Math 5111 (Algebra 1)

Lecture #10 $\sim$ October 15th, 2020

Separability, Transcendence

- Separability of Elements and Extensions, part 2
- Transcendental Extensions

This material represents §2.4.2-2.4.3 from the course notes.

Recall, I

Definition

If F is a field of characteristic p, and every element of F is a pth power (i.e., $F^p = F$) then we say F is a perfect field. (Fields of characteristic 0 are also considered perfect fields.)

Proposition (Separability and Perfect Fields)

If F is a perfect field, then every irreducible polynomial in $F[x]$ is separable. Inversely, if F is not perfect, then there exists an irreducible inseparable polynomial in $F[x]$.

Recall, II

We extended separability and inseparability to algebraic elements by considering their minimal polynomials:

Definition

If K/F is an algebraic extension, then $\alpha \in K$ is separable over F if α is algebraic over K and its minimal polynomial $m(x)$ over F is a separable polynomial.
We say K/F itself is separable if every $\alpha \in K$ is separable over F, and K/F is inseparable if it is not separable.

Definition

If K/F is a field extension, then $\alpha \in K$ is purely inseparable over F if α is algebraic over K and its minimal polynomial $m(x)$ over F has only α as a root.
We say K/F itself is purely inseparable if every $\alpha \in K$ is purely inseparable over F.

Recall, III

Proposition (Properties of Inseparability)

Let L/K and K/F be field extensions of characteristic p. Then

1. *If $q(x) \in F[x]$ is an irreducible inseparable polynomial, then $q(x) = q_{sep}(x^{p^k})$ for a unique positive integer k and a unique irreducible separable polynomial $q_{sep}(x) \in F[x]$.*
2. *The element $\alpha \in K/F$ is purely inseparable if and only if there exists some positive integer k such that $\alpha^{p^k} \in F$.*
3. *The extension K/F is purely inseparable if and only if the minimal polynomial of each $\alpha \in K$ over F is of the form $m_\alpha(x) = x^{p^k} - d$ for some $k \geq 0$ and some $d \in F$.*
4. *K/F is purely inseparable iff K/F is algebraic and the only elements of K separable over F are the elements of F.*
5. *L/F is purely inseparable iff L/K and K/F are purely inseparable.*
6. *Composites of purely inseparable extensions are purely inseparable.*
7. *If K/F has finite degree and $K = F(\alpha_1, \ldots, \alpha_k)$, then K/F is purely inseparable if and only if each α_i is purely inseparable over F.*

Recall, IV

Proposition (Properties of Separability, Part 1)

Let L/K and K/F be field extensions. Then

1. *The algebraic element α is separable over F if and only if there are $[F(\alpha) : F]$ different embeddings of $F(\alpha)/F$ into $\overline{F}/F$.*
2. *If K/F has finite degree, then there are at most $[K : F]$ different embeddings of K/F into $\overline{F}/F$.*
3. *If α is algebraic over F, then α is separable over F if and only if $F(\alpha)$ is separable over F.*
4. *If L/F is separable, then L/K and K/F are separable.*

Recall, V

Proposition (Properties of Separability, Part 2)

Let L/K and K/F be field extensions. Then

5. *If $[K : F]$ is finite, then K/F is separable if and only if there are exactly $[K : F]$ different embeddings of K/F into $\overline{F}/F$.*
6. *If K/F is separable, then α is separable over K if and only if α is separable over F.*
7. *If K/F has finite degree and $K = F(\alpha_1, \ldots, \alpha_k)$, then K/F is separable if and only if each α_i is separable over F.*
8. *If L/K and K/F are separable, then L/F is separable.*
9. *The composite of separable extensions is separable.*

Separable and Inseparable Degrees, I

Using the properties of separable extensions we can define the "separable closure" of F inside K/F:

Definition

If K/F is a field extension, we define the maximal separable extension F^{sep} of F inside K to be the composite of all separable extensions of F inside K.

The elements of F^{sep} consist of all $\alpha \in K$ that are separable over F.

