, since $\mathbb{C}$ is not an algebraic extension of $\mathbb{Q}$. Intuitively, the algebraic closure is the *smallest* algebraically closed extension.

Example

The complex numbers $\mathbb{C}$ are an algebraically closed field (fundamental theorem of algebra). We will give a proof later.

However the algebraic closure of $\mathbb{Q}$ is *not* $\mathbb{C}$, since $\mathbb{C}$ is not an algebraic extension of $\mathbb{Q}$. Intuitively, the algebraic closure is the *smallest* algebraically closed extension.

The algebraic closure of $\mathbb{Q}$ is in fact (by construction) the set $\bar{\mathbb{Q}}$ of all algebraic elements over $\mathbb{Q}$.

Example

The complex numbers $\mathbb{C}$ are an algebraically closed field (fundamental theorem of algebra). We will give a proof later.

However the algebraic closure of $\mathbb{Q}$ is *not* $\mathbb{C}$, since $\mathbb{C}$ is not an algebraic extension of $\mathbb{Q}$. Intuitively, the algebraic closure is the *smallest* algebraically closed extension.

The algebraic closure of $\mathbb{Q}$ is in fact (by construction) the set $\bar{\mathbb{Q}}$ of all algebraic elements over $\mathbb{Q}$.

Bottom line: this clarifies what it means to, given a field F and an irreducible polynomial $p(x)$, "add a root α for $p(x)$, and get $F(\alpha)$".

Example

The complex numbers $\mathbb{C}$ are an algebraically closed field (fundamental theorem of algebra). We will give a proof later.

However the algebraic closure of $\mathbb{Q}$ is *not* $\mathbb{C}$, since $\mathbb{C}$ is not an algebraic extension of $\mathbb{Q}$. Intuitively, the algebraic closure is the *smallest* algebraically closed extension.

The algebraic closure of $\mathbb{Q}$ is in fact (by construction) the set $\bar{\mathbb{Q}}$ of all algebraic elements over $\mathbb{Q}$.

Bottom line: this clarifies what it means to, given a field F and an irreducible polynomial $p(x)$, "add a root α for $p(x)$, and get $F(\alpha)$". Technically this means we look at $F[x]/(p(x))$, identify α with $\bar{x}$, identify F with its image inside this field, etc.

Example

The complex numbers $\mathbb{C}$ are an algebraically closed field (fundamental theorem of algebra). We will give a proof later.

However the algebraic closure of $\mathbb{Q}$ is *not* $\mathbb{C}$, since $\mathbb{C}$ is not an algebraic extension of $\mathbb{Q}$. Intuitively, the algebraic closure is the *smallest* algebraically closed extension.

The algebraic closure of $\mathbb{Q}$ is in fact (by construction) the set $\bar{\mathbb{Q}}$ of all algebraic elements over $\mathbb{Q}$.

Bottom line: this clarifies what it means to, given a field F and an irreducible polynomial $p(x)$, "add a root α for $p(x)$, and get $F(\alpha)$". Technically this means we look at $F[x]/(p(x))$, identify α with $\bar{x}$, identify F with its image inside this field, etc.

Another way to think about it: we fix once and for all an extension K of F containing an algebraic closure $\bar{F}$ of F, then can assume all roots of polynomial in $F[x]$ are in K. We did this already for $F = \mathbb{Q}$ by working in $K = \mathbb{C}$.

Multiplicity of roots

Let F be a field, $f(x) \in F[x]$ be a polynomial with leading coefficient $a_n \neq 0$.

Multiplicity of roots

Let F be a field, $f(x) \in F[x]$ be a polynomial with leading coefficient $a_n \neq 0$.

In the splitting field K of $f(x)$ over F, we can write:

$$f(x) = a_n(x-\alpha_1)^{n_1}(x-\alpha_2)^{n_2}\dots(x-\alpha_k)^{n_k}$$

where $\alpha_1, \dots, \alpha_k \in K$ are distinct, and $n_i \geq 1$ for all i.

Multiplicity of roots

Let F be a field, $f(x) \in F[x]$ be a polynomial with leading coefficient $a_n \neq 0$.

In the splitting field K of $f(x)$ over F, we can write:

$$f(x) = a_n(x - \alpha_1)^{n_1}(x - \alpha_2)^{n_2} \dots (x - \alpha_k)^{n_k}$$

where $\alpha_1, \dots, \alpha_k \in K$ are distinct, and $n_i \geq 1$ for all i.

Definition

The number n_i is called the *multiplicity* of the root α_i. If $n_i = 1$, α_i is called a *simple root*. Otherwise it is called a *multiple root*.

Multiplicity of roots

Let F be a field, $f(x) \in F[x]$ be a polynomial with leading coefficient $a_n \neq 0$.

