Math 5111 (Algebra 1)

Lecture #8 $\sim$ October 5th, 2020

Splitting Fields + Algebraic Closures

- Splitting Fields, part 2
- Algebraic Closures
- Separability, part 1

This material represents §2.3.2-2.4.1 from the course notes.

More Splitting Fields, I

Recall our definition of a splitting field from last time:

Definition

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

As we noted, K is a splitting field for p if and only if $K = F(r_1, \dots, r_n)$ where the r_i are the roots of $p(x)$ in K.

We also proved that splitting fields always exist and are unique up to isomorphism.

More Splitting Fields, II

We also introduced cyclotomic fields last time:

Definition

The splitting field $\mathbb{Q}(\zeta_n)$ of $p(x) = x^n - 1$ over $\mathbb{Q}$ is called the cyclotomic field of nth roots of unity.

Here, ζ_n represents a primitive nth root of unity. One possible choice is $\zeta_n = e^{2\pi i/n} = \cos(2\pi/n) + i\sin(2\pi/n)$.

Cyclotomic fields show up very naturally when looking at field extensions obtained by taking nth roots.

More Splitting Fields, III

It is a nontrivial problem to compute the degree $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$, which is equivalent to determining the degree of the minimal polynomial of ζ_n over $\mathbb{Q}$.

- For some small values of n this is not so hard to do explicitly, since we just have to find the factorization of $x^n - 1$ over $\mathbb{Q}$.
- The easiest way to compute the roots is to use Euler's identity (which of course requires remembering basic trigonometry): the roots of $x^n - 1$ are $\zeta_n^k = \cos(2\pi k/n) + i \sin(2\pi k/n)$.

$n = 2$: $x^2 - 1 = (x-1)(x+1)$, with degree 1 over $\mathbb{Q}$.

$n = 3$: $x^3 - 1 = (x-1)(x^2+x+1)$.

The roots are 1 and $\dfrac{-1 \pm i\sqrt{3}}{2}$. The splitting field has degree 2.

$n = 4$: $x^4 - 1 = (x-1)(x+1)(x^2+1)$.

The roots are 1, -1, i, and $-i$. The splitting field has degree 2.

More Splitting Fields, IV

$n = 5$: $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$.

Here is the first case where it is not so clear what the degree is. In fact, the second polynomial is irreducible over $\mathbb{Q}$ (it does not have any roots nor does it factor as a product of quadratics). By setting $y = x + 1/x$ one can obtain a quadratic for y and solve it to see that the roots are 1, $\dfrac{-1+\sqrt{5} \pm i\sqrt{10+2\sqrt{5}}}{4}$ and $\dfrac{-1-\sqrt{5} \pm i\sqrt{10-2\sqrt{5}}}{4}$. The splitting field has degree 4.

$n = 6$: $x^6 - 1 = (x-1)(x+1)(x^2 + x + 1)(x^2 - x + 1)$.

The roots are 1, -1, and $\dfrac{\pm 1 \pm i\sqrt{3}}{2}$ for all four possible choices of the ± signs. The splitting field has degree 2.

More Splitting Fields, V

$n = 7$: $x^7 - 1 = (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$.
Again, it turns out that the second factor is irreducible (though of course this is even more unpleasant than in the case $n = 5$ to prove directly), so the splitting field has degree 6.

$n = 8$: $x^8 - 1 = (x-1)(x+1)(x^2+1)(x^4+1)$.
The roots are 1, -1, $\pm i$, and $\dfrac{\pm 1 \pm i}{\sqrt{2}}$, for all four choices of sign. The splitting field is $\mathbb{Q}(i, \sqrt{2})$ and has degree 4.

$n = 9$: $x^9 - 1 = (x-1)(x^2+x+1)(x^6+x^3+1)$.
It can be shown that the degree-6 polynomial is irreducible, and so the splitting field has degree 6.

More Splitting Fields, VI

In the case where $n = p$ is a prime, however, we can compute the degree of the splitting field now:

Proposition (Prime Cyclotomic Fields)

If p is a prime, the degree $[\mathbb{Q}(\zeta_p) : \mathbb{Q}]$ is equal to $p - 1$.

The idea is to show that $\dfrac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible.