- All such elements are in this composite since $F(\alpha)/F$ is separable by property (3) of separable extensions
- From this observation, we can see that F^{sep} is indeed the largest subfield of K that is separable over F, whence the name.

Separable and Inseparable Degrees, II

By the observation on the previous slide, since F^{sep} is the largest subfield of K that is separable over Fany element of K not in F^{sep}, that any element of K not in F^{sep} is inseparable over F hence also over F^{sep}.

- So, by property (4) of purely inseparable extensions, this means K/F^{sep} is purely inseparable.
- Indeed, F^{sep} is the only subfield E of K that is separable over F such that K/E is purely inseparable.
- This is merely because any proper subfield of F^{sep} will not have the property that K/E is purely inseparable, since there exist elements of K not in E that are not purely inseparable over E (namely, any element of F^{sep} not in E).

Separable and Inseparable Degrees, II

Using this maximal separable subextension, we can define a notion of separable and inseparable degree for extensions:

Definition

If K/F is algebraic, the separable degree $[K : F]_{sep}$ is defined to be the degree $[F^{sep} : F]$, while the inseparable degree $[K : F]_{insep}$ is defined to be the degree $[K : F^{sep}]$.

- The product of the separable degree and the inseparable degree is the regular degree $[K : F]$.
- Also, since composites and separable extensions of separable extensions are separable, the separable degree (and hence also the inseparable degree) is multiplicative in towers.
- From our properties of purely inseparable extensions, the inseparable degree $[K : F]_{\text{insep}}$ is either ∞ or a power of the characteristic.

Separable and Inseparable Degrees, IV

For simple extensions, we can calculate the separable and inseparable degree using the minimal polynomial of a generator:

Proposition (Separable Degree of Simple Extension)

Suppose α is algebraic over F with minimal polynomial $m(x) = m_{sep}(x^{p^k})$ where k is a nonnegative integer and $m_{sep}(x)$ is a separable polynomial. Then $F^{sep} = F(\alpha^{p^k})$, so that $[F(\alpha) : F]_{sep} = \deg(m_{sep})$ and $[F(\alpha) : F]_{insep} = p^k$.

The idea is to verify that $F(\alpha^{p^k})$ is separable over F, and that K is purely inseparable over $F(\alpha^{p^k})$, since these two properties together characterize F^{sep}.

Separable and Inseparable Degrees, V

Proof:

- Observe that α^{p^k} is a root of m_{sep} since $m_{\text{sep}}(\alpha^{p^k}) = m(\alpha) = 0$, so α^{p^k} is separable over F.
- Thus, $F(\alpha^{p^k})$ is separable over F by property (3) of separable extensions.
- Furthermore, since $K/F(\alpha^{p^k})$ is generated by α, and $\alpha^{p^k} \in F(\alpha^{p^k})$, by properties (3) and (7) of purely inseparable extensions we see that $K/F(\alpha^{p^k})$ is purely inseparable.
- But this means $F(\alpha^{p^k})$ must be F^{sep} by the uniqueness property we noted above.
- For the degree calculations we have $[F(\alpha^{p^k}) : F] = \deg(m_{\text{sep}})$ since m_{sep} is the minimal polynomial of α^{p^k} over F, and also $[F(\alpha) : F(\alpha^{p^k})] = p^k$ since $x^{p^k} - \alpha^{p^k}$ is the minimal polynomial of α over $F(\alpha^{p^k})$.

Separable and Inseparable Degrees, IV

Example: For $F = \mathbb{F}_p(t)$ and $K = F(\alpha)$ where α is a root of the irreducible polynomial $q(x) = x^{2p} - tx^p + t$, find the separable and inseparable degrees of K/F.

Separable and Inseparable Degrees, IV

Example: For $F = \mathbb{F}_p(t)$ and $K = F(\alpha)$ where α is a root of the irreducible polynomial $q(x) = x^{2p} - tx^p + t$, find the separable and inseparable degrees of K/F.

