# Math 5111 (Algebra 1)

## Lecture #9 ∼ October 8th, 2020

Separability and Inseparability

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

This material represents §2.4.1-2.4.2 from the course notes.

# Recall, I

Last time we discussed algebraic closures and algebraically closed fields:

**Definition**

*If $F$ is a field, the field $\overline{F}$ is an algebraic closure of $F$ if $\overline{F}$ is algebraic over $F$ and every polynomial in $F[x]$ splits completely over $\overline{F}$.*

**Definition**

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

We proved that every field has an algebraic closure that is unique up to isomorphism, and that algebraic closures are algebraically closed.

# Recall, II

We also introduced the notion of separability for polynomials:

**Definition**

*If $F$ is a field with $q \in F[x]$, and the factorization of $q(x) = c(x - r_1)^{d_1}(x - r_2)^{d_2} \cdots (x - r_k)^{d_k}$ with the $d_i \geq 1$, we say that $d_i$ is the multiplicity of $r_i$.*
*Furthermore, $r_i$ is a simple root if $d_i = 1$, and is a repeated root (or multiple root) if $d_i \geq 2$.*
*If all of the roots of $q$ are simple, then we say $q$ is separable, and otherwise $q$ is inseparable.*

A separable polynomial is one that has no repeated roots, while an inseparable polynomial has a repeated root.

In general, separable polynomials are “nice”, while inseparable polynomials are “not as nice”.

# Recall, III

We can detect separability using the derivative:

**Proposition (Derivatives and Separability)**

*Let $F$ be a field and $q \in F[x]$. Then $r$ is a repeated root of $q$ (in a splitting field) if and only if $q(r) = q'(r) = 0$. Furthermore, the polynomial $q(x)$ is separable if and only if $q(x)$ and $q'(x)$ are relatively prime in $F[x]$.*

From this criterion, we showed that an irreducible polynomial $q(x)$ can only be inseparable in characteristic $p$.

# More Separability, I

In positive characteristic, there can exist inseparable irreducible polynomials (I gave some examples last time). Let's dig into this a bit more.

- As we noted earlier, over $F = \mathbb{F}_2(t)$, the polynomial $q(x) = x^2 - t$ is irreducible and also inseparable, because it has a repeated root $t^{1/2}$ that is not in $F$.
- In that example, notice that $q'(x) = 2x = 0$ is identically zero, so indeed $q$ and $q'$ have a common divisor of positive degree (namely, $q$ itself).
- Indeed, by degree considerations, the case where $q'$ is the zero polynomial is the only case in which we can have an inseparable irreducible polynomial, since if $q' \neq 0$ then since $\deg q > \deg q'$, it is not possible for $q$ to divide $q'$.

# More Separability, II

We are looking for situations where $q$ can divide its derivative $q'$.

- From the definition of derivative, we can see that if $q(x) = \sum_{k=0}^{n} a_n x^n$ then $q'(x) = \sum_{k=0}^{n} n a_n x^{n-1}$ is zero if and only if $n a_n = 0$ for each $n$, and this is true precisely when the only nonzero coefficients of $q$ are in degrees that are divisible by $p$.
- Equivalently, this means that $q(x) = s(x^p)$ for some polynomial $s \in F[x]$.
- Thus, there is an inseparable irreducible polynomial over $F$ precisely when there is a polynomial $s \in F[x]$ with the property that $s(x^p)$ is irreducible.

# More Separability, III

To examine this property in more detail requires a (very useful!) result on field arithmetic in characteristic $p$:

**Proposition ("Freshman" Binomial Theorem)**

*If the field $F$ has characteristic $p > 0$, then $(a+b)^p = a^p + b^p$ for any $a, b \in F$.*

Proof:

- As you proved on the homework, $(a+b)^p = \sum_{n=0}^{p} \binom{p}{n} a^n b^{p-n}$.
- For each $0 < n < p$, the binomial coefficient $\binom{p}{n} = \frac{p!}{n!(p-n)!}$ is an integer divisible by $p$ (there is a $p$ in the numerator but not in the denominator, and $p$ is prime), so $\binom{p}{n} = 0$ in the field $F$.
- Therefore, all terms in the sum except those for $n = 0$ and $n = p$ are zero: thus $(a+b)^p = a^p + b^p$ for any $a, b \in F$.

# More Separability, IV

The $p$th-power map in characteristic $p$ is very important, so I will tell you its name now:

**Definition**

*If $F$ is a field of characteristic $p$, the Frobenius endomorphism is the map $\varphi : F \to F$ defined by $\varphi(a) = a^p$.*

- Trivially, $\varphi$ respects multiplication, and by the freshman binomial theorem it also respects addition.
- Furthermore, $\varphi$ is injective, because $\varphi(a) = \varphi(b)$ implies $a^p = b^p$ so that $(a-b)^p = 0$ (since $\varphi$ distributes over addition, and $(-1)^p = -1$ in $\mathbb{F}_p$ for any prime $p$) and thus $a = b$ since $F$ is a field.
- Thus, the Frobenius map $\varphi$ is an injective ring homomorphism from $F$ to itself (i.e., an endomorphism).