More Splitting Fields, VII

Proof:

- As noted above, the degree $[\mathbb{Q}(\zeta_p) : \mathbb{Q}]$ is equal to the degree of the minimal polynomial of ζ_p over $\mathbb{Q}$.
- Since $\zeta_p \neq 1$, and since $x - 1$ divides $x^p - 1$, by the factor theorem we see that ζ_p is a root of the polynomial $\Phi_p(x) = \dfrac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$.
- We claim that $\Phi_p(x)$ is irreducible over $\mathbb{Q}$, and is therefore the minimal polynomial of ζ_p.
- To show this, first observe that $\Phi_p(x)$ is irreducible if and only if $\Phi_p(x + 1)$ is irreducible (since any factorization $\Phi_p(x + 1) = a(x)b(x)$ would yield a factorization $\Phi_p(x) = a(x - 1)b(x - 1)$ and vice versa).

More Splitting Fields, VIII

Proof (continuedly):

- Then $\Phi_p(x+1) = \dfrac{(x+1)^p - 1}{(x+1) - 1} = \dfrac{1}{x} \cdot \displaystyle\sum_{k=1}^{p} \binom{p}{k} x^k =$ $\displaystyle\sum_{k=1}^{p} \binom{p}{k} x^{k-1} = x^{p-1} + px^{p-2} + \cdots + p$.
- Each of the binomial coefficients $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ with $0 < k < p$ is divisible by p (since there is a p in the numerator but not the denominator) and the constant term of $\Phi_p(x+1)$ is not divisible by p^2.
- Thus, $\Phi_p(x+1)$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion (with prime p), and so $\Phi_p(x)$ is also irreducible over $\mathbb{Q}$.
- Therefore, $\Phi_p(x)$ is the minimal polynomial of ζ_p, and $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \deg \Phi_p = p - 1$.

More Splitting Fields, IX

Example: If p is a prime, find the splitting field K for $q(x) = x^p - 3$ over $\mathbb{Q}$ and compute the degree $[K : \mathbb{Q}]$.

More Splitting Fields, IX

Example: If p is a prime, find the splitting field K for $q(x) = x^p - 3$ over $\mathbb{Q}$ and compute the degree $[K : \mathbb{Q}]$.

- We begin by observing that the roots of $q(x)$ in $\mathbb{C}$ are $\zeta_p^k \cdot \sqrt[p]{3}$ for $0 \leq k \leq p-1$, since each of these is a root of q and they are all distinct. (Here, as elsewhere, $\sqrt[p]{3}$ represents the real pth root of 3.)
- Therefore, the splitting field for p over $\mathbb{Q}$ is $K = \mathbb{Q}(\sqrt[p]{3}, \zeta_p\sqrt[p]{3}, \dots, \zeta_p^{p-1}\sqrt[p]{3}) = \mathbb{Q}(\sqrt[p]{3}, \zeta_p)$, since both fields contains the generators for the other.

More Splitting Fields, X

Example: If p is a prime, find the splitting field K for $q(x) = x^p - 3$ over $\mathbb{Q}$ and compute the degree $[K : \mathbb{Q}]$.

- Notice that K is the composite of the fields $E = \mathbb{Q}(\sqrt[p]{3})$ and $F = \mathbb{Q}(\zeta_p)$, and so $[K : \mathbb{Q}] \leq [E : \mathbb{Q}] \cdot [F : \mathbb{Q}]$.
- We showed that $[F : \mathbb{Q}] = p - 1$ above, and for $[E : \mathbb{Q}]$, because $x^p - 3$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion (with prime 3), $x^p - 3$ is necessarily the minimal polynomial of $\sqrt[p]{3}$, so $[\mathbb{Q}(\sqrt[p]{3}) : \mathbb{Q}] = p$.
- Therefore, $[K : \mathbb{Q}] \leq p(p - 1)$.
- However, since E and F are both subfields of K, $[K : \mathbb{Q}]$ is divisible by both $[E : \mathbb{Q}] = p$ and $[F : \mathbb{Q}] = p - 1$, and thus (since they are relatively prime) by their product. We must therefore have equality, meaning that $[K : \mathbb{Q}] = p(p - 1)$.