- Note that $m(x) = m_{\text{sep}}(x^p)$ where $m_{\text{sep}}(x) = x^2 - tx + t$.
- Thus, $[K : F]_{\text{sep}} = 2$ and $[K : F]_{\text{insep}} = p$.
- Note that q is irreducible in $F[x]$ since it is Eisenstein at t.
- Explicitly, F^{sep} is the quadratic extension of F generated by a root of $m_{\text{sep}}(x) = x^2 - tx + t$.

Separable and Inseparable Degrees, V

Example: For $F = \mathbb{F}_p(x^p, y^p)$ and $K = \mathbb{F}_p(x, y)$, find the separable and inseparable degrees of K/F.

Separable and Inseparable Degrees, V

Example: For $F = \mathbb{F}_p(x^p, y^p)$ and $K = \mathbb{F}_p(x, y)$, find the separable and inseparable degrees of K/F.

- We have an intermediate field $E = \mathbb{F}_p(x^p, y) = F(y)$.
- The element y is a root of the polynomial $q(Y) = Y^p - y^p$ in $F[Y]$. This polynomial is purely inseparable and irreducible since $y \notin F$, so we have $[E : F]_{\text{sep}} = 1$ and $[E : F]_{\text{insep}} = p$.
- Then, the element x is a root of the polynomial $p(X) = X^p - x^p$ in $E[X]$. This polynomial is likewise purely inseparable and irreducible since $x \notin E$, so we have $[K : E]_{\text{sep}} = 1$ and $[K : E]_{\text{insep}} = p$.
- Thus, we see $[K : F]_{\text{sep}} = 1$ and $[K : F]_{\text{insep}} = p^2$.

This particular field extension is an important source of counterexamples and we will return to analyze it further in a month or so.

Transcendence, I

As our final topic in the basic theory of field extensions, we will discuss a bit more about the structure of transcendental extensions.

- If K/F is any field extension, let E be the field of elements algebraic over F inside K. Then, since algebraic extensions of algebraic extensions are algebraic, any element of K/E not in E must be transcendental over F.
- Our goal is to describe how to analyze this "transcendental part" of the extension.
- To describe the elements of K, the idea is to identify a minimal set of independent generators for K/E, in analogy with the situation in vector spaces.
- Here, however, we do not merely need the generators to be linearly independent, but rather algebraically independent, meaning that there are no algebraic relations between them.

Transcendence, II

Definition

Let K/F be a field extension. We say a subset S of K is algebraically dependent over F if there exists a finite subset $\{s_1, \ldots, s_n\} \in S$ and a nonzero polynomial $p \in F[x_1, \ldots, x_n]$ such that $p(s_1, \ldots, s_n) = 0$.
If there exists no such p for any finite subset of S, we say S is algebraically independent.

The general idea here is that a set of elements is algebraically dependent if they satisfy some algebraic (i.e., polynomial) relation over F.

Transcendence, III

Examples:

1. Over $\mathbb{Q}$, the set $\{\pi, \pi^2\}$ is algebraically dependent, since $p(x, y) = x^2 - y$ has $p(\pi, \pi^2) = 0$.
2. Over $\mathbb{Q}$, the set $\{\sqrt[3]{2}\}$ is algebraically dependent, since $p(x) = x^3 - 2$ has $p(\sqrt[3]{2}) = 0$.
3. More generally, the set $\{\alpha\}$ is algebraically independent over F if and only if α is transcendental over F.
4. Over $\mathbb{R}$, the set $\{x + y, x^2 + y^2\}$ is algebraically independent (here we are of course assuming that x and y are independent indeterminates).
5. The empty set is trivially algebraically independent.

Transcendence, IV

Examples:

6. Over $\mathbb{R}$, the set $\{x+y, x^2+y^2, x^3+y^3\}$ is algebraically dependent, since $p(a,b,c) = a^3 - 3ab + 2c$ has $p(x+y, x^2+y^2, x^3+y^3) = 0$.
7. If $x_1, \ldots, x_n$ are indeterminates inside $F(x_1, \ldots, x_n)$, the function field in n variables, then the set $\{x_1, \ldots, x_n\}$ is algebraically independent over F.
8. Over $\mathbb{Q}$, the set $\{1+x^3, x+x^2\}$ is algebraically dependent, since $p(a,b) = a + 3b - 3ab - a^2 - b^3$ has $p(1+x^3, x+x^2) = 0$.

