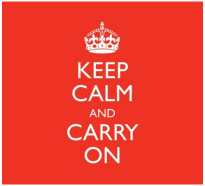
Math-123: finitely generated field extensions

Sebastien Vasey

Harvard University

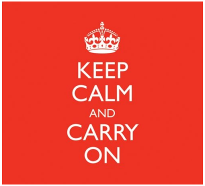
March 11, 2020

Transition to a remote class



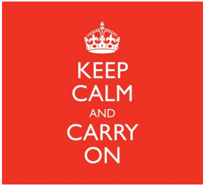
- Use the chat at any point to ask stuff or tell me your thoughts.

Transition to a remote class



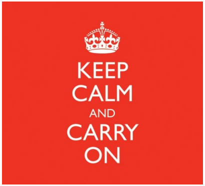
- Use the chat at any point to ask stuff or tell me your thoughts.
- The midterm is canceled.

Transition to a remote class



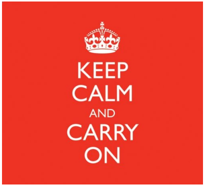
- Use the chat at any point to ask stuff or tell me your thoughts.
- The midterm is canceled.
- I updated the syllabus to describe how your grade will be computed:
  - 35 % final, 65 % assignments.
  - 2 worst assignments dropped.

Transition to a remote class



- Use the chat at any point to ask stuff or tell me your thoughts.
- The midterm is canceled.
- I updated the syllabus to describe how your grade will be computed:
  - 35 % final, 65 % assignments.
  - 2 worst assignments dropped.
- Feel free to email me or the CAs at any point. You can also use the Canvas discussion board.

Transition to a remote class



- Use the chat at any point to ask stuff or tell me your thoughts.
- The midterm is canceled.
- I updated the syllabus to describe how your grade will be computed:
  - 35 % final, 65 % assignments.
  - 2 worst assignments dropped.
- Feel free to email me or the CAs at any point. You can also use the Canvas discussion board.
- Office hours and class meeting will be held with Zoom. Regular class meetings will be recorded. These slides will be on the course webpage.

More organization

- Read ahead of class. The reading for a given week is posted on the course website by the end of the previous week.

More organization

- Read ahead of class. The reading for a given week is posted on the course website by the end of the previous week.
- If you do not have a copy of Dummit and Foote, you can read about the same topics in one of the free resources on the class website (I added a link to some good notes on field theory).

More organization

- Read ahead of class. The reading for a given week is posted on the course website by the end of the previous week.
- If you do not have a copy of Dummit and Foote, you can read about the same topics in one of the free resources on the class website (I added a link to some good notes on field theory).
- Ask yourself what the main points are. Try to summarize what you read.

More organization

- Read ahead of class. The reading for a given week is posted on the course website by the end of the previous week.
- If you do not have a copy of Dummit and Foote, you can read about the same topics in one of the free resources on the class website (I added a link to some good notes on field theory).
- Ask yourself what the main points are. Try to summarize what you read.
- The classes will not always cover proofs systematically, but focus on understanding the main points, and how it all fits together.

More organization

- Read ahead of class. The reading for a given week is posted on the course website by the end of the previous week.
- If you do not have a copy of Dummit and Foote, you can read about the same topics in one of the free resources on the class website (I added a link to some good notes on field theory).
- Ask yourself what the main points are. Try to summarize what you read.
- The classes will not always cover proofs systematically, but focus on understanding the main points, and how it all fits together.
- Use the chat to ask anything, anytime.

Fields: what we know so far

An extension K/F has a *degree*, written $[K : F]$, the dimension of K as an F-vector space. An extension is *finite* if its degree is finite.

Fields: what we know so far

An extension K/F has a *degree*, written $[K : F]$, the dimension of K as an F-vector space. An extension is *finite* if its degree is finite.

An important property of finite extensions: they are algebraic: every element α is the root of a polynomial in $F[x]$ (consider $1, \alpha, \alpha^2, \ldots$).

Fields: what we know so far

An extension K/F has a *degree*, written $[K : F]$, the dimension of K as an F-vector space. An extension is *finite* if its degree is finite.

An important property of finite extensions: they are algebraic: every element α is the root of a polynomial in $F[x]$ (consider $1, \alpha, \alpha^2, ...$).

If K/F is an extension and $\alpha \in K$, $F(\alpha)$ is called a *simple extension* of F. If α is algebraic, the degree of the extension is the degree of the minimal polynomial of α (the monic poly of min degree that α is a root of).

Fields: what we know so far

An extension K/F has a *degree*, written $[K : F]$, the dimension of K as an F-vector space. An extension is *finite* if its degree is finite.

