Math 5111 (Algebra 1)

Lecture #6 $\sim$ September 28, 2020

Algebraic Extensions

- Algebraic Extensions
- Extension Degrees and Towers
- Examples of Extensions

This material represents §2.2.4-2.2.5 from the course notes.

Algebraic Extensions, I

Now that we have described simple extensions, we can expand our focus to other field extensions. A natural class of extensions are those in which every element is algebraic:

Definition

The field extension K/F is algebraic if every $\alpha \in K$ is algebraic over F: in other words, if every α is a root of a nonzero polynomial in $F[x]$.

Our goal for today is to study algebraic extensions. It turns out that we will able to "bootstrap" quite a lot of results from some comparatively easy observations, as you will see.

Algebraic Extensions, II

We start with the simplest possible case (pun intended): namely, the situation of a simple extension:

Proposition (Simple Algebraic Extensions)

A simple extension $F(\alpha)/F$ is algebraic if and only if it has finite degree. Furthermore, if $[F(\alpha) : F] = n$, then every element in $F(\alpha)$ satisfies a nonzero polynomial of degree at most n in $F[x]$.

The point here is just to use the structure of simple extensions that we identified last time.

Algebraic Extensions, III

Proof:

- If $F(\alpha)$ is algebraic then $\alpha \in F(\alpha)$ is algebraic over F. If the minimal polynomial for α has degree n, then as we showed earlier, $[F(\alpha) : F] = n$, so the extension has finite degree.
- Conversely, suppose $F(\alpha)/F$ has degree n and let $\beta \in F(\alpha)$. Observe the set $\{1, \beta, \beta^2, \dots, \beta^n\}$ has $n+1$ elements, so since $F(\alpha)$ only has dimension n over F, it must be linearly dependent.
- In other words, there exist $c_i \in F$, not all zero, with $c_0 + c_1\beta + \cdots + c_n\beta^n = 0$: thus, β is the root of a nonzero polynomial in $F[x]$, so β is algebraic over F. The second statement is also immediate.

Algebraic Extensions, IV

As an immediate but very useful corollary, we see that finite-degree extensions are algebraic:

Corollary

Finite-degree extensions are algebraic.

Proof:

- By the previous proposition, any element of a degree-n extension satisfies a polynomial of degree at most n, and is therefore algebraic.

We will remark that there exist algebraic extensions of infinite degree, so the converse of this result is not true.

Algebraic Extensions, V

Next we analyze extensions with a finite number of generators: $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ for some $\alpha_i \in K$.

- If any of the α_i are transcendental over F, then clearly K is non-algebraic since it contains a transcendental element.
- On the other hand, if all of the α_i are algebraic over F, it seems reasonable to hypothesize that K itself will also be algebraic over F, since every element of K is a combination of algebraic elements.
- The key idea is to observe that we can obtain K as a "tower" of simple extensions by adjoining the α_i one at a time.

Algebraic Extensions, VI

To illustrate, suppose $K = F(\alpha, \beta, \gamma)$.

- Then K contains $F(\alpha)$ along with β, and so it contains the extension field $F(\alpha)(\beta)$.
- But $F(\alpha, \beta)$ is by definition the smallest subfield of K containing α and β, so $F(\alpha, \beta)$ is contained in $F(\alpha)(\beta)$.
- On the other hand, since $F(\alpha, \beta)$ contains $F(\alpha)$ and β, since $F(\alpha)(\beta)$ is the smallest subfield of K containing $F(\alpha)$ and β, we see that $F(\alpha)(\beta)$ is contained in $F(\alpha, \beta)$.
- Thus, $F(\alpha, \beta) = F(\alpha)(\beta)$, so $F(\alpha, \beta)/F(\alpha)$ is a simple extension.

Algebraic Extensions, VI

We continue to suppose $K = F(\alpha, \beta, \gamma)$.

- We just observed that $F(\alpha, \beta)/F(\alpha)$ is a simple extension generated by β.
- In the same way, we can see that $K = F(\alpha, \beta, \gamma)/F(\alpha, \beta)$ is also a simple extension.
- Thus, we can obtain K from F using a chain of 3 simple extensions $F(\alpha, \beta, \gamma)/F(\alpha, \beta)/F(\alpha)/F$.
- In order to show that the resulting field K will be algebraic if each α_i is algebraic, we need to know how extension degrees behave in these towers of field extensions.

Algebraic Extensions, VII

Theorem (Degrees in Towers)

If L/K and K/F are both field extensions, then so is L/F, and $[L:F] = [L:K] \cdot [K:F]$ (where if one side is infinite, then so is the other). In particular, $[K:F]$ divides $[L:F]$.