# More Separability, V

The Frobenius endomorphism need not be an isomorphism, since it does not have to be surjective. However, fields where it is surjective tend to be nice:

## 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.)*

Examples:

- If $F$ is a finite field, then $F$ is perfect. This follows by the fact that the Frobenius map is an injective map from a finite set to itself, hence is also surjective.
- The function field $F = \mathbb{F}_p(t)$ is not perfect, since the element $t \in F$ is not the $p$th power of any element of $F$.

# More Separability, VI

The point of this excursion, in our case, is that perfect fields behave very nicely with respect to separability:

- Specifically, as noted earlier, if $q$ is an irreducible inseparable polynomial, then we must have $q(x) = s(x^p)$ for some polynomial $s \in F[x]$.
- By iterating the additivity of $\varphi$, we can see that $(a_0 + a_1 x + \cdots + a_n x^n)^p = a_0^p + a_1^p x^p + \cdots + a_n^p x^{np}$.
- Applying this in reverse, we can see that if all of the coefficients of $s(x)$ are $p$th powers in $F$, then $s(x^p)$ is a $p$th power, and therefore cannot be irreducible.
- This means that any irreducible polynomial over a perfect field must be separable.

# More Separability, VII

More precisely:

**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 $F[x]$.*

We showed last time that if $q$ is irreducible, then $q$ is inseparable if and only if $q$ divides its derivative $q'$: the point is that they cannot be relatively prime, but the only possible gcds, which are divisors of $q$, are 1 and $q$ up to associates.

# More Separability, VIII

Proof:

- Every field of characteristic 0 is separable: if $q(x)$ has degree $n$, then $q'$ has degree $n-1$ so $q$ cannot divide $q'$.
- So now assume $F$ has characteristic $p$. Then $q$ still divides $q'$, and the only way this can occur is if $q'$ is zero, meaning that $q(x) = s(x^p)$ for some polynomial $s \in F[x]$.
- If $F$ is perfect, then every coefficient of $s$ is a $p$th power, so we may write $s(x) = a_0^p + a_1^p x + \cdots + a_n^p x^n$. But then $q(x) = s(x^p) = a_0^p + a_1^p x^p + \cdots + a_n^p x^{np} = (a_0 + a_1 x + \cdots + a_n x^n)^p$ is not irreducible, which is a contradiction.

# More Separability, IX

Proof (continuatedly):

- Now suppose $F$ is not perfect: then there exists some element $\alpha \in F$ that is not a $p$th power in $F$.
- Consider $q(x) = x^p - \alpha$: if we set $\beta = \alpha^{1/p}$ (inside a splitting field for $q$) then in $F(\beta)$ we may write $q(x) = x^p - \beta^p = (x - \beta)^p$ so $q$ is inseparable.
- In fact, $q$ is also irreducible in $F[x]$: if it had a factorization $q(x) = c(x)d(x)$ in $F[x]$: then up to constant factors in $F$ we must have $c(x) = (x - \beta)^d$ for some $0 < d < p$.
- But this cannot happen: $c(x) = x^d - d\beta x^{d-1} + \cdots + (-1)^d \beta^d$, and if $d\beta \in F$ then because $d \neq 0$ in $F$ (since $0 < d < p$) we would have $\beta \in F$.
- But this contradicts the assumption that $\alpha$ is not a $p$th power in $F$. Thus, $q$ is an irreducible inseparable polynomial over the non-perfect field $F$.

# Fun With Finite Fields, I

As an application of our results, we can show that there exists a finite field with $p^n$ elements, and that it is unique up to isomorphism:

**Theorem (Existence and Uniqueness of Finite Fields)**

*For any prime $p$ and any positive integer $n$, there exists a finite field of degree $n$ over $\mathbb{F}_p$, and this field has $p^n$ elements. Furthermore, any two finite fields with $p^n$ elements are isomorphic.*

This is, in some sense, a strong converse of the result you established on the homework (that every finite field has a prime-power number of elements).

# Fin With Funite Fields, II

Proof:

- Consider the polynomial $q(x) = x^{p^n} - x$ over $\mathbb{F}_p$, and let $K$ be its splitting field.
- We see that $q'(x) = p^n x^{p^n - 1} - 1 = -1$: thus, $q$ is separable and so it has precisely $p^n$ roots in $K$.
- If $r$ and $s$ are any two roots of $q$ in $K$, then $r^{p^n} = r$ and $s^{p^n} = s$. We can then see that $(rs)^{p^n} = r^{p^n} s^{p^n} = rs$, and $(r - s)^{p^n} = r^{p^n} - s^{p^n} = r - s$, and if $r \neq 0$ then $(r^{-1})^{p^n} = (r^{p^n})^{-1} = r^{-1}$.
- These three calculations show that if $r$ and $s$ are roots of $q$, then so are $rs$, $r - s$, and $r^{-1}$. Together with the trivial observations that 0 and 1 are roots of $q$, this says that the set of roots of $q$ is a subfield of $K$.