In the splitting field K of $f(x)$ over F, we can write:

$$f(x) = a_n(x - \alpha_1)^{n_1}(x - \alpha_2)^{n_2} \dots (x - \alpha_k)^{n_k}$$

where $\alpha_1, \dots, \alpha_k \in K$ are distinct, and $n_i \geq 1$ for all i.

Definition

The number n_i is called the *multiplicity* of the root α_i. If $n_i = 1$, α_i is called a *simple root*. Otherwise it is called a *multiple root*.

Definition

We call $f(x)$ *separable* if it has no multiple roots (i.e. $n_i = 1$ for all i). We call $f(x)$ *inseparable* otherwise.

Example

- $x^2 - 2 \in \mathbb{Q}[x]$ is separable: it has distinct roots $\sqrt{2}$ and $-\sqrt{2}$.

Example

- $x^2 - 2 \in \mathbb{Q}[x]$ is separable: it has distinct roots $\sqrt{2}$ and $-\sqrt{2}$.
- $(x^2 - 2)^3$ is inseparable: $\sqrt{2}$ and $-\sqrt{2}$ have multiplicity 3.

Example

- $x^2 - 2 \in \mathbb{Q}[x]$ is separable: it has distinct roots $\sqrt{2}$ and $-\sqrt{2}$.
- $(x^2 - 2)^3$ is inseparable: $\sqrt{2}$ and $-\sqrt{2}$ have multiplicity 3.
- A nontrivial example: take $F = \mathbb{F}_2(t)$, the field of rational functions in t. Consider $x^2 - t \in F[x]$.

Example

- $x^2 - 2 \in \mathbb{Q}[x]$ is separable: it has distinct roots $\sqrt{2}$ and $-\sqrt{2}$.
- $(x^2 - 2)^3$ is inseparable: $\sqrt{2}$ and $-\sqrt{2}$ have multiplicity 3.
- A nontrivial example: take $F = \mathbb{F}_2(t)$, the field of rational functions in t. Consider $x^2 - t \in F[x]$. It is irreducible (!) by Eisenstein: t is a prime element of $\mathbb{F}_2[t]$.

Example

- $x^2 - 2 \in \mathbb{Q}[x]$ is separable: it has distinct roots $\sqrt{2}$ and $-\sqrt{2}$.
- $(x^2 - 2)^3$ is inseparable: $\sqrt{2}$ and $-\sqrt{2}$ have multiplicity 3.
- A nontrivial example: take $F = \mathbb{F}_2(t)$, the field of rational functions in t. Consider $x^2 - t \in F[x]$. It is irreducible (!) by Eisenstein: t is a prime element of $\mathbb{F}_2[t]$.
  Let $\sqrt{t}$ denote a root (in some extension). Then
  $(x - \sqrt{t})^2 = x^2 + t = x^2 - t$ (because $2 = 0$ in this field!).
  Thus $x^2 - t$ is inseparable: $\sqrt{t}$ has multiplicity 2.

Testing for multiple roots

Definition

If $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \in F[x]$, the *derivative* of $f(x)$ is the polynomial
$D_x f(x) := n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \ldots + 2a_2 x + a_1 \in F[x]$.

Testing for multiple roots

Definition

If $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \in F[x]$, the *derivative* of $f(x)$ is the polynomial
$D_x f(x) := n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \ldots + 2a_2 x + a_1 \in F[x]$.

Exercise: check that the sum and product rules for derivatives hold in this context.

Theorem

A polynomial $f(x)$ has multiple root α if and only if α is a root of both $f(x)$ and $D_x f(x)$.

Corollary

$f(x)$ has multiple root α if and only if $f(x)$ and $D_x f(x)$ are both divisible by the minimal polynomial of α (over the base field). In particular, $f(x)$ is separable if and only if it is coprime to $D_x f(x)$.

Corollary

$f(x)$ is separable if and only if it is coprime to $D_x f(x)$.

Corollary

Every irreducible polynomial $f(x)$ over a field of characteristic 0 is separable.

Corollary

$f(x)$ is separable if and only if it is coprime to $D_x f(x)$.

Corollary

Every irreducible polynomial $f(x)$ over a field of characteristic 0 is separable.

Proof.

If f has degree $n \geq 1$, then $D_x f(x)$ has degree $n - 1$. In particular, it is not zero. The only divisors of f are 1 and $f(x)$, and by degree consideration, $f(x)$ does not divide $D_x f(x)$. □

Corollary

$f(x)$ is separable if and only if it is coprime to $D_x f(x)$.

Corollary

Every irreducible polynomial $f(x)$ over a field of characteristic 0 is separable.

Proof.

If f has degree $n \geq 1$, then $D_x f(x)$ has degree $n - 1$. In particular, it is not zero. The only divisors of f are 1 and $f(x)$, and by degree consideration, $f(x)$ does not divide $D_x f(x)$. □

Question to think about: where does this fail in characteristic p?