Although we will not need it, in fact a more general statement is true: if V is a K-vector space and K/F is a field extension, then (under the same operations) V is also an F-vector space, and $\dim_F V = [K:F] \cdot \dim_K V$.

The theorem is the special case where V is the K-vector space L.

Algebraic Extensions, VIII

Proof:

- First suppose that $[K : F] = n$ with basis $\{a_1, a_2, \dots, a_n\}$ and $[L : K] = m$ with basis $\{v_1, v_2, \dots, v_m\}$ are both finite.
- We claim that the set β of the mn pairwise products $a_i v_j$ for $1 \leq i \leq n$ and $1 \leq j \leq m$ is a basis for L/F.
- First, we observe that no two of these pairwise products are equal, so this set actually does have mn elements.
- To see this, suppose $a_i v_j = a_k v_l$ so that $a_i v_j - a_k v_l = 0$. If $j \neq l$ then v_j, v_l would be K-linearly dependent (contrary to our assumption), and if $j = l$ then cancelling v_j (which is nonzero since it is a basis element) would yield $a_i = a_k$.

Algebraic Extensions, IX

<u>Proof</u> (continued):

- To see that β is a spanning set, for any $w \in L$ by the hypothesis that $\{v_1, v_2, \dots, v_m\}$ spans L/K, we may write $w = b_1 v_1 + \cdots + b_m v_m$ for some $b_i \in K$. Furthermore, since the $b_i \in K$, by the hypothesis that $\{a_1, a_2, \dots, a_n\}$ spans K/F, we may write $b_i = c_{i,1} a_1 + \cdots + c_{i,n} a_n$ for some $c_{i,j} \in F$.
- Now substituting in the expressions for the b_i in terms of the $c_{i,j}$ and the a_i to the expression for w yields

$$\begin{aligned} w &= b_1 v_1 + \cdots + b_m v_m \\ &= (c_{1,1} a_1 + \cdots + c_{1,n} a_n) v_1 + \cdots + (c_{m,1} a_1 + \cdots + c_{m,n} a_n) v_m \\ &= c_{1,1} a_1 v_1 + \cdots + c_{m,n} a_n v_m \end{aligned}$$

  and therefore w is an F-linear combination of the elements of β, meaning that β is a spanning set.

Algebraic Extensions, X (Marks The Spot)

Proof (continued more):

- To see that β is linearly independent, suppose we had a linear combination $c_{1,1}a_1v_1 + \cdots + c_{m,n}a_nv_m = 0$ for some $c_{i,j} \in F$.
- By the previous slide's calculation (in reverse) if we set $b_i = c_{i,1}a_1 + \cdots + c_{i,n}a_n$ then $b_i \in K$ for each i and $b_1v_1 + \cdots + b_mv_m = 0$. Since the v_i are linearly independent over K, this means $b_i = 0$ for each i.
- Then since $b_i = c_{i,1}a_1 + \cdots + c_{i,n}a_n$ and the a_i are linearly independent over F, we conclude that $c_{i,j} = 0$ for each i, j, and so β is also linearly independent, hence a basis.
- This establishes the case where $[L : K]$ and $[K : F]$ are finite.

Algebraic Extensions, XI

Proof (continued still more):

- For the infinite-degree cases, if $[K : F] = \infty$ then any basis of K/F is an infinite linearly-independent subset of L/F, meaning that $[L : F] = \infty$ as well.
- Likewise, if $[L : K] = \infty$, then any basis of L/K is an infinite K-linearly independent subset, which is also clearly F-linearly independent (since any linear dependence over F would also hold over K), and so $[L : F] = \infty$ again.
- Finally, if $[L : F] = \infty$, then at least one of $[L : K]$ and $[K : F]$ must be infinite, since if both are finite then our proof above shows that $[L : F]$ is also finite.

Algebraic Extensions, XII

We can apply this result to establish that an extension generated by finitely many elements is algebraic precisely when all of the generators are algebraic, and also bound the resulting extension's degree:

Corollary (Finite Algebraic Extensions)

If K/F is a field extension with $K = F(\alpha_1, \alpha_2, \dots, \alpha_n)$, then K/F is algebraic if and only if each of the α_i are algebraic over F. In this case, $[K : F] \leq \prod_{i=1}^{n} [F(\alpha_i) : F]$, and every element of K is a polynomial (with coefficients from F) in the α_i.