# Fields With Finite Fun, III

Proof (additionally):

- But since $K$ is generated (as a field) by the set of roots of $q$, this means that the set of roots is all of $K$.
- So: the splitting field of $q(x) = x^{p^n} - x$ over $\mathbb{F}_p$ is merely the set of roots of $q$, so $\#K = p^n$.
- Thus, we have shown the existence of a finite field with $p^n$ elements, as required.
- Also, as you saw on the homework, if $K/F$ has dimension $k$, then the number of elements of $K/F$ is $(\#F)^n = p^k$.
- So this also tells us that $[K : \mathbb{F}_p] = n$.

# Fine Finite Field Funs, IV

Now we interject with a quick lemma:

**Lemma**

*If $K$ is a field with $\#K = p^n$, then $r^{p^n-1} = 1$ for all nonzero $r \in K$.*

Proof (of lemma):

- Let $S = \{u_1, \dots, u_{p^n-1}\}$ be the set of nonzero elements of $K$.
- For any nonzero $r \in K$, multiplication by $r$ is an injective function on $S$ (since $r$ is in fact a unit), hence is a bijection.
- Thus, the elements $\{ru_1, \dots, ru_{p^n-1}\}$ are the same as the elements $\{u_1, \dots, u_{p^n-1}\}$, though possibly in a different order.
- In particular, the products of these collections of elements are equal: so, $r^{p^n-1}(u_1 \cdots u_{p^n-1}) = u_1 \cdots u_{p^n-1}$ so cancelling the units $u_1, \dots, u_{p^n-1}$ yields $r^{p^n-1} = 1$, as claimed.

This is really just Lagrange's theorem applied inside the group $F^\times$, by the way. (We will get there in a few weeks, don't worry!)

# Fine Finite Field Fumblings, V

Proof (back to the theorem again):

- Now we establish the uniqueness up to isomorphism: so suppose $K$ is a finite field with $p^n$ elements.
- By the lemma, this means $r^{p^n-1} = 1$ for all nonzero $r \in K$.
- Equivalently, this says that every element in $K$ (including 0) is a root of the polynomial $q(x) = x^{p^n} - x$.
- Thus, $K$ is contained in the splitting field for $q(x)$.
- But as we have just shown earlier in the proof of this theorem, the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$ already has $p^n$ elements, so it must be equal to $K$.
- Finally, since splitting fields are unique up to isomorphism, $K$ is unique up to isomorphism. Victory.

# Five Fine Fun Finite Field Fumblings, VI

To summarize, our theorem tells us that for any prime $p$, there is a finite field $K$ with $p^n$ elements, and it is unique up to isomorphism.

- This field is the splitting field of $q(x) = x^{p^n} - x$. However, this description, while very explicit, is not terribly amenable for computations, since it does not actually give us a particularly nice way to describe the elements of the field.
- If we want a nicer description, we can try running through the construction of the splitting field, by picking an irreducible factor $f$ and then adjoining a root by using our polynomial quotient construction $\mathbb{F}_p[x]/(f)$.
- We might hope that there would be an irreducible factor $f$ of degree $n$: if there were, then in fact the field extension $\mathbb{F}_p[x]/(f)$ would have degree $n$ hence actually be our field $K$.
- Pleasantly, this is always true, and we will prove it later as an easy application of Galois theory.

# Fabulous Fourth Fun Finite-Field Frobenius Fact, VII

I will also observe here that although it was never mentioned by name, the Frobenius map $\varphi_p : K \to K$ with $\varphi_p(r) = r^p$ played an important role in the proof.

- Roughly speaking, the first half of the argument boils down to proving that the $n$-fold iterate $\varphi_p^n = \underbrace{\varphi_p \circ \varphi_p \circ \cdots \circ \varphi_p}_{n \text{ times}}$ is the identity map on $K$.
- The second half essentially reduces to showing the converse; namely, that if the $n$-fold iterate of $\varphi_p$ is the identity map on $K$, then $K$ has $p^n$ elements and is unique up to isomorphism.

In light of all this, it may not surprise you to learn that we will be able to recast most everything one can say about finite fields purely in terms of properties of the Frobenius map.

# Separable and Inseparable Extensions, I

We can also extend these notions of 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 $\alpha$ 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.*

# Separable and Inseparable Extensions, II

Examples:

1. Any algebraic element in an extension of characteristic 0 is separable, so algebraic extensions of characteristic-0 fields are separable.
2. More generally, any algebraic element in an extension $K/F$ where $F$ is a perfect field is separable, so algebraic extensions of perfect fields are separable.
3. The element $t^{1/2} \in \mathbb{F}_2(t^{1/2})$ is not separable over $\mathbb{F}_2(t)$, since its minimal polynomial is the inseparable polynomial $p(x) = x^2 - t$.
4. The element $t^{1/3} \in \mathbb{F}_2(t^{1/3})$ is separable over $\mathbb{F}_2(t)$, since its minimal polynomial is the separable polynomial $p(x) = x^3 - t$.