Transcendence, V

The notion of algebraic independence generalizes the notion of linear independence, and as such the two concepts are related in various ways.

- It is easy to see that any subset of an algebraically independent set is algebraically independent, while any set containing an algebraically dependent set is algebraically dependent.
- Also, we observe that linear dependence is a special type of algebraic dependence; namely, a set is linearly dependent precisely when it is algebraically dependent where the polynomial p is linear.
- We have already defined the algebraic notion of the span of a set S: it is simply the subfield generated by S.

Transcendence, VI

We might therefore hope to define a "transcendence basis" to be an algebraically independent set that generates the extension K/F.

- Unfortunately, such a set need not exist: for example, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ has no such set, because there are no transcendental elements at all.
- The correct analogy is instead to observe that a basis for a vector space is a maximal linearly independent set (which was the object we used Zorn's lemma to construct).

Transcendence, VII

Definition

Let K/F be a field extension. A transcendence base for K/F is an algebraically independent subset S of K that is maximal in the set of all algebraically independent subsets of K.

- Remark: The term "transcendence basis" is also used occasionally. We will prefer to use the word "base" to keep a distinction between a basis of a vector space and a transcendence base of a field extension.
- By a straightforward Zorn's lemma argument (homework problem inbound!), every extension has a transcendence base.

Transcendence, VIII

Examples:

1. The empty set $\emptyset$ is a transcendence base for $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$.
2. More generally, K/F is algebraic if and only if $\emptyset$ is a transcendence base.
3. The set $\{x\}$ is a transcendence base for $F(x)$ over F.
4. The set $\{x^{2020}\}$ is a transcendence base for $F(x)$ over F. (This is not immediately obvious, but intuitively,)

Transcendence, IX

Here are some of the fundamental properties of transcendence bases, many of which are analogous to properties of vector spaces:

Proposition (Properties of Transcendence Bases, Part 1)

Suppose K/F is a field extension and S is a subset of K.

1. *If S is algebraically independent and $\alpha \in K$, then $S \cup \{\alpha\}$ is algebraically independent over F if and only if α is transcendental over $F(S)$.*
2. *S is a transcendence base of K/F if and only if K is algebraic over $F(S)$.*
3. *If T is a subset of K such that $K/F(T)$ is algebraic, then T contains a transcendence base of K/F.*
4. *If T is an algebraically independent subset of K, then T can be extended to a transcendence base of K/F.*

Transcendence, X

Here are some of the fundamental properties of transcendence bases, many of which are analogous to properties of vector spaces:

Proposition (Properties of Transcendence Bases, Part 2)

Suppose K/F is a field extension and S is a subset of K.

5. *If $S = \{s_1, \ldots, s_n\}$ is a transcendence base for K/F and $T = \{t_1, \ldots, t_m\}$ is any algebraically independent set, then there is a reordering of S, say $\{a_1, \ldots, a_n\}$, such that for each $1 \leq k \leq m$, the set $\{t_1, t_2, \ldots, t_k, a_{k+1}, \ldots, a_n\}$ is a transcendence base for K/F.*
6. *If S is a (finite) transcendence base for K/F, then any subset T of K having larger cardinality than S must be algebraically dependent.*
7. *Any two transcendence bases S and T for K/F have the same cardinality.*

Transcendence, XI

1. If S is algebraically independent and $\alpha \in K$, then $S \cup \{\alpha\}$ is algebraically independent over F if and only if α is transcendental over $F(S)$.