In particular, this result says $F(\alpha_1, \alpha_2, \dots, \alpha_n) = F[\alpha_1, \alpha_2, \dots, \alpha_n]$ when the α_i are algebraic over F.

Algebraic Extensions, XIII: Triskaidekaphilia

Proof:

- If any of the α_i are transcendental over F then K is not algebraic over F.
- So now suppose each of the α_i are algebraic.
- As noted earlier, we may obtain K as a chain of simple extensions $K/F(\alpha_1, \dots, \alpha_{n-1})/\cdots/F(\alpha_1, \alpha_2)/F(\alpha_1)/F$.
- By hypothesis, for each $1 \leq i \leq n$, α_i is algebraic over F, so α_i is also algebraic over $F(\alpha_1, \dots, \alpha_{i-1})$, since the minimal polynomial for α_i over F may also be thought of as a polynomial over $F(\alpha_1, \dots, \alpha_{i-1})$.

Algebraic Extensions, XIV

Proof (continued):

- Therefore, since a simple extension is algebraic if and only if it has finite degree, we see that $[F(\alpha_1, \dots, \alpha_i) : F(\alpha_1, \dots, \alpha_{i-1})]$ is finite for each i.
- Then by the multiplicativity of extension degrees (and a trivial induction), we conclude that $[K : F] = \prod_{i=1}^{n} [F(\alpha_1, \dots, \alpha_i) : F(\alpha_1, \dots, \alpha_{i-1})]$ is finite. Since finite-degree extensions are algebraic, this means K/F is algebraic as claimed.

Algebraic Extensions, XV

Proof (continued more):

- For the second statement, consider the minimal polynomial $m(x)$ of α_i over F and the minimal polynomial $m'(x)$ of α_i over $F(\alpha_1, \dots, \alpha_{i-1})$.
- Since $m(x)$ is also a polynomial in $F(\alpha_1, \dots, \alpha_{i-1})$ having α_i as a root, by properties of minimal polynomials we see that $m'(x)$ divides $m(x)$, so $\deg m' \leq \deg m$.
- Converting to a statement about extension degrees yields $[F(\alpha_1, \dots, \alpha_i) : F(\alpha_1, \dots, \alpha_{i-1})] \leq [F(\alpha_i) : F]$, and then taking the product from $i = 1$ to n yields $[K : F] \leq \prod_{i=1}^{n} [F(\alpha_i) : F]$.

Algebraic Extensions, XVI

Proof (continued yet more):

- For the last statement, since $E[\beta] = E(\beta)$ when β is algebraic over E, by an easy induction we see that every element of K is a polynomial in the α_i.

Remark: More explicitly, every element of K is an F-linear combination of elements of the form $\alpha_1^{c_1}\alpha_2^{c_2}\cdots\alpha_n^{c_n}$, where each c_i is an integer with $0 \le c_i \le [F(\alpha_i) : F]$.

- This also follows by a straightforward induction, using the fact that every element of $E(\beta)$ is of the form $b_0 + b_1\beta + \cdots + b_{d-1}\beta^{d-1}$ where $[E(\beta) : E] = d$, as both the base case and inductive step.

Algebraic Extensions, XVII

We can also show that every finite-degree extension is generated by a finite set of algebraic elements, and that an algebraic extension of an algebraic extension is also algebraic:

Corollary (Characterization of Finite Extensions)

If K/F is a field extension, then K/F has finite degree if and only if $K = F(\alpha_1, \dots, \alpha_n)$ for some elements $\alpha_1, \dots, \alpha_n \in K$ that are algebraic over F.

The point here is that this is a very easy condition to check if we are given a set of generators for K/F, and inversely tells us we can always find a finite set of generators for a finite-degree extension.

Algebraic Extensions, XVIII

Proof:

- We already showed that $F(\alpha_1, \ldots, \alpha_n)/F$ is finite if $\alpha_1, \ldots, \alpha_n$ are algebraic over F, which is the reverse direction.
- For the forward direction, suppose K/F has finite degree: then by definition, K has a finite basis $\{\alpha_1, \ldots, \alpha_n\}$ as an F-vector space, and so $K = F(\alpha_1, \ldots, \alpha_n)$.
- Furthermore, since $F(\alpha_i)$ is a subfield of the finite-degree extension K/F, we see that $[F(\alpha_i) : F]$ is also finite (by the multiplicativity of extension degrees): thus α_i is algebraic over F for each i, as required.