# Separable and Inseparable Extensions, III

The inverse notion to a separable element is of an inseparable element that is "as inseparable as possible", where all of the roots of its minimal polynomial are the same:

**Definition**

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

From the definition it is not clear that purely inseparable extensions exist (and of course if $F$ is perfect, they cannot). We will characterize them in a moment.

# Separable and Inseparable Extensions, IV

Examples:

1. The element $t^{1/2} \in \mathbb{F}_2(t^{1/2})$ is purely inseparable over $\mathbb{F}_2(t)$: its minimal polynomial is the inseparable polynomial $m(x) = x^2 - t$, which factors as $m(x) = (x - t^{1/2})^2$ over $\mathbb{F}_2(t^{1/2})$, and this polynomial has only $t^{1/2}$ as a root.
2. The element $t^{1/5} \in \mathbb{F}_5(t^{1/25})$ is purely inseparable over $\mathbb{F}_5(t)$: its minimal polynomial is the inseparable polynomial $m(x) = x^5 - t$, which factors as $m(x) = (x - t^{1/5})^5$ over $\mathbb{F}_5(t^{1/25})$, and this polynomial has only $t^{1/5}$ as a root. This factorization also shows $m$ is irreducible, since no lower power $(x - t^{1/5})^k$ for $1 \leq k \leq 4$ actually yields a polynomial with coefficients in $\mathbb{F}_5(t)$.

# Separable and Inseparable Extensions, IV

Examples:

3. The element $t^{1/25} \in \mathbb{F}_5(t^{1/25})$ is purely inseparable over $\mathbb{F}_5(t)$: its minimal polynomial is the inseparable polynomial $m(x) = x^{25} - t$, which can be seen to factor as $m(x) = (x - t^{1/25})^{25}$ over $\mathbb{F}_5(t^{1/25})$, and this polynomial has only $t^{1/25}$ as a root. This polynomial $m(x)$ is irreducible for the same reason as in the last example. Alternatively, $m(x)$ is Eisenstein-irreducible with prime $t$.

I would give more examples, but these are essentially the only kind, as we will see in a moment.

# Purely Inseparable Extensions, I

## 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 $\alpha_i$ is purely inseparable over $F$.*

# Purely Inseparable Extensions, II

1. If $q(x) \in F[x]$ is an irreducible inseparable polynomial, then $q(x) = q_{\text{sep}}(x^{p^k})$ for a unique positive integer $k$ and a unique irreducible separable polynomial $q_{\text{sep}}(x) \in F[x]$.

Proof:

- As we showed earlier, if an irreducible polynomial $q$ is inseparable, then $q(x) = q_1(x^p)$ for some $q_1 \in F[x]$.
- If $q_1$ is separable, then it must necessarily be irreducible since otherwise any factorization of $q_1(x) = f(x)g(x)$ would give a factorization of $q(x) = q_1(x^p) = f(x^p)g(x^p)$.
- Otherwise, if $q_1$ is inseparable, then by the argument above, we must have $q_1(x) = q_2(x^p)$ for some $q_2(x) \in F[x]$.
- By iterating this argument (formally, by a trivial induction), eventually we must obtain a polynomial $q_k(x)$ that is separable and irreducible. Then $q(x) = q_{\text{sep}}(x^{p^k})$ as claimed.

# Purely Inseparable Extensions, III

2. The element $\alpha \in K/F$ is purely inseparable if and only if there exists some positive integer $k$ such that $\alpha^{p^k} \in F$.

Proof:

- First suppose $\alpha$ is purely inseparable and let $m(x) \in F[x]$ be the minimal polynomial of $\alpha$ over $F$.
- Then $m(x)$ is an irreducible purely inseparable polynomial, so $m(x) = q_{\text{sep}}(x^{p^k})$ for some separable polynomial $q_{\text{sep}}$ by (1).
- If $q_{\text{sep}}$ had two distinct roots $r_1$ and $r_2$, then (in an appropriate splitting field) $m$ would have roots $s_1$ and $s_2$ satisfying $s_1^{p^k} = r_1$ and $s_2^{p^k} = r_2$.
- But since the $p$th-power map is injective and $r_1 \neq r_2$, this would mean that $s_1 \neq s_2$ and thus that $m$ has two distinct roots, contradicting the assumption that $m$ was purely inseparable.

# Purely Inseparable Extensions, IV

2. The element $\alpha \in K/F$ is purely inseparable if and only if there exists some positive integer $k$ such that $\alpha^{p^k} \in F$.

Proof (furthermore):

- Conversely, if $\alpha^{p^k} \in F$, then $\alpha$ is a root of the polynomial $q(x) = x^{p^k} - \alpha^{p^k} = (x - \alpha)^{p^k}$ in $K[x]$.
- Then the minimal polynomial of $\alpha$ over $F$ must therefore divide $q$, but since $q$ has only one root $\alpha$, that means $m$ also has only one root $\alpha$. Thus, $\alpha$ is purely inseparable.

Notice that this result shows that the examples we gave of inseparable elements above are essentially the only possible ones.

# Purely Inseparable Extensions, V

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 nonnegative integer $k$ and some $d \in F$.