An important property of finite extensions: they are algebraic: every element α is the root of a polynomial in $F[x]$ (consider $1, \alpha, \alpha^2, \ldots$).

If K/F is an extension and $\alpha \in K$, $F(\alpha)$ is called a *simple extension* of F. If α is algebraic, the degree of the extension is the degree of the minimal polynomial of α (the monic poly of min degree that α is a root of).

Example

Example ($K = \mathbb{C}$): $\mathbb{Q}(\sqrt[3]{2})$ has degree 3. The minimal polynomial of $\sqrt[3]{2}$ is $x^3 - 2$.

Finitely generated field extensions

We now want to analyze potentially more complicated extensions, like $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$. Such extensions (of the form $F(A)$, for A finite) are called *finitely generated*.

Finitely generated field extensions

We now want to analyze potentially more complicated extensions, like $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$. Such extensions (of the form $F(A)$, for A finite) are called *finitely generated*.

Observe that $F(\alpha, \beta) = (F(\alpha))(\beta)$ (exercise!). So *any finitely generated extension can be obtained by iterating simple extensions.*

Finitely generated field extensions

We now want to analyze potentially more complicated extensions, like $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$. Such extensions (of the form $F(A)$, for A finite) are called *finitely generated*.

Observe that $F(\alpha, \beta) = (F(\alpha))(\beta)$ (exercise!). So *any finitely generated extension can be obtained by iterating simple extensions.*

More precisely, if $K = F(\alpha_1, \ldots, \alpha_n)$, then letting $F_0 = F$, $F_{i+1} = F_i(\alpha_{i+1})$, we get a chain of extensions $F_0 \subseteq F_1 \subseteq \ldots \subseteq F_n$, where $F_i = F(\alpha_1, \ldots, \alpha_i)$. In particular, $F_n = K$.

Finitely generated field extensions

We now want to analyze potentially more complicated extensions, like $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$. Such extensions (of the form $F(A)$, for A finite) are called *finitely generated*.

Observe that $F(\alpha, \beta) = (F(\alpha))(\beta)$ (exercise!). So *any finitely generated extension can be obtained by iterating simple extensions.*

More precisely, if $K = F(\alpha_1, \ldots, \alpha_n)$, then letting $F_0 = F$, $F_{i+1} = F_i(\alpha_{i+1})$, we get a chain of extensions $F_0 \subseteq F_1 \subseteq \ldots \subseteq F_n$, where $F_i = F(\alpha_1, \ldots, \alpha_i)$. In particular, $F_n = K$.

Theorem (Multiplicativity of degrees)

If $F \subseteq K \subseteq L$ are field extensions, then $[L : F] = [K : F][L : K]$.

Consequence of multiplicativity of degrees

Thus if we have $K = F(\alpha_1, \ldots, \alpha_n)$, then letting $F_0 = F$, $F_{i+1} = F_i(\alpha_{i+1})$, and the chain of extensions $F_0 \subseteq F_1 \subseteq \ldots \subseteq F_k$ as before, we have:

$$[K : F] = [F_k : F_{k-1}][F_{k-1} : F_{k-2}] \ldots [F_1 : F_0]$$

Consequence of multiplicativity of degrees

Thus if we have $K = F(\alpha_1, \ldots, \alpha_n)$, then letting $F_0 = F$, $F_{i+1} = F_i(\alpha_{i+1})$, and the chain of extensions $F_0 \subseteq F_1 \subseteq \ldots \subseteq F_k$ as before, we have:

$$[K : F] = [F_k : F_{k-1}][F_{k-1} : F_{k-2}] \ldots [F_1 : F_0]$$

So if for each i, α_{i+1} is algebraic over F, and of degree n_i, then K/F is algebraic of degree at most $n_1 \cdot n_2 \cdot \ldots n_k$.

Consequence of multiplicativity of degrees

Thus if we have $K = F(\alpha_1, \ldots, \alpha_n)$, then letting $F_0 = F$, $F_{i+1} = F_i(\alpha_{i+1})$, and the chain of extensions $F_0 \subseteq F_1 \subseteq \ldots \subseteq F_k$ as before, we have:

$$[K : F] = [F_k : F_{k-1}][F_{k-1} : F_{k-2}] \ldots [F_1 : F_0]$$

So if for each i, α_{i+1} is algebraic over F, and of degree n_i, then K/F is algebraic of degree at most $n_1 \cdot n_2 \cdot \ldots n_k$.