Algebraic Extensions, XIX

We also see that an algebraic extension of an algebraic extension is algebraic:

Corollary (Towers of Algebraic Extensions)

If L/K is an algebraic extension, and K/F is an algebraic extension, then L/F is an algebraic extension.

These results are obvious if the extensions have finite degree: the content is when one of the extensions has infinite degree (but is still algebraic).

Algebraic Extensions, XX: Dos Equis

Proof:

- Let $\alpha \in L$: then since α is algebraic over K it is the root of some polynomial $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ with the $a_i \in K$.
- Since K/F is also algebraic, each of the a_i are algebraic over F, and so the extension $E = F(a_0, a_1, \dots, a_n)$ has finite degree over F.
- Furthermore, $E(\alpha)/E$ also has finite degree, because α is the root of a nonzero polynomial in $E[x]$.
- Thus, since $E(\alpha)/E$ and E/F both have finite degree, so does $E(\alpha)/F$: this means α satisfies a polynomial of finite degree over F, so α is algebraic over F.
- This holds for all $\alpha \in L$, so L is algebraic over F.

Algebraic Extensions, XXI

We can also extend these results on degree to general "composite fields":

Definition

If K_1 and K_2 are subfields of K, the composite field K_1K_2 is the intersection of all subfields of K containing both K_1 and K_2.

- We can also consider composites of an arbitrary collection of subfields (namely, the intersection of all subfields containing every field in the collection), although we generally will not need to bother much with infinite composites.
- Like with subfields generated by a set, it is easy to see that the composite field is the smallest subfield of K that contains both K_1 and K_2, and is also equal to $K_1(K_2)$ and $K_2(K_1)$.

Algebraic Extensions, XXII

We can say some things about the extension degree of a composite extension:

Proposition (Degrees of Composites)

If K_1/F and K_2/F are both finite-degree subextensions of K/F, then $\mathrm{lcm}([K_1 : F], [K_2 : F]) \leq [K_1K_2 : F] \leq [K_1 : F] \cdot [K_2 : F]$. In particular, if the degrees $[K_1 : F]$ and $[K_2 : F]$ are relatively prime, then equality always holds.

Algebraic Extensions, XXIII

Proof:

- For the upper bound, suppose K_1/F has basis $\alpha_1, \dots, \alpha_n$ and K_2/F has basis $\beta_1, \dots, \beta_m$.
- Then K_1K_2 contains F and each of $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m$ hence it contains $F(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)$.
- On the other hand, $F(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)$ contains both K_1 and K_2, hence also K_1K_2.
- So, $K_1K_2 = F(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m) = K_1(\beta_1, \dots, \beta_m)$.
- Thus, $\beta_1, \dots, \beta_m$ span K_1K_2/K_1, so $[K_1K_2 : K_1] \le [K_2 : F]$.
- Then $[K_1K_2 : F] = [K_1K_2 : K_1] \cdot [K_1 : F] \le [K_1 : F] \cdot [K_2 : F]$ as claimed.

Algebraic Extensions, XXIV

Proof (continued):

- For the lower bound and the second statement, note that $[K_1K_2 : F]$ must be divisible by both $[K_1 : F]$ and $[K_2 : F]$, since we have the towers $K_1K_2/K_1/F$ and $K_1K_2/K_2/F$.
- Therefore, $[K_1K_2 : F]$ is divisible by $\mathrm{lcm}([K_1 : F], [K_2 : F])$, hence is greater than or equal to it.
- If m and n are relatively prime, the lcm is simply the product, so the upper and lower bounds are the same, meaning that we get equality.

Examples of Extensions, I

By using our results on simple and composite extensions, along with the multiplicativity of field degrees in towers, we can often say a great deal about extensions of small degree.

- The goal here is to show how much we can now say about a number of different examples, using the various results we have developed so far, along with a few additional tricks.

Examples of Extensions, II

First, as an ur-example, we can characterize quadratic extensions:

Proposition (Quadratic Extensions)

Suppose F is a field of characteristic not equal to 2 and K/F is a quadratic extension (i.e., degree 2). Then $K = F(\alpha)$ for any $\alpha \in K$ not in F, and in fact we can take $K = F(\beta)$ for some element with $\beta^2 \in F$ and $\beta \notin F$.

- The last statement says (essentially) that $K = F(\sqrt{D})$ for some $D \in F$ that is not a square in F. (It is hard to be more precise than this, because it is difficult to define what "$\sqrt{D}$" means without ultimately being circular!)
- In particular, the quadratic extensions of $\mathbb{Q}$ (inside $\mathbb{C}$) are precisely the extensions $\mathbb{Q}(\sqrt{D})$ that we have previously described.