Proof:

- This is the algebraic analogue of the statement that if S is linearly independent, then $S \cup \{\alpha\}$ is linearly independent if and only if α is not in the span of S.
- Suppose $S \cup \{\alpha\}$ is algebraically dependent.
- Then there exists $s_i \in S$ and $p \in F[x]$ with $p(\alpha, s_1, \ldots, s_n) = 0$ and $p \neq 0$.
- View p as a polynomial in its first variable with coefficients in $F[s_1, \ldots, s_n]$: there must be at least one term involving α, as otherwise p would give an algebraic dependence in S.
- Then α is the root of a nonzero polynomial with coefficients in $F[s_1, \ldots, s_n] \subseteq F(S)$, so it is algebraic over $F(S)$.

Transcendence, XII

1. If S is algebraically independent and $\alpha \in K$, then $S \cup \{\alpha\}$ is algebraically independent over F if and only if α is transcendental over $F(S)$.

Proof (conversely):

- Conversely, suppose that α is algebraic over $F(S)$. Then α is the root of some nonzero polynomial with coefficients in $F(S)$.
- Each coefficient of this polynomial is an element of $F(S)$; clearing denominators yields a nonzero polynomial p with coefficients in $F[s_1, \ldots, s_n]$ for the elements $s_i \in S$ that appear in these coefficients.
- This polynomial yields an algebraic dependence in $S \cup \{\alpha\}$.

Transcendence, XIII

2. If S is algebraically independent and $\alpha \in K$, then $S \cup \{\alpha\}$ is algebraically independent over F if and only if α is transcendental over $F(S)$.

Proof:

- This follows from (1) and the maximality of transcendence bases.
- Specifically, S is a transcendence base if and only if no elements in K can be adjoined to S while preserving algebraic independence.
- By (1), this is equivalent to saying that all elements in K are algebraic over $F(S)$.

Transcendence, XIV

3. If T is a subset of K such that $K/F(T)$ is algebraic, then T contains a transcendence base of K/F.

Proof:

- By Zorn's lemma, there must be a maximal algebraically independent subset of T.
- But a maximal element M in this collection must be a transcendence base for K/F: if $\beta \in K$ then β must be algebraic over $K/F(M)$ by the maximality of M, and then M is a transcendence base by (2).

Transcendence, XV

4. If T is an algebraically independent subset of K, then T can be extended to a transcendence base of K/F.

Proof:

- This is the analogue of the fact that every linearly independent subset can be extended to a basis.
- The proof follows from a similar Zorn's lemma argument.

Transcendence, XVI

5. If $S = \{s_1, \ldots, s_n\}$ is a transcendence base for K/F and $T = \{t_1, \ldots, t_m\}$ is any algebraically independent set, then there is a reordering of S, say $\{a_1, \ldots, a_n\}$, such that for each $1 \leq k \leq m$, the set $\{t_1, t_2, \ldots, t_k, a_{k+1}, \ldots, a_n\}$ is a transcendence base for K/F.

Proof:

- This is the analogue of the replacement theorem, and the proof proceeds inductively in essentially the same way.
- I will skip this one, since I think we've all suffered enough (and also I skipped the replacement theorem for vector spaces anyway).

Transcendence, XVII

6. If S is a (finite) transcendence base for K/F, then any subset T of K having larger cardinality than S must be algebraically dependent.

Proof:

- If $S = \{s_1, \ldots, s_n\}$ is finite, apply the replacement theorem (5) to S and T.
- At the end of the replacement, the result is that $\{t_1, \ldots, t_n\}$ is a transcendence base.
- But then by (2), any additional element of T would be algebraic over $\{t_1, \ldots, t_n\}$, contradicting the algebraic independence of T.

Transcendence, XVIII

7. Any two transcendence bases S and T for K/F have the same cardinality.

Proof:

- If the bases are infinite the result is immediate.
- Otherwise, suppose S has finite cardinality n.
- Apply (6): then T's cardinality m must satisfy $m \leq n$, since T is algebraically independent and S is a transcendence base.
- But also, (6) requires $n \leq m$ since S is algebraically independent and T is a transcendence base.
- So $m = n$ as claimed.

Transcendence, XIX

The result of the last part of the proposition shows that any two transcendence bases have the same cardinality.

