Math 5111 (Algebra 1)

Lecture #7 ∼ October 1, 2020

Classical Constructions + Splitting Fields

- Classical Euclidean Geometry Constructions
- Splitting Fields, part 1

This material represents §2.2.6-2.3.2 from the course notes.

Classical Geometry, I

One aspect of classical Euclidean geometry, per Euclid, is concerned with describing geometric constructions using straightedge and compass.

- Among various problems that can be solved with straightedge and compass are: bisecting (or trisecting) a segment, bisecting an angle, projecting a point onto a line, or drawing a line parallel to a given line passing through a given point.

Classical Geometry, II

As a pleasant application of some of our results on degrees in field extensions, we can establish the impossibility of several classical geometric problems, originally posed by the ancient Greeks:

- **Doubling the Cube**: Is it possible to construct, with straightedge and compass, a cube whose volume is twice that of a given cube?
- **Trisecting an Angle**: Given an arbitrary angle, is it possible to trisect it with straightedge and compass? (In other words, to construct an angle with $1/3$ the measure of the given angle.)
- **Squaring the Circle**: Given a circle, is it possible using straightedge and compass to construct a square with the same area as the circle?

Classical Geometry, III

In order to discuss these problems, we must first translate the allowed operations of straightedge-and-compass constructions into algebraic language.

- A straightedge is an (unmarked) straight segment of arbitrary length, and may be used to draw the line between two given points.
- A compass may be used to draw a circle with center at one given point passing through another given point.
- If two lines, a line and a circle, or two circles intersect, we may draw a new point where they intersect.

Classical Geometry, IV

Each of these problems begins with two given points: by translating and rescaling, we may assume the distance is 1 and the points are $(0, 0)$ and $(1, 0)$.

- Any distance is determined by its length in terms of this unit distance, so we may view distances as elements of $\mathbb{R}$, and view points as elements of the Cartesian plane $\mathbb{R}^2$.

Classical Geometry, V

Definition

A point $(x, y) \in \mathbb{R}^2$ is constructible if, starting with the points $(0, 0)$ and $(1, 0)$, there is a sequence of straightedge-and-compass constructions creating (x, y), while a real number d is constructible if we can construct two points of distance d.

Constructibility of lengths and points are equivalent:

- It is a standard Euclidean construction to project a point onto a line, so if we can construct $(a, b) \in \mathbb{R}^2$, we can construct both a and b.
- Conversely, if we can construct lengths a and b, then we may construct (a, b) by drawing $x = a$ and $y = b$ and finding their intersection.
- Any problem of constructibility reduces to determining whether the appropriate coordinates are constructible.

Classical Geometry, VI

The set of constructible real numbers is a field, and we can also take square roots:

Proposition

If a and b are constructible lengths, then so are $a \pm b$, ab, a/b, and $\sqrt{a}$. In particular, the set of constructible lengths is a field.

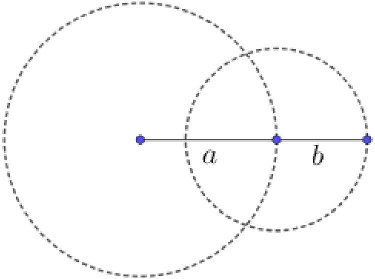
From the proposition we can immediately see that the set of constructible lengths (and their negatives) is a subfield of $\mathbb{R}$.

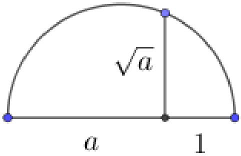
- In particular, we can construct all of $\mathbb{Q}$, and we may also take arbitrary square roots (possibly iteratively).

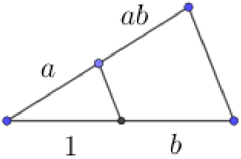
Classical Geometry, VII

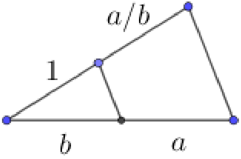
Proof:

- Each of these is a standard Euclidean geometry construction:









Classical Geometry, VIII

What we would now like to do is characterize constructible numbers using field theory.