Examples of Extensions, III

Proof:

- Suppose K/F is a quadratic extension.
- If $\alpha \in K$ is not in F, then the set $\{1, \alpha\}$ is F-linearly independent, and since $[K : F] = 2$ it must therefore be a basis for K.
- Thus, $K = F(\alpha)$.

Examples of Extensions, IV

Proof (continued):

- For the second statement, consider the minimal polynomial for any $\alpha \in K$ not in F.
- Since $K = F(\alpha)$ and $[K : F] = 2$ we see that the minimal polynomial for α has degree 2: say, $x^2 + bx + c$.
- Then $\alpha^2 + b\alpha + c = 0$, so completing the square (here is where we require the characteristic not to be equal to 2, since we must divide by 2 to do this) and setting $\beta = \alpha + b/2$ yields $(\alpha + b/2)^2 + (c - b^2/4) = 0$.
- Setting $\beta = \alpha + b/2$ shows that $\beta^2 = (b^2 - 4c)/4 \in F$.
- Furthermore, β is not in F since otherwise this would imply that $\alpha = \beta - b/2$ was in F.
- Thus, $K = F(\beta)$ for some β with $\beta^2 \in F$ and $\beta \notin F$, as claimed.

Examples of Extensions, V

Example: Determine the degree of $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$.

- The field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a finite algebraic extension of $\mathbb{Q}$, and since $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ we see that the extension degree is at least 2 and at most 4.
- In particular, by the remark following the corollary on finite algebraic extensions, we see that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}[\sqrt{2}, \sqrt{3}] = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \ : \ a, b, c, d \in \mathbb{Q}\}$, which establishes that the latter ring is in fact a field. (Notice how much simpler this argument is than the explicit calculations we performed earlier!)

Examples of Extensions, V

Example: Determine the degree of $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$.

- In fact, since $\mathbb{Q}(\sqrt{2})$ is a subfield of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, the extension degree $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$ must in fact be divisible by 2, so it is either 2 or 4.
- To determine which of these cases holds we need to compute $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})]$, which is either 1 or 2 since $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$.
- If $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 1$, then the degree of the minimal polynomial of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$ is 1, which is to say, $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$.
- But this is not true: if $\sqrt{3} = a + b\sqrt{2}$ for $a, b \in \mathbb{Q}$ then squaring yields $3 = (a^2 + 2b^2) + 2ab\sqrt{2}$, so since $\sqrt{2}$ is irrational, one of a, b would be zero (otherwise we could write $\sqrt{2} = (3 - a^2 - 2b^2)/(2ab)$). However, we cannot have $a = \sqrt{3}$ or $b\sqrt{2} = \sqrt{3}$ because $\sqrt{3}$ and $\sqrt{6}$ are also irrational.

Examples of Extensions, VI

Example: Determine the degree of $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$.

- Therefore, we must have $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.
- This implies some other things: for example, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$, and in turn this means that the minimal polynomial for $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$ must have degree 2.
- Since $\sqrt{3}$ is a root of $x^2 - 3$, that means the polynomial $x^2 - 3$ is irreducible in $\mathbb{Q}(\sqrt{2})$.
- Furthermore, since $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a spanning set for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, the fact that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ tells us that this set is a basis (and thus linearly independent), which is also not so easy to prove directly.

Examples of Extensions, VII

Example: Determine the degree of $L = \mathbb{Q}(\sqrt{3}, \sqrt[3]{3})$ over $\mathbb{Q}$.

- If we let $K_1 = \mathbb{Q}(\sqrt[3]{3})$ and $K_2 = \mathbb{Q}(\sqrt{3})$, then $L = K_1 K_2$.
- Furthermore, $[K_1 : \mathbb{Q}] = 3$ and $[K_2 : \mathbb{Q}] = 2$ since K_1 is generated by a root of the irreducible polynomial $x^3 - 3$ and K_2 is generated by a root of the irreducible polynomial $x^2 - 3$.
- Then from our result on the degree of a composite extension, we know that $[L : \mathbb{Q}] \leq [K_1 : \mathbb{Q}] \cdot [K_2 : \mathbb{Q}] = 6$.
- Furthermore, since K_1 and K_2 are both subfields of L, we see that $[L : \mathbb{Q}]$ is divisible by both $[K_1 : \mathbb{Q}] = 2$ and $[K_2 : \mathbb{Q}] = 3$, and hence by 6.
- Therefore, since $[L : \mathbb{Q}] \leq 6$, the only possibility is to have $[L : \mathbb{Q}] = 6$.