Proof:

- The forward direction follows immediately from (2).
- The reverse direction follows from the observation above that $m_\alpha(x) = (x - \alpha)^{p^k}$ inside $K$, so $m_\alpha$ has only the single root $\alpha$.

# Purely Inseparable Extensions, VI

4. $K/F$ is purely inseparable if and only if $K/F$ is algebraic and the only elements of $K$ separable over $F$ are the elements of $F$.

Proof:

- If $K/F$ is purely inseparable, then by (3) any $\alpha \in K$ has minimal polynomial of the form $m_\alpha(x) = x^{p^k} - d = (x - \alpha)^{p^k}$ in $K$.
- Such a polynomial cannot be separable unless $k = 0$, in which case it has the form $m_\alpha(x) = x - d$, implying $\alpha \in F$.

This result is the reason for the terminology of "purely inseparable": all elements of the extension, other than the elements of the ground field $F$ themselves, are inseparable over $F$.

# Purely Inseparable Extensions, VII

4. $K/F$ is purely inseparable if and only if $K/F$ is algebraic and the only elements of $K$ separable over $F$ are the elements of $F$.

Proof (conversely):

- Conversely, suppose $K/F$ is algebraic and the only elements of $K$ separable over $F$ are the elements of $F$.
- For any $\alpha \in K$ consider its minimal polynomial $m(x)$, which by hypothesis must be inseparable.
- By (1), we have $m(x) = m_{\text{sep}}(x^{p^k})$ for some positive integer $k$, where $m_{\text{sep}}$ is separable.
- But then the minimal polynomial of $\alpha^{p^k}$ is $m_{\text{sep}}(x)$, which is separable. Therefore, $\alpha^{p^k}$ must be an element of $F$, and then $\alpha$ is purely inseparable by (2).

This result is the reason for the terminology of "purely inseparable": all elements of the extension, other than the elements of the ground field $F$ themselves, are inseparable over $F$.

# Purely Inseparable Extensions, VIII

5. $L/F$ is purely inseparable if and only if $L/K$ and $K/F$ are purely inseparable.

Proof (forwardly):

- If $L/F$ is purely inseparable, then by (2), for any $\alpha \in L\backslash F$ we have $\alpha^{p^k} \in F$ for some positive integer $k$.
- In particular this holds for any $\alpha \in K\backslash F$, so $K/F$ is purely inseparable.
- Furthermore, if $\alpha \in L\backslash F$ then since $\alpha^{p^k} \in F$ we have $\alpha^{p^k} \in K$, so $L/K$ is purely inseparable by (2).

# Purely Inseparable Extensions, IX

5. $L/F$ is purely inseparable if and only if $L/K$ and $K/F$ are purely inseparable.

Proof (reversely):

- Conversely, suppose $L/K$ and $K/F$ are purely inseparable.
- Then by (2), for any $\alpha \in L$ we have $\alpha^{p^{k_1}} \in K$ for some $k_1$, and also if $\beta = \alpha^{p^{k_1}}$ we have $\beta^{p^{k_2}} \in F$ for some $k_2$.
- But then $\alpha^{p^{k_1+k_2}} = \beta^{p^{k_1}} \in F$, so by (2) again, this means $\alpha$ is purely inseparable, so $L/F$ is purely inseparable.

# Purely Inseparable Extensions, X

6. The composite of purely inseparable extensions over $F$ is also purely inseparable over $F$.

Proof:

- Let $K$ be a composite of purely inseparable extensions of $F$.
- Then any $\gamma \in K$ is of the form $\gamma = \dfrac{p(\alpha_1, \dots, \alpha_i)}{q(\alpha_{i+1}, \dots, \alpha_{i+j})} \in K$ where $\alpha_1, \dots, \alpha_i, \alpha_{i+1}, \dots, \alpha_{i+j}$ are purely inseparable over $F$ and $p, q$ are polynomials with coefficients in $F$.
- By (2), there exist integers $k_1, \dots, k_{i+j}$ such that $\alpha_l^{p^{k_l}} \in F$ for each $1 \leq l \leq i+j$. If $M = \max(k_l)$, then $\alpha_l^{p^M} \in F$ for each $l$.
- Then $\gamma^{p^M}$ is a rational function with coefficients from $F$ in the elements $\alpha_l^{p^M} \in F$, so $\gamma^{p^M} \in F$.
- Hence by (2), $\gamma$ is purely inseparable over $F$, and so $K/F$ is purely inseparable.

# Purely Inseparable Extensions, XI

7. If $K/F$ has finite degree and $K = F(\alpha_1, \dots, \alpha_k)$, then $K/F$ is purely inseparable if and only if each $\alpha_i$ is purely inseparable over $F$.

Proof:

- If $K/F$ is purely inseparable, then by (5) each of the extensions $F(\alpha_i)$ is purely inseparable, so each $\alpha_i$ is inseparable.
- Conversely, if each of the $F(\alpha_i)$ is purely inseparable, then by (6) so is their composite field $K = F(\alpha_1, \dots, \alpha_k)$.