Example

It could be strictly less: take $F = \mathbb{Q}$, $\alpha_1 = \sqrt{2}$, $\alpha_2 = \sqrt[6]{2}$. Then $n_1 = 2$, $n_2 = 6$, but $\mathbb{Q}(\alpha_1, \alpha_2) = \mathbb{Q}(\alpha_2)$ has degree $6 < 2 \cdot 6$.

Consequence of multiplicativity of degrees

Thus if we have $K = F(\alpha_1, \ldots, \alpha_n)$, then letting $F_0 = F$, $F_{i+1} = F_i(\alpha_{i+1})$, and the chain of extensions $F_0 \subseteq F_1 \subseteq \ldots \subseteq F_k$ as before, we have:

$$[K : F] = [F_k : F_{k-1}][F_{k-1} : F_{k-2}] \ldots [F_1 : F_0]$$

So if for each i, α_{i+1} is algebraic over F, and of degree n_i, then K/F is algebraic of degree at most $n_1 \cdot n_2 \cdot \ldots n_k$.

Example

It could be strictly less: take $F = \mathbb{Q}$, $\alpha_1 = \sqrt{2}$, $\alpha_2 = \sqrt[6]{2}$. Then $n_1 = 2$, $n_2 = 6$, but $\mathbb{Q}(\alpha_1, \alpha_2) = \mathbb{Q}(\alpha_2)$ has degree $6 < 2 \cdot 6$.

We saw last time we can also deduce that $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}(\sqrt{2})] = 3$ (to do this directly, we would have to show $\sqrt[6]{2} \notin \mathbb{Q}(\sqrt{2})$, which is annoying).

Some important conclusions

Let K/F be an extension.

- (Characterization of finite extensions) K/F is finite if and only if K is generated by finitely-many algebraic elements.

Some important conclusions

Let K/F be an extension.

- (Characterization of finite extensions) K/F is finite if and only if K is generated by finitely-many algebraic elements. *[Why? $\Rightarrow$: We saw before that finite implies algebraic, so take a basis. $\Leftarrow$: if $K = F(\alpha_1, \ldots, \alpha_k)$ and each α_i is algebraic of degree n_i, K/F has degree at most $n_1 \ldots n_k$, which is finite]*

Some important conclusions

Let K/F be an extension.

- (Characterization of finite extensions) K/F is finite if and only if K is generated by finitely-many algebraic elements. *[Why? $\Rightarrow$: We saw before that finite implies algebraic, so take a basis. $\Leftarrow$: if $K = F(\alpha_1, \ldots, \alpha_k)$ and each α_i is algebraic of degree n_i, K/F has degree at most $n_1 \ldots n_k$, which is finite]*
- (Algebraic numbers form a field) If $\alpha, \beta \in K$ are algebraic over F, then $\alpha + \beta$, $\alpha \cdot \beta$, $-\alpha$, and α^{-1} ($\alpha \neq 0$) are all algebraic over F.

Some important conclusions

Let K/F be an extension.

- (Characterization of finite extensions) K/F is finite if and only if K is generated by finitely-many algebraic elements. *[Why? $\Rightarrow$: We saw before that finite implies algebraic, so take a basis. $\Leftarrow$: if $K = F(\alpha_1, \ldots, \alpha_k)$ and each α_i is algebraic of degree n_i, K/F has degree at most $n_1 \ldots n_k$, which is finite]*
- (Algebraic numbers form a field) If $\alpha, \beta \in K$ are algebraic over F, then $\alpha + \beta$, $\alpha \cdot \beta$, $-\alpha$, and α^{-1} ($\alpha \neq 0$) are all algebraic over F.
  [Why? because all these numbers are in $F(\alpha, \beta)$, which is finite by the previous part, hence algebraic.]

Some important conclusions

Let K/F be an extension.

- (Characterization of finite extensions) K/F is finite if and only if K is generated by finitely-many algebraic elements.
  [Why? $\Rightarrow$: We saw before that finite implies algebraic, so take a basis. $\Leftarrow$: if $K = F(\alpha_1, \dots, \alpha_k)$ and each α_i is algebraic of degree n_i, K/F has degree at most $n_1 \dots n_k$, which is finite]
- (Algebraic numbers form a field) If $\alpha, \beta \in K$ are algebraic over F, then $\alpha + \beta$, $\alpha \cdot \beta$, $-\alpha$, and α^{-1} ($\alpha \neq 0$) are all algebraic over F.
  [Why? because all these numbers are in $F(\alpha, \beta)$, which is finite by the previous part, hence algebraic.]
- (Transitivity of being algebraic) If K is algebraic over F and L is algebraic over K, then L is algebraic over F.

(Transitivity of being algebraic) If K is algebraic over F and L is algebraic over K, then L is algebraic over F.