More Splitting Fields, XI

Example: If p is a prime, find the splitting field K for $q(x) = x^p - 3$ over $\mathbb{Q}$ and compute the degree $[K : \mathbb{Q}]$.

- We can glean some non-obvious facts from this calculation $[K : \mathbb{Q}] \le p(p-1)$.
- For example, because K/E has degree $p-1$ and is generated by ζ_p (which is a root of the degree-$(p-1)$ polynomial $\Phi_p(x) \in \mathbb{Q}[x]$), we see in fact that $\Phi_p(x)$ is irreducible over $\mathbb{Q}(\sqrt[p]{3})$.
- By the same reasoning, we can also deduce that $x^p - 3$ is irreducible over $\mathbb{Q}(\zeta_p)$.

More Splitting Fields, XII

Example: Find the splitting field K for $p(x) = x^8 - 2$ over $\mathbb{Q}$ and compute the degree $[K : \mathbb{Q}]$.

More Splitting Fields, XII

Example: Find the splitting field K for $p(x) = x^8 - 2$ over $\mathbb{Q}$ and compute the degree $[K : \mathbb{Q}]$.

- As in the previous example, we can see that the roots of $p(x)$ in $\mathbb{C}$ are $\zeta_8^k \cdot \sqrt[8]{2}$ for $0 \leq k \leq 7$.
- Therefore, the splitting field for p over $\mathbb{Q}$ is $K = \mathbb{Q}(\sqrt[8]{2}, \zeta_8\sqrt[8]{2}, \dots, \zeta_8^7\sqrt[8]{2}) = \mathbb{Q}(\sqrt[8]{2}, \zeta_8)$, since both fields contains the generators for the other.
- We can compute (in fact, I did earlier!) that $\zeta_8 = \cos(2\pi/8) + i\sin(2\pi/8) = \sqrt{2}/2 + i\sqrt{2}/2$, and so since $\sqrt{2} = (\sqrt[8]{2})^4$, we see that K contains $\sqrt{2} \cdot \zeta_8 - 1 = i$.
- Then, since K contains i and $\sqrt[8]{2}$, and because $\mathbb{Q}(\sqrt[8]{2}, i)$ contains the generators of K, we in fact have $K = \mathbb{Q}(\sqrt[8]{2}, i)$.

More Splitting Fields, XIII

Example: Find the splitting field K for $p(x) = x^8 - 2$ over $\mathbb{Q}$ and compute the degree $[K : \mathbb{Q}]$.

- By the multiplicativity of field degrees, $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[8]{2})] \cdot [\mathbb{Q}(\sqrt[8]{2}) : \mathbb{Q}]$.
- Because $x^8 - 2$ is irreducible over $\mathbb{Q}$, it is necessarily the minimal polynomial of $\sqrt[8]{2}$, and so $[\mathbb{Q}(\sqrt[8]{2}) : \mathbb{Q}] = 8$.
- To compute $[K : \mathbb{Q}(\sqrt[8]{2})]$, notice that $\mathbb{Q}(\sqrt[8]{2})$ is a subfield of $\mathbb{R}$ but K is not, since it contains the nonreal number i.
- On the other hand, since $K/\mathbb{Q}(\sqrt[8]{2})$ is generated by i, the extension degree is at most the degree of the minimal polynomial of i over $\mathbb{Q}$, which is 2.
- Thus, the only possibility is to have $[K : \mathbb{Q}(\sqrt[8]{2})] = 2$, and so $[K : \mathbb{Q}] = 16$.

More Splitting Fields, XIV

Example: Find the splitting field K for $p(x) = x^8 - 2$ over $\mathbb{Q}$ and compute the degree $[K : \mathbb{Q}]$.

- If we simply tried to reproduce the same argument given in the example for $x^p - 3$, we would first proceed by noting that $K = \mathbb{Q}(2^{1/8}, \zeta_8)$.
- Then we would compute $\mathbb{Q}(2^{1/8}) = 8$ and $\mathbb{Q}(\zeta_8) = 4$, since the respective minimal polynomials are $x^8 - 2$ and $x^4 + 1$.
- However, this information by itself only implies that $[K : \mathbb{Q}]$ is 8, 16, or 32. We can eliminate 8 by noting that $\zeta_8 \notin \mathbb{R}$.
- In order to show that the degree is 16 and not 32, we would have to identify an algebraic relation between ζ_8 and $2^{1/8}$.
- It is perhaps not so obvious how to do this, but one such relation is $\zeta_8 + \zeta_8^7 = \sqrt{2} = (2^{1/8})^4$.
- The point is that the information we can deduce depends a lot on what generators we select.