# Purely Inseparable Extensions, XII

8. Every finite-degree purely inseparable extension has degree equal to a power of $p$.

Proof:

- This follows from applying the degree tower formula to (7) and by noting that any simple purely inseparable extension has degree equal to a power of $p$ by (3).

# Purely Inseparable Extensions, XIII

In general, separability is nice, while inseparability can often be inconvenient.

- We frequently will want to discuss the various relations between roots of a particular irreducible polynomial.
- If some of the roots are the same, then we can end up with unintuitive behaviors when we pose questions that involve the set of roots, since the set will be smaller than we expect.
- The point of discussing purely inseparable extensions is to give you more of an idea of when and where inseparability can show up, and what happens when it does.

# Separable Extensions, I

We will now discuss separable extensions, which do tend to behave more nicely, but the actual proofs are rather complicated.

- In order to establish results about separable extensions, we will first need to discuss some results about embeddings of fields into their algebraic closures.

**Definition**

*If $K/F$ is an algebraic extension, an embedding of $K/F$ into $\overline{F}/F$ is an injective ring homomorphism $\sigma : K \to \overline{F}$ such that $\sigma$ fixes $F$ (i.e., $\sigma(x) = x$ for all $x \in F$).*

We call this an embedding because we can think of $\sigma$ as (essentially) "pasting" a copy of $K/F$ inside the algebraic closure $\overline{F}/F$.

# Separable Extensions, II

Example: Consider the algebraic extension $K/\mathbb{Q}$ where $K = \mathbb{Q}[x]/(x^2 - 2)$.

- An embedding of $K/\mathbb{Q}$ into $\overline{\mathbb{Q}}/\mathbb{Q}$ is completely determined by the image of $\overline{x}$.
- Since $\overline{x}^2 = 2$, applying $\sigma$ yields $\sigma(\overline{x})^2 = \sigma(2) = 2$ since $\sigma$ fixes $\mathbb{Q}$.
- This means $\overline{x}$ must be mapped either to $\sqrt{2}$ or to $-\sqrt{2}$.
- Both of these choices work, so we see that there are two embeddings of $K/\mathbb{Q}$ into $\overline{\mathbb{Q}}/\mathbb{Q}$. Note here that $x^2 - 2$ is irreducible and has degree 2: the possible embeddings correspond to the roots of the polynomial in $\overline{\mathbb{Q}}$.

# Separable Extensions, III

Example: Consider the algebraic extension $K/F$ where $F = \mathbb{F}_3(t)$ and $K = F[x]/(x^3 - t)$. (Morally, $K = F(t^{1/3})$, but I want to keep the notation the same as the last example.)

- An embedding of $K/F$ into $\overline{F}/F$ is, like in the last example, completely determined by the image of $\overline{x}$.
- Since $(\overline{x})^3 = t$, the image of $\overline{x}$ must be mapped to an element whose cube is $t$. But there is only one such element in $\overline{F}$, namely, $t^{1/3}$, since $x^3 - t = (x - t^{1/3})^3$ in $\overline{F}$.
- This means $\overline{x}$ must be mapped to $t^{1/3}$, and so there is only one possible embedding of $K/F$ into $\overline{F}/F$.
- Note here that the element $t^{1/3}$ is not separable, so although its degree over $F$ is 3, there is only 1 possible embedding.

# Separable Extensions, IV

As suggested by the examples, counting the number of embeddings of an extension into the algebraic closure give us a way to detect separability.

- This is the main engine behind the proofs we will give about separable extensions.
- The general idea is to show that the idea of the examples holds in general for simple extensions, and then to "bootstrap" to more complicated extensions.

# Separable Extensions, V

**Proposition (Properties of Separability, Part 1)**

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

1. *The algebraic element $\alpha$ 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 $\alpha$ is algebraic over $F$, then $\alpha$ 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.*

# Separable Extensions, VI

## Proposition (Properties of Separability, Part 2)

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

5. *If $K/F$ has finite degree, 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 $\alpha$ is separable over $K$ if and only if $\alpha$ is separable over $F$.*
7. *If $K/F$ has finite degree and $K = F(\alpha_1, \dots, \alpha_k)$, then $K/F$ is separable if and only if each $\alpha_i$ 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 Extensions, VII

1. The algebraic element $\alpha$ is separable over $F$ if and only if there are $[F(\alpha) : F]$ different embeddings of $F(\alpha)/F$ into $\overline{F}/F$.

Proof:

- Suppose $\alpha$ is separable over $F$, let its minimal polynomial be $m(x)$ of degree $n$, and let $L$ be the splitting field of $m$ over $F$.
- As in the examples, $\sigma(\alpha)$ must also be a root of $m(x)$ inside $\overline{F}$, since $m(\sigma(\alpha)) = \sigma(m(\alpha)) = \sigma(0) = 0$.
- Now let $\beta$ be any root of $m(x)$.
- By the theorem on the uniqueness of splitting fields, the identity map on $F$ extends to an isomorphism of $L$ with itself that maps $\alpha$ to $\beta$, since the identity map sends the minimal polynomial of $\alpha$ to the minimal polynomial of $\beta$ (since they have the same minimal polynomial $m(x)$).