Corollary

$f(x)$ is separable if and only if it is coprime to $D_x f(x)$.

Corollary

Every irreducible polynomial $f(x)$ over a field of characteristic 0 is separable.

Proof.

If f has degree $n \geq 1$, then $D_x f(x)$ has degree $n - 1$. In particular, it is not zero. The only divisors of f are 1 and $f(x)$, and by degree consideration, $f(x)$ does not divide $D_x f(x)$. □

Question to think about: where does this fail in characteristic p? We will talk more about it next time.

Theorem

A polynomial $f(x)$ has multiple root α if and only if α is a root of both $f(x)$ and $D_x f(x)$.

Theorem

A polynomial $f(x)$ has multiple root α if and only if α is a root of both $f(x)$ and $D_x f(x)$.

Proof.

Assume α is a root of $f(x)$ of multiplicity n. Then $f(x) = (x - \alpha)^n g(x)$ (in a splitting field), for some $n \geq 1$. Take derivatives, get $D_x f(x) = n(x - \alpha)^{n-1} g(x) + (x - \alpha)^n D_x g(x)$.

Theorem

A polynomial $f(x)$ has multiple root α if and only if α is a root of both $f(x)$ and $D_x f(x)$.

Proof.

Assume α is a root of $f(x)$ of multiplicity n. Then $f(x) = (x - \alpha)^n g(x)$ (in a splitting field), for some $n \geq 1$. Take derivatives, get $D_x f(x) = n(x - \alpha)^{n-1} g(x) + (x - \alpha)^n D_x g(x)$.

If $n \geq 2$, $n - 1 \geq 1$ and α is a root of $D_x f(x)$.

Theorem

A polynomial $f(x)$ has multiple root α if and only if α is a root of both $f(x)$ and $D_x f(x)$.

Proof.

Assume α is a root of $f(x)$ of multiplicity n. Then $f(x) = (x-\alpha)^n g(x)$ (in a splitting field), for some $n \geq 1$. Take derivatives, get $D_x f(x) = n(x-\alpha)^{n-1} g(x) + (x-\alpha)^n D_x g(x)$.

If $n \geq 2$, $n-1 \geq 1$ and α is a root of $D_x f(x)$.

If $n = 1$, then $D_x f(x) = g(x) + (x-\alpha)^n D_x g(x)$. Evaluating at α, we get $g(\alpha)$. By definition of multiplicity, $g(\alpha) \neq 0$, so α is not a root of $D_x f(x)$. □

Summary

- Splitting fields are unique. Proof: iterate the uniqueness of simple algebraic extensions.

Summary

- Splitting fields are unique. Proof: iterate the uniqueness of simple algebraic extensions.
- The splitting field of $x^n - 1$ is called the *cyclotomic field of nth roots of unity.* It is generated by $\zeta_n = e^{2\pi i/n}$. When n, is prime, it has degree $n - 1$. In general it has degree $\phi(n)$ (to be seen).

Summary

- Splitting fields are unique. Proof: iterate the uniqueness of simple algebraic extensions.
- The splitting field of $x^n - 1$ is called the *cyclotomic field of nth roots of unity.* It is generated by $\zeta_n = e^{2\pi i/n}$. When n, is prime, it has degree $n-1$. In general it has degree $\phi(n)$ (to be seen).
- A field is *algebraically closed* if all polynomials factor into linear terms. The complex numbers are algebraically closed.

Summary

- Splitting fields are unique. Proof: iterate the uniqueness of simple algebraic extensions.
- The splitting field of $x^n - 1$ is called the *cyclotomic field of nth roots of unity.* It is generated by $\zeta_n = e^{2\pi i/n}$. When n, is prime, it has degree $n - 1$. In general it has degree $\phi(n)$ (to be seen).
- A field is *algebraically closed* if all polynomials factor into linear terms. The complex numbers are algebraically closed.
- The *algebraic closure* is the smallest algebraically closed extension of a given field. Every field has a unique algebraic closure.

Summary

- Splitting fields are unique. Proof: iterate the uniqueness of simple algebraic extensions.
- The splitting field of $x^n - 1$ is called the *cyclotomic field of nth roots of unity.* It is generated by $\zeta_n = e^{2\pi i/n}$. When n, is prime, it has degree $n - 1$. In general it has degree $\phi(n)$ (to be seen).
- A field is *algebraically closed* if all polynomials factor into linear terms. The complex numbers are algebraically closed.
- The *algebraic closure* is the smallest algebraically closed extension of a given field. Every field has a unique algebraic closure.
- A polynomial is *separable* if it has no multiple roots, equivalently if it is coprime to its derivative. In characteristic zero, irreducible implies separable.