(Transitivity of being algebraic) If K is algebraic over F and L is algebraic over K, then L is algebraic over F.

[Why? Let $\alpha \in L$. Since α is algebraic over K, α is the root of a polynomial $a_0 + a_1 x + \ldots + a_n x^n$, with each $a_i \in K$. Since K is algebraic over F, each a_i is algebraic over F. Thus the extension $F(a_0, \ldots, a_n)/F$ is finite. The extension $F(a_0, \ldots, a_n)(\alpha)/F(a_0, \ldots, a_n)$ is also finite. Thus $F(a_0, \ldots, a_n, \alpha)$ is finite, so α is algebraic over F.]

Example

Let $F = \mathbb{Q}$, $K = \mathbb{C}$. Let $\bar{\mathbb{Q}}$ denote *all* algebraic complex numbers (over $\mathbb{Q}$). What is $[\bar{\mathbb{Q}} : \mathbb{Q}]$?

Example

Let $F = \mathbb{Q}$, $K = \mathbb{C}$. Let $\bar{\mathbb{Q}}$ denote *all* algebraic complex numbers (over $\mathbb{Q}$). What is $[\bar{\mathbb{Q}} : \mathbb{Q}]$?

Well, for each n, $\sqrt[n]{2}$ is algebraic, and its minimal polynomial is $x^n - 2$ (it is irreducible by Eisenstein).

Example

Let $F = \mathbb{Q}$, $K = \mathbb{C}$. Let $\bar{\mathbb{Q}}$ denote *all* algebraic complex numbers (over $\mathbb{Q}$). What is $[\bar{\mathbb{Q}} : \mathbb{Q}]$?

Well, for each n, $\sqrt[n]{2}$ is algebraic, and its minimal polynomial is $x^n - 2$ (it is irreducible by Eisenstein).

Thus $[\bar{\mathbb{Q}} : \mathbb{Q}] \geq [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$, for each n, so $\bar{\mathbb{Q}}/\mathbb{Q}$ is an infinite extension.

Example

Let $F = \mathbb{Q}$, $K = \mathbb{C}$. Let $\bar{\mathbb{Q}}$ denote *all* algebraic complex numbers (over $\mathbb{Q}$). What is $[\bar{\mathbb{Q}} : \mathbb{Q}]$?

Well, for each n, $\sqrt[n]{2}$ is algebraic, and its minimal polynomial is $x^n - 2$ (it is irreducible by Eisenstein).

Thus $[\bar{\mathbb{Q}} : \mathbb{Q}] \geq [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$, for each n, so $\bar{\mathbb{Q}}/\mathbb{Q}$ is an infinite extension.

However it is algebraic! So finite implies algebraic, but not conversely! We need to assume finitely generated to get the converse.

Example

Let $F = \mathbb{Q}$, $K = \mathbb{C}$. Let $\bar{\mathbb{Q}}$ denote *all* algebraic complex numbers (over $\mathbb{Q}$). What is $[\bar{\mathbb{Q}} : \mathbb{Q}]$?

Well, for each n, $\sqrt[n]{2}$ is algebraic, and its minimal polynomial is $x^n - 2$ (it is irreducible by Eisenstein).

Thus $[\bar{\mathbb{Q}} : \mathbb{Q}] \geq [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$, for each n, so $\bar{\mathbb{Q}}/\mathbb{Q}$ is an infinite extension.

However it is algebraic! So finite implies algebraic, but not conversely! We need to assume finitely generated to get the converse.

A fun exercise: prove that $\bar{\mathbb{Q}}$ is countable (*hint: see the book*).

Example

Let $F = \mathbb{Q}$, $K = \mathbb{C}$. Let $\bar{\mathbb{Q}}$ denote *all* algebraic complex numbers (over $\mathbb{Q}$). What is $[\bar{\mathbb{Q}} : \mathbb{Q}]$?

Well, for each n, $\sqrt[n]{2}$ is algebraic, and its minimal polynomial is $x^n - 2$ (it is irreducible by Eisenstein).

Thus $[\bar{\mathbb{Q}} : \mathbb{Q}] \geq [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$, for each n, so $\bar{\mathbb{Q}}/\mathbb{Q}$ is an infinite extension.

However it is algebraic! So finite implies algebraic, but not conversely! We need to assume finitely generated to get the converse.

A fun exercise: prove that $\bar{\mathbb{Q}}$ is countable (*hint: see the book*).

Since $\mathbb{C}$ (or $\mathbb{R}$) are uncountable, this shows there are transcendental elements. However proving specific elements (like e or π) are transcendental is much harder.

Composite fields

How do we "put two fields together"?