# Separable Extensions, VIII

1. The algebraic element $\alpha$ is separable over $F$ if and only if there are $[F(\alpha) : F]$ different embeddings of $F(\alpha)/F$ into $\overline{F}/F$.

Proof:

- Restricting this isomorphism to $F(\alpha)$ yields an embedding of $F(\alpha)$ into $\overline{F}$ whose image is $F(\beta)$.
- Since any map $\sigma : F(\alpha) \to \overline{F}$ fixing $F$ is completely determined by the value of $\sigma(\alpha)$, we see that this correspondence yields a bijection between embeddings of $F(\alpha)/F$ into $\overline{F}/F$ with the distinct roots $\beta$ of $m(x)$.
- The result then follows immediately, since $\alpha$ is separable if and only if $m(x)$ has $\deg(m) = [F(\alpha) : F]$ distinct roots.

# Separable Extensions, IX

2. If $K/F$ has finite degree, then there are at most $[K : F]$ different embeddings of $K/F$ into $\overline{F}/F$.

Proof:

- Induct on the number $n$ of generators of $K/F$.
- The case $n = 1$, where $K = F(\alpha_1)$, was shown in (1), since in this situation the embeddings are in bijection with the distinct roots of the minimal polynomial $m$ of the generator $\alpha_1$, and the number of such roots is bounded above by the degree of $m$, which equals $[K : F]$ in this case.

# Separable Extensions, X

2. If $K/F$ has finite degree, then there are at most $[K:F]$ different embeddings of $K/F$ into $\overline{F}/F$.

Proof:

- For the inductive step, suppose the result holds for extensions having $k$ generators and suppose $K = F(\alpha_1, \ldots, \alpha_{k+1})$, and set $E = F(\alpha_1, \ldots, \alpha_k)$, so that $K = E(\alpha_{k+1})$.
- Then any embedding of $K/F$ into $\overline{E} = \overline{F}$ is determined by the image of $E$, which has at most $[E:F]$ possible choices by the induction hypothesis, and the image of $\alpha_{k+1}$, which has at most $[K:E]$, the degree of the minimal polynomial of $\alpha_{k+1}$ over $E$, possible choices once the image of $E$ is determined.
- Therefore, the number of embeddings is at most $[K:E] \cdot [E:F] = [K:F]$, as claimed.

# Separable Extensions, XI

3. If $\alpha$ is algebraic over $F$, then $\alpha$ is separable over $F$ if and only if $F(\alpha)$ is separable over $F$.

<u>Proof</u>:

- Trivially, if $F(\alpha)/F$ is separable then $\alpha$ is separable over $F$.
- Now suppose $\alpha$ is separable over $F$ and suppose there were an inseparable element $\beta \in F(\alpha)$.
- Then by (1), the number $n_{F(\beta)/F}$ of embeddings of $F(\beta)/F$ is strictly less than $[F(\beta) : F]$.
- Also, by (2), the number of embeddings $n_{F(\alpha)/F(\beta)}$ of $F(\alpha)/F(\beta)$ into $\overline{F(\beta)} = \overline{F}$ is at most $[F(\alpha) : F(\beta)]$.
- Therefore, since any embedding of $F(\alpha)/F$ is determined uniquely by the embeddings of $F(\beta)/F$ and $F(\alpha)/F(\beta)$, the number of embeddings $n_{F(\alpha)/F}$ of $F(\alpha)/F$ is at most $n_{F(\alpha)/F(\beta)} \cdot n_{F(\beta)/F} < [F(\alpha) : F(\beta)] \cdot [F(\beta) : F] = [F(\alpha) : F]$.
- But since $F(\alpha)/F$ is separable, (1) gives a contradiction.

# Separable Extensions, XII

4. If $L/F$ is separable, then $L/K$ and $K/F$ are separable.

Proof:

- First suppose that $L/F$ is separable, so that every element of $L$ is separable over $F$. Then because $K$ is a subset of $L$, this means every element of $K$ is separable over $F$, so $K/F$ is separable.
- Furthermore, for any $\alpha \in L$, if $m_F(x)$ is the minimal polynomial of $\alpha$ over $F$, then the minimal polynomial $m_K(x)$ of $\alpha$ over $K$ divides it, since $m_F(\alpha) = 0$ in $K$.
- All roots of $m_F(x)$ are distinct since $\alpha$ is separable, so all roots of $m_K(x)$ are also distinct. Thus, $L/K$ is separable.

We will show the converse is true in a bit.

# Separable Extensions, XIII

5. If $K/F$ has finite degree, then $K/F$ is separable if and only if there are exactly $[K:F]$ different embeddings of $K/F$ into $\overline{F}/F$.