Examples of Extensions, VIII

Example: Determine the degree of $L = \mathbb{Q}(\sqrt{3}, \sqrt[3]{3})$ over $\mathbb{Q}$.

- Another approach is to observe that L contains the element $\alpha = \sqrt{3}/\sqrt[3]{3} = 3^{1/6}$.
- But since $\sqrt{3} = \alpha^3$ and $\sqrt[3]{3} = \alpha^2$ we conclude that $L = \mathbb{Q}(\alpha)$.
- Then since α is a root of the (Eisenstein) irreducible polynomial $x^6 - 3$, we see that $L = \mathbb{Q}(\alpha)$ has degree 6 over $\mathbb{Q}$.
- Indeed, we even get a basis, namely $\{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5\}$.

Examples of Extensions, IX

Example: Determine the degree of $L = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}\sqrt[3]{2})$ over $\mathbb{Q}$.

- If we let $K_1 = \mathbb{Q}(\sqrt[3]{2})$ and $K_2 = \mathbb{Q}(e^{2\pi i/3}\sqrt[3]{2})$, then $L = K_1 K_2$.
- Furthermore, from our earlier discussion of these fields, we know that $[K_1 : \mathbb{Q}] = [K_2 : \mathbb{Q}] = 3$, since both fields are generated by an element whose minimal polynomial over $\mathbb{Q}$ is $x^3 - 2$.
- Then $[L : \mathbb{Q}] = [L : K] \cdot [K : \mathbb{Q}]$ so $[L : \mathbb{Q}]$ is divisible by 3, and we also know that $[L : \mathbb{Q}] \leq [K_1 : \mathbb{Q}] \cdot [K_2 : \mathbb{Q}] = 9$.
- We might expect $[L : \mathbb{Q}]$ to be 9, but in fact, it is not!

Examples of Extensions, X

Example: Determine the degree of $L = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}\sqrt[3]{2})$ over $\mathbb{Q}$.

- To see why not, observe that L also contains the element $\zeta = e^{2\pi i/3} = (-1 + i\sqrt{3})/2$, and one can verify that $\zeta^2 + \zeta + 1 = 0$.
- Thus, ζ is a root of the polynomial $x^2 + x + 1$, which is irreducible over $\mathbb{Q}$, and so for $K_3 = \mathbb{Q}(\zeta)$ we have $[K_3 : \mathbb{Q}] = 2$.
- Since $\mathbb{Q}(\zeta)$ is also a subfield of L, we see that $[L : \mathbb{Q}]$ is divisible by 2. Since it is also divisible by 3 and ≤ 9, the only possibility is for $[L : \mathbb{Q}] = 6$.

Examples of Extensions, XI

Example: Determine the degree of $L = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}\sqrt[3]{2})$ over $\mathbb{Q}$.

- In fact, it is not hard to see that $L = \mathbb{Q}(\sqrt[3]{2}, \zeta) = K_1 K_3$.
- Specifically, the point is that the field $\mathbb{Q}(\sqrt[3]{2}, \zeta)$ contains both generators $\sqrt[3]{2}, e^{2\pi i/3}\sqrt[3]{2}$ for L.
- Inversely L contains both generators for $K_1 K_3$. Thus, the fields contain each other's generators, so they are the same.
- With this description $L = K_1 K_3$, it is much easier to see that $[L : \mathbb{Q}] = 6$, since $[K_1 : \mathbb{Q}] = 3$ and $[K_1 : \mathbb{Q}] = 2$.

Examples of Extensions, XII

Example: Determine the degree of $L = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}\sqrt[3]{2})$ over $\mathbb{Q}$.

- We will make some remarks about why the degree of the composite is strictly less than the product of the field degrees is that the minimal polynomial of $e^{2\pi i/3}\sqrt[3]{2}$.
- Specifically, the reason is that $x^3 - 2$, is not irreducible over K_1, since it factors as $x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$, and the other generator $e^{2\pi i/3}\sqrt[3]{2}$ is a root of the second, quadratic factor.
- Thus, to generate L/K_1, we need only adjoin the root of a quadratic polynomial, not a cubic polynomial.
- Another way to approach this is to see that the basis $\{1, e^{2\pi i/3}\sqrt[3]{2}, e^{4\pi i/3}\sqrt[3]{4}\}$ for $K_2/\mathbb{Q}$ is not linearly independent over K_1, because $2 + (\sqrt[3]{4})[e^{2\pi i/3}\sqrt[3]{2}] + (\sqrt[3]{2})[e^{4\pi i/3}\sqrt[3]{4}] = 0$.