Algebraic Closures, I

As we have shown, for any polynomial $p \in F[x]$, there exists a field extension K/F with the property that K contains all of the roots of p.

- A natural extension of this question is: does there exist a field extension K/F with the property that K contains all of the roots of *every* polynomial $p \in F[x]$?
- One example of such an extension is $\mathbb{C}/\mathbb{R}$, since every polynomial in $\mathbb{R}[x]$ splits completely over $\mathbb{C}$. (This statement is really just a rephrasing of the fundamental theorem of algebra.)
- Given an arbitrary field F, we would like to construct an analogous extension that contains all of the roots of all polynomials in $F[x]$: this extension represents the closure of F under algebraic operations (i.e., solving polynomials) and is called the algebraic closure of F.

Algebraic Closures, II

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 $\overline{F}$.

This is a perfectly reasonable definition, of course, but it is not clear that F must actually have an algebraic closure, nor whether algebraic closures are necessarily unique.

It does seem fairly reasonable to think that such an extension would exist (since we may construct towers of extensions having roots of more and more polynomials of larger and larger degrees), but in fact this question is substantially more delicate than it might seem.

Algebraic Closures, III

Intuitively, we would like to think of the algebraic closure of F as the composite of all of the splitting fields of the polynomials in $F[x]$.

- However, the composite of two arbitrary fields is not defined: we have only defined the composite of two subfields of a larger field.
- Thus, saying that the algebraic closure is "the composite of all of the splitting fields" presupposes the existence of some larger field that contains all of these splitting fields, and this is entirely circular since this larger field is precisely what the algebraic closure would be!

Algebraic Closures, IV

Let us instead examine another feature of $\mathbb{C}$: not only is it the algebraic closure of $\mathbb{R}$, it is the algebraic closure of itself.

- This follows by the observation that every polynomial in $\mathbb{C}[x]$ splits completely over $\mathbb{C}$ (which is, again, simply the fundamental theorem of algebra).
- This tells us that $\mathbb{C}$ has no nontrivial algebraic extensions: if $L/\mathbb{C}$ were an algebraic extension, any element $\alpha \in L$ would be a root of its minimal polynomial in $\mathbb{C}[x]$, but the only irreducible polynomials in $\mathbb{C}[x]$ are linear polynomials.

Algebraic Closures, V

In other words, $\mathbb{C}$ is “algebraically closed”:

Definition

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

- By the factor theorem and a trivial induction, if every polynomial in $F[x]$ has a root in F, then in fact it must split completely over F.
- Equivalently, by the same logic as given above for $\mathbb{C}$, a field is algebraically closed whenever it has no nontrivial algebraic extensions.

Algebraic Closures, VI

Based on the similarity of the names, and the fact that $\mathbb{C}$ is both an algebraic closure (namely, of $\mathbb{R}$) and is itself algebraically closed, it is reasonable to guess that algebraic closures are algebraically closed. This is in fact true:

Proposition (Algebraic Closures are Algebraically Closed)

If F is any field, then any algebraic closure $\overline{F}$ is algebraically closed. Symbolically, $\overline{\overline{F}} = \overline{F}$.

Algebraic Closures, VII

Proof:

- Suppose that $p(x) \in \overline{F}[x]$ is a polynomial and α is any root of $p(x)$ in $\overline{\overline{F}}$. Then $\overline{F}(\alpha)$ is an algebraic extension of $\overline{F}$, and $\overline{F}$ is an algebraic extension of F.
- We have previously shown that an algebraic extension of an algebraic extension is algebraic, so applying it to $\overline{F}(\alpha)/\overline{F}$ and $\overline{F}/F$ shows that $\overline{F}(\alpha)/F$ is algebraic, which is to say, α is algebraic over F.
- But since $\overline{F}$ contains all elements algebraic over F, we see $\alpha \in \overline{F}$, so $\overline{\overline{F}} = \overline{F}$.