- Suppose that all of the lengths in our constructions so far lie in the field F: we want to know what kind of field extension we may obtain by performing another construction step. We will go through all of the possible operations (there are five):
  1. We may draw a line through two points.
  2. We may find the intersection of two lines.
  3. We may draw a circle with a given center and radius.
  4. We may find the intersection of a line and a circle.
  5. We may find the intersection of two circles.

Classical Geometry, IX

1. We may draw a line through two constructible points.
   - Suppose the points are $P = (a, b)$ and $Q = (c, d)$.
   - It is straightforward to verify that an equation for this line is $(c - a)(y - b) = (d - b)(x - a)$, which has the form $Ax + By = C$ for A, B, C rational functions in terms of a, b, c, d.
   - Thus, if $a, b, c, d \in F$, then $A, B, C \in F$ as well.
2. We may find the intersection of two lines.
   - If the coefficients of the lines are elements of a field F, then so are the coefficients of the intersection points, since the solution to two simultaneous equations $Ax + By = C$ and $A'x + B'y = C'$ with $A, B, C, A', B', C' \in F$ will also have $x, y \in F$ by basic linear algebra.

Classical Geometry, X

3. We may draw a circle with a given center and radius.
   - The equation of such a circle has the form $(x-h)^2 + (y-k)^2 = r^2$ where $h, k, r \in F$.
   - We can see, again, that all of the coefficients of the equation of the circle lie in F.
4. We may find the intersection of a line and a circle.
   - If the line has equation $Ax + By = C$ and the circle has equation $(x-h)^2 + (y-k)^2 = r^2$, then by solving for x or y in the equation of the line and plugging into the equation of the circle, we end up with a quadratic equation for the other variable.
   - Thus, both x and y lie in a quadratic extension of F.

Classical Geometry, XI

5. We may find the intersection of two circles.
   - Suppose the equations are $(x-h)^2+(y-k)^2=r^2$ and $(x-h')^2+(y-k')^2=(r')^2$.
   - By subtracting the two equations, we may equivalently intersect the circle $(x-h)^2+(y-k)^2=r^2$ with the line $2(h'-h)x+2(k'-k)y=r^2-(r')^2-h^2+(h')^2-k^2+(k')^2$.
   - Note that this is just the line through the two intersection points of the circles, presuming that they intersect.
   - By the previous analysis, x and y again both lie in a quadratic extension of F.

Since we have gone through all the possible operations, we see that every operation either yields another element in F or an element in a quadratic extension of F.

Classical Geometry, XII

Putting all of this together yields the following characterization:

Proposition (Constructibility)

The element $\alpha \in \mathbb{R}$ is constructible if and only if the field $\mathbb{Q}(\alpha)$ can be obtained by a sequence of quadratic extensions of $\mathbb{Q}$. In particular, if α is constructible, then $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is a power of 2.

Proof:

- From our proposition on constructible lengths, and our characterization of quadratic extensions (as being obtained via taking square roots), we can see that any α in an extension field of $\mathbb{Q}$ obtained by a sequence of quadratic is in fact constructible.
- The converse follows from our discussion of the possible extension fields obtained by each step of the construction, as each individual field extension is either trivial or quadratic.

Classical Geometry, XIII

We can now establish the impossibility of the three classical Greek problems we listed earlier:

Corollary

None of the three classical Greek problems (doubling the cube, trisecting an angle, and squaring the circle) can be solved using straightedge-and-compass constructions.

The point is to show that each of these problems would require constructing a non-constructible number.

Classical Geometry, XIV

Proof:

- Doubling the cube is possible if and only if $\sqrt[3]{2}$ is constructible.
- However, as we have discussed, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, which is not a power of 2. Thus, $\sqrt[3]{2}$ is not constructible.
- For trisection, we will show that 20° is not constructible (thus, trisecting an angle of 20° is impossible).
- If the angle θ can be constructed with straightedge and compass, then by orienting the angle from the positive x-axis and intersecting the corresponding ray with the unit circle, then $\cos\theta$ is constructible.
- Conversely, if $\cos\theta$ is constructible, then the angle θ can be obtained in the same way by intersecting the line $y = \cos\theta$ with the unit circle.
- So we only need to show that $\cos 20^\circ$ is not constructible.