Algebraic Elements, I

If K/F is any field extension, we can also consider the collection of all elements of K that are algebraic over F. This is a subfield:

Proposition (Algebraic Elements)

If K/F is any field extension and $\alpha, \beta \in K$ are algebraic over F, then so are $\alpha \pm \beta$, $\alpha\beta$, and α^{-1} (the latter presuming $\alpha \neq 0$). In particular, the collection of all elements of K that are algebraic over F is a subfield of K.

We can use this observation to construct infinite algebraic extensions.

Algebraic Elements, II

Proof:

- The field $F(\alpha, \beta)$ has finite degree over F when α and β are both algebraic over F, hence $F(\alpha, \beta)$ is algebraic over F.
- Then every element in $F(\alpha, \beta)$ is algebraic over F, including (in particular) $\alpha \pm \beta$, $\alpha\beta$, and α^{-1}.
- The second statement follows immediately from the first one, upon applying the subfield criterion.

Algebraic Elements, III

Example: Consider the collection $\overline{\mathbb{Q}}$ of all elements of $\mathbb{C}$ that are algebraic over $\mathbb{Q}$.

- We claim that every element of $\overline{\mathbb{Q}}$ has finite degree over $\mathbb{Q}$, but that $\overline{\mathbb{Q}}/\mathbb{Q}$ is an infinite (algebraic) extension.
- The first statement follows immediately from our discussion of algebraic elements.
- To show that $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$, notice that (for any positive integer n) the element $\sqrt[n]{2}$ is contained in $\overline{\mathbb{Q}}$, hence the entire field $\mathbb{Q}(\sqrt[n]{2})$ is a subfield of $\overline{\mathbb{Q}}$.
- Because $\sqrt[n]{2}$ has minimal polynomial $x^n - 2$ (irreducible by Eisenstein), we see that $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$.
- Therefore, $[\overline{\mathbb{Q}} : \mathbb{Q}] \geq [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$ for every positive integer n, so we must have $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$.

Algebraic Elements, IV

Example: Consider the collection $\overline{\mathbb{Q}}$ of all elements of $\mathbb{C}$ that are algebraic over $\mathbb{Q}$.

- We will also remark that although $\overline{\mathbb{Q}}$ is much larger than $\mathbb{Q}$, it still only has a countably infinite number of elements: every element of $\overline{\mathbb{Q}}$ is a root of a monic polynomial with rational coefficients, and there are only countably infinitely many such polynomials (and each one has a finite number of roots).
- In particular, because $\mathbb{R}$ and $\mathbb{C}$ are both uncountable, there exist (very many!) transcendental real and complex numbers.
- Nonetheless, it is typically quite difficult to prove that any particular transcendental number (like e or π) is actually transcendental.

Liouville Numbers, I

Speaking of proving transcendentality, I thought you might like to see how some of these transcendentality proofs tend to go.

I was going to make this a homework problem, but it has slightly more analysis than I want to bother you with, so I'm doing it in class instead. (You're welcome.)

Liouville Numbers, II

If you are familiar with some elementary number theory, you may know the following result:

Theorem (Approximation By Rationals)

If α is any real number and n is a positive integer, there exists a rational number p/q such that $q \leq n$ and $\left|\alpha - \dfrac{p}{q}\right| \leq \dfrac{1}{q(n+1)}$.

There are various proofs. One method is simply to write down all of the rationals with denominator at most n (the Farey sequence of level n) and bound the greatest distance between any consecutive pair. Another is to use continued fraction expansions.

Now consider what happens if you apply this theorem to an increasing sequence of values of n.

Liouville Numbers, II

Corollary (Irrational Approximation By Rationals)

If α is a irrational real number and n is a positive integer, there exist infinitely many rational numbers $\frac{p}{q}$ with $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$.

The point is that this corollary's condition is false if α is rational:

- Specifically, if $\alpha = \frac{a}{b}$, then $\left|\alpha - \frac{p}{q}\right| = \frac{|aq - bp|}{bq}$.
- Then, since the numerator is an integer, if q is large enough the only way to have $\frac{|aq - bp|}{bq} < \frac{1}{q^2}$ is to have $aq - bp = 0$.
- But this would mean $a/b = p/q$, which doesn't work.

This observation gives us an explicit way to identify irrational numbers: α is irrational if and only if we can find infinitely many p/q such that $|\alpha - p/q| < 1/q^2$.