Definition

For K_1, K_2 subfields of K, let K_1K_2, the *composite field of* K_1 *and* K_2, be the smallest subfield of K containing K_1 and K_2.

Composite fields

How do we "put two fields together"?

Definition

For K_1, K_2 subfields of K, let $K_1 K_2$, the *composite field of* K_1 *and* K_2, be the smallest subfield of K containing K_1 and K_2.

Example

$\mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2})$. Why is the last equality true?

Composite fields

How do we "put two fields together"?

Definition

For K_1, K_2 subfields of K, let $K_1 K_2$, the *composite field of* K_1 *and* K_2, be the smallest subfield of K containing K_1 and K_2.

Example

$\mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2})$. Why is the last equality true?

- $\subseteq$: $\sqrt{2} \in \mathbb{Q}(\sqrt[6]{2})$ as $\sqrt{2} = \sqrt[6]{2}^3$. Similarly, $\sqrt[3]{2} \in \mathbb{Q}(\sqrt[6]{2})$.
- $\supseteq$: $\sqrt[6]{2} = 2^{\frac{1}{6}} = 2^{\frac{1}{2}-\frac{1}{3}} = \frac{\sqrt{2}}{\sqrt[3]{2}} \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$.

Degree of composite extensions

Observe that if K_1, K_2 are finite extensions of F with bases $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_m$, then $K_1K_2 = F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$.

Degree of composite extensions

Observe that if K_1, K_2 are finite extensions of F with bases $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_m$, then $K_1 K_2 = F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$.

This means that $K_1 K_2$ is generated by product and sums of α_i and β_j's.

Degree of composite extensions

Observe that if K_1, K_2 are finite extensions of F with bases $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_m$, then $K_1K_2 = F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$.

This means that K_1K_2 is generated by product and sums of α_i and β_j's.

Product of α_i's (like α_1^2) are F-linear combinations of α_i's (as the α_i form a basis). Similarly for product of β_j's.

Degree of composite extensions

Observe that if K_1, K_2 are finite extensions of F with bases $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_m$, then $K_1 K_2 = F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$.

This means that $K_1 K_2$ is generated by product and sums of α_i and β_j's.

Product of α_i's (like α_1^2) are F-linear combinations of α_i's (as the α_i form a basis). Similarly for product of β_j's.

This implies that $(\alpha_i \beta_j)_{i=1\ldots n, j=1\ldots m}$ spans $K_1 K_2$, so $[K_1 K_2 : F] \leq nm = [K_1 : F][K_2 : F]$.

Degree of composite extensions: picture

If $[K_1 : F] = n$, $[K_2 : F] = m$, then $[K_1K_2 : F] \leq nm$.

$$
\begin{tikzcd}
& K_1K_2 \arrow[dl, dash, "\leq m"'] \arrow[dr, dash, "\leq n"'] & \\
K_1 \arrow[dr, dash, "n"'] & & K_2 \arrow[dl, dash, "m"'] \\
& F &
\end{tikzcd}
$$

Degree of composite extensions: picture

If $[K_1 : F] = n$, $[K_2 : F] = m$, then $[K_1K_2 : F] \leq nm$.

$$\begin{tikzcd}
& K_1K_2 & \\
K_1 \arrow[ur, dash, "\leq m"] & & K_2 \arrow[ul, dash, "\leq n"'] \\
& F \arrow[ul, dash, "n"] \arrow[ur, dash, "m"'] &
\end{tikzcd}$$

Note that if $\gcd(n, m) = 1$, then equality holds! $[K_1K_2 : F] = nm$.
We can use this to get another proof that $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] = 6$.

Summary

- Finite extensions are exactly the iterations of simple extensions by algebraic elements.

Summary

- Finite extensions are exactly the iterations of simple extensions by algebraic elements.
- Thus finite is equivalent to "generated by finitely-many algebraic elements".

Summary

- Finite extensions are exactly the iterations of simple extensions by algebraic elements.
- Thus finite is equivalent to “generated by finitely-many algebraic elements”.
- It follows that algebraic elements form a field, and that the iterations of two algebraic extensions is algebraic.

Summary

- Finite extensions are exactly the iterations of simple extensions by algebraic elements.
- Thus finite is equivalent to “generated by finitely-many algebraic elements”.
- It follows that algebraic elements form a field, and that the iterations of two algebraic extensions is algebraic.
- We can either think of $F(\alpha, \beta)$ as $(F(\alpha))(\beta)$, or as the composite of the extensions $F(\alpha)$ and $F(\beta)$. If the degrees of these are n and m, we get that the degree of the composite is $\leq nm$, and equality holds if n and m are coprime.