Classical Geometry, XV

Proof (continued):

- The triple angle formula for cosine states $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$, so taking $\theta = 20^\circ$, and writing $\alpha = 2\cos 20^\circ$, yields $\frac{1}{2} = \alpha^3/2 - 3\alpha/2$, so $\alpha^3 - 3\alpha - 1 = 0$.
- By the rational root test, $x^3 - 3x - 1$ has no rational roots and is therefore irreducible (since it has degree 3).
- Therefore, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, and so α, and thus $\alpha/2 = \cos 20^\circ$, is not constructible.
- This means trisecting a 60°-angle is not possible.
- Finally, squaring the circle requires constructing $\sqrt{\pi}$.
- Since π is transcendental, π itself is not even constructible (let alone $\sqrt{\pi}$).

Classical Geometry, XVI

Another classical constructibility question is: which n-gons are constructible?

- Since the interior angle of a regular n-gon is $\pi - 2\pi/n$, whose cosine is $-\cos(2\pi/n)$, this question is equivalent to asking: for which n is the number $\cos(2\pi/n)$ constructible?
- We will return to this problem later once we discuss cyclotomic extensions, but we will mention that there are standard constructions for an equilateral triangle ($n = 3$) and a regular pentagon ($n = 5$).
- From the addition and subtraction formulas for cosine, and the half-angle formulas, we can then see that $\cos 3^\circ$ is constructible (corresponding to a 120-gon).
- Since $\cos 20^\circ$ is not constructible, this means that $\cos 1^\circ$ and $\cos 2^\circ$ are not constructible, so the smallest constructible integer-valued angle is 3°.

Classical Geometry, XVII

As a final remark, all of the constructions we have described rely on an unmarked straightedge. By using different tools, it is possible to give solutions to some of these classical problems.

- For example, if one uses a ruler (a device that allows one to mark off specific lengths, while positioning the ruler arbitrarily), there do exist ruler-and-compass constructions for doubling the cube and for trisecting an arbitrary angle.
- Alternatively, by using a formalization of the operations allowed in origami (paper folding), it can also be shown that there exist origami constructions for doubling the cube and trisecting an arbitrary angle. (One may compute cube roots using origami, in addition to the Euclidean operations.)
- However, a marked ruler and origami constructions can only create algebraic distances, and therefore squaring the circle is still impossible, even with these additional tools.

Splitting Fields, I

We now continue investigating the connections between fields and roots of polynomials.

- We have already shown that if p is an irreducible polynomial in $F[x]$, then F has a field extension that contains a root of p: explicitly, in the extension $K = F[t]/p(t)$, the element $\overline{t} \in K$ has the property that $p(\overline{t}) = 0$.
- This observation, although it follows essentially tautologically from our development of polynomial modular arithmetic, neatly resolves a foundational issue, namely, the question of whether there must exist a field "somewhere" in which $p(x)$ has a root.

Splitting Fields, II

We may extend this observation to any polynomial p as follows:

- First, find the factorization of p over $F[x]$, and choose any irreducible factor $q(x)$.
- Then construct the field extension $K = F[t]/q(t)$, and like before, observe that the element $\overline{t} \in K$ has the property that $q(\overline{t}) = 0$.
- Finally, since q divides p in $F[x]$, we also have $p(\overline{t}) = 0$.

Thus, we see that if p is any polynomial in $F[x]$, then there exists a field extension of F that contains a root of p.

We will now extend this argument to show that there is a field extension that contains “all the roots” of p, and in fact there is a well-defined notion of a “smallest” such field.

Splitting Fields, III

First, we define the notion of when all of a polynomial's roots lie in a field:

Definition

If K is an extension field of F, the polynomial $p(x) \in F[x]$ splits completely (or factors completely) in $K[x]$ if there exist $c, r_1, r_2, \dots, r_n \in K$ such that $p(x) = c(x - r_1)(x - r_2) \cdots (x - r_n)$ in $K[x]$.

The terminology is referring to the fact that the individual irreducible factors of $p(x)$ in $F[x]$ split apart into linear factors (i.e., as completely as possible) inside $K[x]$.