Liouville Numbers, III

The clever idea of Liouville is that one can extend this criterion to exclude algebraic numbers of degree n by increasing the exponent of q on the right-hand side of the inequality. It is easier to show the contrapositive assertion:

Lemma (Liouville)

Suppose α is algebraic of degree $n > 1$ over $\mathbb{Q}$, and suppose its minimal polynomial $m(x) \in \mathbb{Z}[x]$. Then there exists a positive real number A such that $\left|\alpha - \frac{p}{q}\right| \geq \frac{A}{q^n}$ for any rational number p/q.

The idea of the proof is to use the mean value theorem to bound the difference between $m(\alpha)$ and $m(p/q)$ and the fact that we can express $m(p/q)$ as $1/q^n$ times an integer.

Liouville Numbers, IV

Proof:

- Let M be the maximum value of $|m'(x)|$ on $[\alpha - 1, \alpha + 1]$.
- Suppose $m(x) = (x - \alpha)(x - \beta_1) \cdots (x - \beta_{n-1})$ over $\mathbb{C}$.
- Set $A = \min(1, 1/M, |\alpha - \beta_i|)$. We claim this value works.
- So suppose that $|\alpha - p/q| < A/q^n$.
- Then since $A \leq 1$, p/q lies in $[\alpha - 1, \alpha + 1]$.
- Also since $A \leq |\alpha - \beta_i|$, we see $p/q \neq \beta_i$ and there is no root of m between α and p/q.
- If $m(x) = \sum c_i x^i$ then $|m(p/q)| = \frac{1}{q^n} |\sum c_i p^i q^{n-i}| \geq \frac{1}{q^n}$ since $\sum c_i p^i q^{n-i} \in \mathbb{Z}$ and the sum is not zero as $m(p/q) \neq 0$.
- Also, by hypothesis, $A \leq 1/M$, so $|1/m'(x_0)| \geq A$.
- Then, by the mean value theorem, there exists $x_0 \in (p/q, \alpha)$ such that $m(\alpha) - m(p/q) = (\alpha - p/q) \cdot m'(x_0)$.
- Taking absolute values and rearranging gives $\left|\alpha - \frac{p}{q}\right| = \left|m(\alpha) - m(\frac{p}{q})\right| \cdot \frac{1}{|m'(x_0)|} \geq \frac{1}{q^n} \cdot A$, contradiction.

Liouville Numbers, V

We can reformulate the lemma to get a recipe for transcendental numbers:

Corollary (Liouville)

Suppose α is a real irrational number and that there exists a constant $c > 0$ and a sequence of rational numbers p_n/q_n such that $\left|\alpha - \frac{p_n}{q_n}\right| < \frac{c}{q_n^n}$. Then α is transcendental.

The point is that this sequence of rational numbers p_n/q_n contradicts the assertion that α is algebraic of degree n for every n, by the previous lemma, so α must be transcendental.

Liouville Numbers, VI

Corollary (Liouville)

Suppose α is a real irrational number and that there exists a constant $c > 0$ and a sequence of rational numbers p_n/q_n such that $\left|\alpha - \frac{p_n}{q_n}\right| < \frac{c}{q_n^n}$. Then α is transcendental.

It only remains to give some examples of such α.

- We want to arrange matters so that each successive rational approximation is substantially better than the previous.
- We can do this by taking α to be a sum of rational numbers whose sizes drop very fast, where p_n/q_n is the nth partial sum of the series.
- Then we need only ensure that the tail $\alpha - p_n/q_n$ of the series is on the order of q_n^n.

Liouville Numbers, VII

Liouville's example was the number $\alpha = \displaystyle\sum_{k=0}^{\infty} \frac{1}{10^{k!}}$.

- If p_n/q_n is the nth partial sum, then $q_n = 10^{n!}$ and so $|\alpha - p_n/q_n| = \sum_{k=n+1}^{\infty} \dfrac{1}{10^{k!}} < 2/10^{(n+1)!} < 2/(q_n)^n$.
- Thus, α satisfies the requested bound, and so it is transcendental.
- More generally, in place of the 1 in the numerators, one may put any base-10 digit d_n, and the result still holds (simply change the 2 in the inequality to a 20).
- It is not hard to see that this general class of examples yields uncountably many transcendental real numbers.

Summary

We discussed algebraic extensions and various properties of extension degrees.

We discussed a number of examples of low-degree field extensions.

We discussed some miscellaneous things about algebraic and transcendental numbers.

Next lecture: Classical geometric constructions, splitting fields.