Algebraic Closures, VIII

It is not so clear how we can actually try to establish the existence of algebraic closures, but the issues are very similar those we had with splitting fields.

- Our construction of the splitting field for $p(x)$ over F proceeded by adjoining the roots of p one at a time, using the quotient ring $F[x]/(q)$ for an irreducible factor q.
- To construct an algebraic closure, we could try the same thing: just start iteratively extending by taking splitting fields of polynomials, one at a time, and continue doing this until we have exhausted all polynomials in $F[x]$.
- Unfortunately, there are infinitely many polynomials in $F[x]$, perhaps even uncountably many.
- However, there does not seem to be any obvious obstruction to an approach of this form. This is precisely the kind of situation where Zorn's lemma comes in handy.

Algebraic Closures, IX

Our strategy for showing that every field F has an algebraic closure is to show that F is a subfield of an algebraically closed field L, and we will accomplish this using Zorn's lemma.

- If we can show the above, then the subfield of L consisting of all elements algebraic over F is then an algebraic closure of F. (Recall that we showed previously that the collection of all algebraic elements is a subfield.)

Theorem (Algebraic Closures)

If F is a field, then F is a subfield of an algebraically closed field.

The approach here, which was first given by Artin, is to use polynomial rings to do the necessary bookkeeping.

Algebraic Closures, X

Proof:

- First observe that in any commutative ring R with 1, if I is any proper ideal of R, then there exists a maximal ideal M of R containing I.
- This fact is a consequence of Zorn's lemma, and is a mild generalization of a problem from last week's homework (to show that any ring with 1 has a maximal ideal).
- We also require another important fact about maximal ideals in commutative rings; namely, that if M is maximal then R/M is a field. (This is in fact an if-and-only-if.)
- This follows immediately from the fourth isomorphism theorem: there is a bijection between ideals of R containing I and ideals of R/I, so since R/I is a field if and only if its only ideals are 0 and R/I, that means R/I is a field if and only if the only ideals of R containing I are I and R.

Algebraic Closures, XI

Proof (more):

- Now take R to be a polynomial ring in infinitely many variables X_f, indexed by the polynomials $f(x) \in F[x]$ of positive degree. (The elements of R are the polynomials involving finitely many of the X_f, with coefficients from F.)
- Let I be the smallest ideal of R containing all of the elements $f_i(X_{f_i})$, for each polynomial $f_i \in F[x]$ of positive degree.
- Then I is a proper ideal of R, because if not, 1 would be an element of I and so there would exist a relation of the form $r_1 f_1(X_{f_1}) + r_2 f_2(X_{f_2}) + \cdots + r_n f_n(X_{f_n}) = 1$ for some irreducible $f_i \in F[x]$ of positive degree and some elements $r_i \in R$. If we take K to be the splitting field of $f_1 f_2 \cdots f_n$ and choose a root $\alpha_i \in K$ of each f_i, then evaluating both sides of this relation at $X_{f_1} = \alpha_1$, ... , $X_{f_n} = \alpha_n$ yields $0 = 1$, which is impossible.

Algebraic Closures, XII

Proof (morer):

- Thus, I is a proper ideal of R so it is contained in some maximal ideal M.
- The quotient ring $L = R/M$ is then a field.
- We can view this field as an extension of F, since F embeds in L as the images of the constant polynomials.
- Every polynomial $f(x) \in F[x]$ of positive degree then has a root in L since $f(\overline{X_f}) = \overline{0}$ in the quotient ring (this is because $f(X_f) \in M$ since it is in I).
- Unfortunately. this is not quite enough to say that L is algebraically closed: although every polynomial in $F[x]$ now has a root in L, there may exist polynomials in $L[x]$ having no roots in L.