- In analogy with the situation for vector spaces, this cardinality behaves somewhat like an extension degree:

Definition

Let K/F be a field extension. The transcendence degree of K/F, denoted $\mathrm{trdeg}(K/F)$, is the cardinality of any transcendence base of K/F.

Transcendence, XX

The key property of transcendence degree is that it is additive in towers:

Theorem (Transcendence in Towers)

If $L/K/F$ is a tower of extensions, then $\operatorname{trdeg}(L/F) = \operatorname{trdeg}(L/K) + \operatorname{trdeg}(K/F)$.

The idea here is quite simple: we want to show that the union of transcendence bases for K/F and L/K gives a transcendence base for L/F.

Transcendence, XXI

Proof:

- First suppose that both $\mathrm{trdeg}(K/F)$ and $\mathrm{trdeg}(L/K)$ are finite, and let $S = \{s_1, \ldots, s_n\}$ and $T = \{t_1, \ldots, t_m\}$ be transcendence bases for K/F and L/K. Then $S \cap T = \emptyset$ since each t_i is transcendental over K.
- Furthermore, K is algebraic over $F(S)$, so $K(T)$ is algebraic over $F(T)(S) = F(S \cup T)$ by our results on algebraic extensions.
- Then since L is algebraic over $K(T)$, we deduce that L is algebraic over $F(S \cup T)$, also by our results on algebraic extensions.
- Thus, by property (3) of transcendence bases, $S \cup T$ contains a transcendence base of L/F.

Transcendence, XXII

Proof (continued):

- Finally, we claim $S \cup T$ is algebraically independent over F, so suppose that $p(s_1, \ldots, s_n, t_1, \ldots, t_m) = 0$ for some $p \in F[x_1, \ldots, x_n, y_1, \ldots, y_m]$.
- Separate monomial terms to write $p(s_1, \ldots, s_n, t_1, \ldots, t_m) = 0$ as a sum $\sum f_i(s_1, \ldots, s_n) g_i(t_1, \ldots, t_m) = 0$ with $f_i \in F[x_1, \ldots, x_n]$ and $g_i \in F[y_1, \ldots, y_m]$.
- Now, since T is algebraically independent over $F(S) \subseteq K$, all of the $f_i(s_1, \ldots, s_n)$ must be zero (as elements of K). But since S is algebraically independent over F, that means all of the polynomials $f_i(x_1, \ldots, x_n)$ must be zero (as polynomials).
- This means p is the zero polynomial, and so $S \cup T$ is algebraically independent.

Transcendence, XXIII

Fields that are generated by a transcendence base are particularly convenient:

Definition

The extension K/F is purely transcendental if $K = F(S)$ for some transcendence base S of K/F.

- Equivalently, K/F is purely transcendental when it is generated (as a field extension) by an algebraically independent set.
- If $S = \{s_1, \ldots, s_n\}$, then the purely transcendental extension $K = F(S)$ is ring-isomorphic to the function field $F(x_1, \ldots, x_n)$ in n variables: it is not hard to check that the map sending s_i to x_i is an isomorphism.

Transcendence, XXIV

If K/F has transcendence degree 1 or 2 and E/F is an intermediate extension, then in fact E is also purely transcendental.

- The degree-1 case is a theorem of Lüroth, while the degree-2 case is a theorem of Castelnuovo.
- In higher degrees, there do exist extensions that are not purely transcendental, but it is not easy to verify this fact.

Transcendence, XXV

Since any extension K/F has a transcendence base S, property (2) of transcendence bases implies that K/F is an algebraic extension of the purely transcendental extension $F(S)/F$.

- This shows that any field extension can be written as an algebraic extension of a purely transcendental extension.
- One might wonder whether it is possible to reverse the order and put the algebraic piece first: the answer turns out to be no, for reasons related to algebraic geometry.
- For example, if F is algebraically closed (e.g., $\mathbb{C}$) any example of a transcendental extension that is not purely transcendental cannot have the order reversed, since there are no algebraic extensions of $\mathbb{C}$.