Proof (directly):

- Let $K = F(\alpha_1, \dots, \alpha_k)$ and $E_i = F(\alpha_1, \dots, \alpha_i)$ for $0 \leq i \leq k$.
- By (2), the total number of different embeddings of $K/F$ into $\overline{F}/F$ is at most $[K:F]$ by (2).
- If $K$ is separable, then by (4), each subextension $E(\alpha_{i+1})/E$ is separable, and then by (3), the argument in (1), and a trivial induction, this means the number of embeddings of $E(\alpha_{i+1})/F$ into $\overline{F}/F$ is $[E(\alpha_{i+1}) : E] \cdot [E:F] = [E(\alpha_{i+1}) : F]$, since each embedding of $E(\alpha_{i+1})/F$ is realized by an embedding of $E/F$ along with an embedding of $E(\alpha_{i+1})/E$.
- Thus, taking $i = k$ yields that the number of embeddings of $K/F$ into $\overline{F}/F$ is equal to $[K:F]$, as required.

# Separable Extensions, XIV

5. If $K/F$ has finite degree, then $K/F$ is separable if and only if there are exactly $[K : F]$ different embeddings of $K/F$ into $\overline{F}/F$.

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

- Inversely, if $K$ is not separable, then it contains some inseparable element $\beta$.
- Then $F(\beta)/F$ has fewer than $[F(\beta) : F]$ embeddings into $\overline{F}/F$ by (1).
- Since the number of embeddings of $K/F(\beta)$ is at most $[K : F(\beta)]$ by (2), by the same argument as on the previous slide, the total number of embeddings of $K/F$ into $\overline{F}$ is strictly fewer than $[K : F(\beta)] \cdot [F(\beta) : F] = [K : F]$.

# Separable Extensions, XV

6. If $K/F$ is separable, then $\alpha$ is separable over $K$ if and only if $\alpha$ is separable over $F$.

Proof (finite-degree case):

- First suppose $[K : F] < \infty$ and $\alpha$ is separable over $K$. Consider the tower $K(\alpha)/K/F$.
- By (3), $K(\alpha)/K$ is separable, and then by (5), the number of embeddings of $K(\alpha)/K$ into $\overline{K} = \overline{F}$ is equal to $[K(\alpha) : K]$. Also by (5), there are $[K : F]$ embeddings of $K/F$ into $\overline{F}$.
- Furthermore, it is easy to see by composing the appropriate maps that if we have an embedding of $K/F$ into $\overline{F}$ and an embedding of $K(\alpha)/K$ into $\overline{K} = \overline{F}$, then it yields a unique embedding of $K(\alpha)/F$ into $\overline{F}$.
- Therefore, the total number of embeddings of $K(\alpha)/F$ into $\overline{F}$ equals $[K(\alpha) : K] \cdot [K : F] = [K(\alpha) : F]$. Then by (5) again, $K(\alpha)/F$ is separable, so $\alpha$ is separable over $F$.

# Separable Extensions, XVI

6. If $K/F$ is separable, then $\alpha$ is separable over $K$ if and only if $\alpha$ is separable over $F$.

Proof (general case):

- The general case follows from the finite-degree case.
- Specifically, if the minimal polynomial for $\alpha$ over $K$ is $m(x) = b_d x^d + \cdots + b_0$ for $b_i \in K$, then $\alpha$ is separable over $F(b_0, \dots, b_d)$ since it is separable over $K$.
- The point is that $\alpha$ has the same minimal polynomial over both fields, but now $F(b_0, \dots, b_d)/F$ has finite degree since it is algebraic over $F$ with finitely many generators.
- The converse direction is trivial, since if $\alpha$ is separable over $F$ then by the argument in (4), it is separable over $K$.

# Separable Extensions, XVII

7. If $K/F$ has finite degree and $K = F(\alpha_1, \dots, \alpha_k)$, then $K/F$ is separable if and only if each $\alpha_i$ is separable over $F$.

- Proof: This follows by repeatedly applying (6) to the tower $K/F(\alpha_1, \dots, \alpha_{k-1})/\cdots/F(\alpha_1)/F$.

8. If $L/K$ and $K/F$ are separable, then $L/F$ is separable.

- Proof: If $L/K$ has finite degree then this follows by writing $L = K(\alpha_1, \dots, \alpha_k)$ and applying (7).
- The general case follows from the finite-degree case because for each $\alpha \in L$, $\alpha$ is separable over $F$ if and only if $K(\alpha)/F$ is separable over $L$ by (3).

# Separable Extensions, XVIII

9. The composite of separable extensions is separable.

- If the extensions have finite degree then this follows from (7) by writing $K_1 = F(\alpha_1, \dots, \alpha_k)$ and $K_2 = F(\beta_1, \dots, \beta_l)$ and noting that $K_1 K_2 = F(\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_l)$.
- The general case follows from the finite-degree case since any element of a composite extension is a rational function in finitely many elements from the given fields.

# Separable Extensions: Finally, We're Done

Okay, so all of that was a technical slog, but now we can basically forget everything about the annoying proofs and just remember the results. Enjoy the long weekend!

Specifically, this is intended as a reminder that there is no class next Monday, October 12th, as it is a university holiday. I will not be holding office hours that day, as well.

# Summary

We used our results on separability to prove some results about finite fields.

We discussed separability and inseparability for field extensions.

Next lecture: Separable and inseparable degrees, transcendental extensions.