Algebraic Closures, XIII

Proof (morerer):

- To deal with this issue, we iterate the construction to obtain an infinite sequence of fields $F \subseteq L_1 \subseteq L_2 \subseteq L_3 \subseteq \cdots$, where every polynomial in $L_i[x]$ has at least one root in L_{i+1}.
- We may then take the union of this infinite sequence of fields (technically, we actually take a colimit, because this collection of fields is not naturally a subset of any particular set we have identified) to obtain a set $\overline{F}$.
- By essentially the same argument as from homework 1, the union of an ascending chain of fields is a field, so $\overline{F}$ is a field.
- Each element of $\overline{F}$ is contained in some L_i, so any polynomial with coefficients from $\overline{F}$ has all its coefficients from some L_i, and this polynomial has a root in L_{i+1} (hence in $\overline{F}$).
- Thus, this colimit field $\overline{F}$ is algebraically closed, meaning that F embeds into an algebraically closed field, as claimed.

Algebraic Closures, XIV

We can now deduce the existence of algebraic closures, as promised:

Corollary (Existence of Algebraic Closures)

If F is a field, then there exists an algebraic closure $\overline{F}$ of F. Furthermore, the algebraic closure $\overline{F}$ is unique up to isomorphism.

Proof:

- By the previous theorem, F is a subfield of an algebraically closed field L. Then the collection of all elements of L that are algebraic over F is a subfield of L, and is an algebraic closure of F.
- For the uniqueness, one may use an argument similar to the one we used to establish that splitting fields are unique up to isomorphism.

Algebraic Closures, XV

Proof (semi-continued):

- More explicitly, by a similar argument as used for splitting fields (along with an invocation of Zorn's lemma), one may show that if K/F is algebraic and L/K is also algebraic, then there exists an embedding of K into $\overline{F}$, and an embedding extending this one that embeds L into $\overline{F}$. (By "an embedding of E into F" we mean a map that is an isomorphism of E with a subfield of F.)
- Now suppose that E_1 and E_2 are both algebraic closures of F.
- By applying the above observation, we obtain an embedding of E_1 into E_2, and so E_1 is isomorphic to a subfield of E_2.
- But then E_2 is an algebraic extension of (a field isomorphic to) E_1, but E_1 has no nontrivial algebraic extensions: thus, the embedding of E_1 into E_2 is actually an isomorphism.

Algebraic Closures, XVI

The existence of algebraic closures is very useful, because it allows us (in essentially any situation) to make any of our general calculations with field extensions more concrete.

- For example, since $\mathbb{C}$ is algebraically closed by the fundamental theorem of algebra, by the argument above it contains an algebraic closure of any of its subfields.
- In particular, this means that we can always view any question about algebraic extensions of $\mathbb{Q}$ as taking place inside of $\mathbb{C}$ (as, in fact, we have already implicitly been doing).
- Furthermore, we also see that the set $\overline{\mathbb{Q}}$ of elements of $\mathbb{C}$ that are algebraic over $\mathbb{Q}$ is an algebraically closed field.

Separability, I

As we have shown, for any field F and any polynomial $p \in F[x]$, there exists an extension field K/F that contains all the roots of p.

- In many cases, the roots of a polynomial will be distinct. However, there certainly exist cases in which polynomials have "repeated roots", such as $p(x) = x^3$ or $p(x) = x^2(x-1)^2$.
- None of these polynomials is irreducible, and it is difficult (and as we will explain, with good reason!) to find examples of irreducible polynomials with repeated roots.

Separability, II

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 <u>multiplicity</u> of r_i.
Furthermore, r_i is a <u>simple root</u> if $d_i = 1$, and is a <u>repeated root</u> (or <u>multiple root</u>) if $d_i \geq 2$.
If all of the roots of q are simple, then we say q is <u>separable</u>, and otherwise q is <u>inseparable</u>.

To emphasize, a separable polynomial is one that has no repeated roots (we often phrase this as saying the polynomial has "distinct roots"), while an inseparable polynomial has a repeated root.

Separability, III

Examples:

1. The polynomial $x^2(x-1)^2(x^2+1)$ has two repeated roots (0 and 1) and two simple roots (i and $-i$) over $\mathbb{Q}$, and is inseparable.
2. The polynomial x^3+4x has three simple roots (0, $2i$, and $-2i$) over $\mathbb{Q}$, and is separable.
3. Over $F = \mathbb{F}_2(t)$, the field of rational functions in t with coefficients in $\mathbb{F}_2$, the polynomial $q(x) = x^2 - t$ is irreducible (it has no roots in F since there is no rational function whose square is t). Nonetheless, q has a repeated root $t^{1/2}$, because in its splitting field the polynomial $q(x)$ factors as $q(x) = (x - t^{1/2})^2$, and so q is inseparable. The root $t^{1/2}$ of $q(x)$ is a repeated root.