Transcendence, XXVI

One example of such a field is the elliptic function field $\mathbb{C}(t, \sqrt{t^3 + t})$.

- This field arises as the function field of the elliptic curve $y^2 = x^3 + x$.
- The relationship between these two follows from the fact that $\mathbb{C}(t, \sqrt{t^3 + t}) \cong \mathbb{C}[x, y]/(y^2 - x^3 - x)$.
- We have barely scratched the surface of what can be said here, but as a closing remark I will note that much of elementary algebraic geometry is concerned with understanding these connections between algebraic properties of function fields and geometric properties of varieties.
- To hear (much) more about all of this, take Math 5112 and then learn algebraic geometry!

Where Do We Go From Here?, I

Let me now preview where we are headed.

- Now that we've discussed transcendental extensions, our overarching goal is to study the structure of algebraic field extensions and (more or less equivalently) the roots of polynomials.
- So far we have taken a very element-centric approach: we have focused primarily on elements of extensions and how to compute things in terms of generators.
- However, one of the main principles of the modern approach to algebra is that we really should be studying (structure-preserving) maps.

Where Do We Go From Here?, II

In fact, in some sense we have already been studying maps (i.e., ring homomorphisms) on fields.

- As noted before, if $\varphi : F_1 \to F_2$ is a ring homomorphism, then $\ker F_1$ is an ideal of F_1.
- Since there are not so many ideals of F_1, this means either φ is the zero map (not so exciting) or is one-to-one.
- In the latter case, φ yields an isomorphism of F_1 with its image inside F_2, which is to say, it gives an embedding of F_1 inside F_2.
- If we imprecisely think of F_1 as actually being equal to its image, then this merely says F_2 is a field extension of F_1.

Where Do We Go From Here?, III

If we allow ourselves to feel comfortable with the field extension part of this discussion, we're still left with having to think about the nature of the isomorphism of $\varphi : F_1 \to \mathrm{im}\varphi$.

- Equivalently, what we need to understand is the structure of isomorphisms of F_1 with itself look like.
- We give a special name to an isomorphism of an object with itself: it is called an automorphism.

Where Do We Go From Here?, IV

Definition

If F is a field, a (ring) isomorphism $\sigma : F \to F$ of F with itself is called a field automorphism of F.

Our interest in field automorphisms comes from the fact that they naturally act on roots of polynomials.

- Specifically, suppose $\sigma : K \to K$ is a field automorphism that fixes the subfield F of K.
- If $p(x) \in F[x]$ and $p(\alpha) = 0$, then $p(\sigma(\alpha)) = \sigma(p(\alpha) = \sigma(0) = 0$, since σ fixes all of the coefficients of p since they are in F.
- This means $\sigma(\alpha)$ is also a root of $p(x)$.

Where Do We Go From Here?, V

The fundamental idea of Galois theory is to exploit field automorphisms to study fields. To do this, we first need to understand the automorphisms themselves:

Question

If F is a field, what does the set of field automorphisms $\sigma : F \to F$ look like? What are its properties? Does it have any kind of nice structure?

Where Do We Go From Here?, VI

Some relevant observations in the direction of those questions:

- The identity map is an automorphism of F.
- If σ and τ are automorphisms of F, then so is the composition $\sigma \circ \tau$.
- Composition of automorphisms of F is associative (it is, after all, just function composition).
- If σ is an automorphism of F, then so is its inverse σ^{-1}.

Where Do We Go From Here?, VI

Some relevant observations in the direction of those questions:

- The identity map is an automorphism of F.
- If σ and τ are automorphisms of F, then so is the composition $\sigma \circ \tau$.
- Composition of automorphisms of F is associative (it is, after all, just function composition).
- If σ is an automorphism of F, then so is its inverse σ^{-1}.

The point here is that the set of automorphisms of F naturally forms a group under function composition.

So, we now take a detour to develop basic group theory, which will give us the tools we need to understand field automorphisms.

Summary

We discussed separability and inseparability for field extensions.

We discussed transcendental extensions and formulated the notion of transcendence degree.

Next lecture: Groups.