Separability, III

Examples:

4. Over $F = \mathbb{F}_3(t)$, the polynomial $q(x) = x^6 - t$ is irreducible: this is not so easy to see directly, but we can also use Eisenstein's criterion here with the "prime" equal to t. (If you like, you can go through the details of proving Eisenstein's criterion for polynomials with coefficients from $F[t]$.)
   Inside its splitting field, we can factor this polynomial as $q(x) = (x - t^{1/6})^3(x + t^{1/6})^3$, so q is inseparable since it has two repeated roots $t^{1/6}$ and $-t^{1/6}$.

Separability, IV

As a first goal, we can give a necessary condition for when a polynomial has repeated roots.

- Recall from calculus that we can test whether a polynomial has a double root at r by testing whether $q(r) = q'(r) = 0$. By the factor theorem, this is equivalent to saying that q and q' are both divisible by $x - r$.
- We can formulate a similar test over any field, since we may give a purely algebraic definition of the derivative. (In fact, you saw one way of doing this on homework 1.)

Separability, V

Definition

If $q(x) = \sum_{k=0}^{n} a_k x^k$ *is a polynomial in* $F[x]$*, its* ***derivative*** *is the polynomial* $q'(x) = \sum_{k=0}^{n} k a_k x^{k-1}$.

The standard differentiation rules apply:
$(f+g)'(x) = f'(x) + g'(x)$ and $(fg)'(x) = f'(x)g(x) + f(x)g'(x)$.
(These are now just calculations.)

Examples:

- In $\mathbb{C}[x]$, the derivative of $x^6 - 4x^2 + x$ is $6x^5 - 8x + 1$.
- In $\mathbb{F}_p[x]$, the derivative of $x^{p^2} - x$ is $p^2 x^{p^2-1} - 1 = -1$. Notice here that although the degree of the original polynomial is p^2, the degree of its derivative is 0.

Separability, VI

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 $F[x]$.

Separability, VII

Proof:

- First suppose $q(x)$ has a repeated root r in some extension K/F: then $q(x) = (x-r)^2 s(x)$ for some $s(x) \in K[x]$.
- Taking the derivative yields $q'(x) = 2(x-r)s(x) + (x-r)^2 s'(x) = (x-r) \cdot [2s(x) + (x-r)s'(x)]$.
- Thus, q' is also divisible by $x - r$ in $K[x]$. By the factor theorem, we conclude that $q(r) = q'(r) = 0$.

Separability, VIII

Proof (continuated):

- Conversely, if $q(r) = q'(r) = 0$, then by the factor theorem $x - r$ divides $q(x)$, so we may write $q(x) = (x - r)a(x)$.
- Then $q'(x) = a(x) + (x - r)a'(x)$, so $q'(r) = a(r)$.
- Thus $a(r) = 0$ and so $x - r$ divides $a(x)$: then $q(x)$ is divisible by $(x - r)^2$ so r is a repeated root.
- For the statement about separability, any root of a common factor of q and q' is a multiple root (by the above) and conversely any repeated root of q yields a nontrivial common factor of q and q' in $F[x]$ (namely, the minimal polynomial of the repeated root).

Separability, IX

In characteristic 0, this result implies that every irreducible polynomial is separable:

Corollary (Separability in Characteristic 0)

If F is a field of characteristic 0 and $q(x) \in F[x]$ is irreducible, then $q(x)$ is separable.

Proof:

- From the result above, we know that q is separable if and only if q and q' have a common factor in $F[x]$.
- Since q is irreducible in $F[x]$, up to associates the only possible common factors are q and 1.
- In characteristic 0, if q has degree n then q' has degree $n-1$, so q cannot divide q'.
- Thus, the only possibility is for q and q' to be relatively prime, meaning that q is separable.

Summary

We discussed some more examples of splitting fields, along with some properties of cyclotomic extensions.

We discussed algebraic closures and algebraically closed fields.

We introduced separability for polynomials.

Next lecture: More separability and inseparability.