Splitting Fields, IV

Examples:

1. The polynomial $x^4 - 1 \in \mathbb{R}[x]$ splits completely over $\mathbb{C}$ as $(x-1)(x+1)(x-i)(x+i)$.
2. The polynomial $x^2 - 5 \in \mathbb{Q}[x]$ splits completely over $\mathbb{C}$ as $(x-\sqrt{5})(x+\sqrt{5})$. In fact, it also splits completely with the same factorization over $\mathbb{R}$, or over $\mathbb{Q}(\sqrt{5})$.
3. More generally, every polynomial splits completely over $\mathbb{C}$: this is the content of the fundamental theorem of algebra.
4. The polynomial $x^4 - 16x^2 + 16$ splits completely over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ as $(x-\sqrt{2}-\sqrt{6})(x-\sqrt{2}+\sqrt{6})(x+\sqrt{2}-\sqrt{6})(x+\sqrt{2}+\sqrt{6})$.

We would like to show that there is always some extension field of F in which $p(x)$ splits completely.

Splitting Fields, V

The idea is simply to iterate the construction given before:

- We start with an extension K_1/F in which $p(x)$ has a root r_1.
- By the factor theorem, we can then write $p(x) = (x - r_1) \cdot p_1(x)$ for a polynomial $p_1(x) \in K_1[x]$.
- Now applying the argument to $p_1(x)$ over $K_1[x]$ shows that there exists a field extension K_2/K_1 in which $p_1(x)$ has at least one root r_2, so like before we can write $p_1(x) = (x - r_2) \cdot p_2(x)$ for a polynomial $p_2(x) \in K_2[x]$.
- By iterating this argument we eventually obtain a tower of field extensions $K_n/K_{n-1}/\cdots/K_1/K$, where $n = \deg p$ and $p_{i-1}(x) = (x - r_i)p_i(x)$ where $p_i(x) \in K_i[x]$ has degree $n - i$.
- Then p_n has degree 0 so it is some constant c, and so we obtain $p(x) = c(x - r_1)(x - r_2)\cdots(x - r_n)$ for some $c, r_1, r_2, \ldots, r_n \in K_n$.

Splitting Fields, VI

So, we see that every polynomial in $F[x]$ does split completely over some field extension K/F.

- If $p \in F[x]$ splits completely over K, then p also splits completely over any extension field of K: indeed, we saw this before with the example of $x^2 - 5$, which splits completely over $\mathbb{Q}(\sqrt{5})$ and also in its field extensions $\mathbb{R}$ and $\mathbb{C}$.
- It is therefore natural to ask: what is the "smallest possible" field extension of F in which p splits completely?
- When we discussed simple extensions inside the extension K/F, we defined the field $F(\alpha)$ to be the intersection of all subfields of K containing F and α.
- It might seem reasonable to try to use the same approach here.

Splitting Fields, VII

It seems valid to define this "smallest possible" field extension of F in which p splits completely to be the intersection of all extension fields K/F in which p splits completely.

- But in fact, this definition only makes sense when all of these extension fields are themselves subsets of some larger field.
- This may seem like a minor inconvenience, but it's actually very important.

Splitting Fields, VIII

We can illustrate the difficulties with an example: consider the polynomial $p(x) = x^2 + 4 \in \mathbb{R}[x]$.

- We can see that $p(x) = x^2 + 4$ splits completely over $\mathbb{C}$ as $p(x) = (x - 2i)(x + 2i)$, and $p(x)$ also splits completely over the field extension $\mathbb{R}[t]/(t^2 + 4)$ as $p(x) = (x - \overline{t})(x + \overline{t})$.
- Since both of these fields are degree-2 extensions of $\mathbb{R}$, they both seem valid candidates for the "smallest possible" field extension of $\mathbb{R}$ in which p splits completely.
- Here, it does not really make sense to ask what "the intersection" of $\mathbb{C}$ and $\mathbb{R}[t]/(t^2 + 4)$ is!
- We would need to specify the manner in which these two fields are to be considered as subsets of some larger collection before the intersection would make sense.

Splitting Fields, IX

We can avoid this particular thorny issue by instead posing the definition entirely within the field K itself.

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 over K, and p does not split completely over any proper subfield of K.

- If p splits over K as $p(x) = c(x - r_1)(x - r_2) \cdots (x - r_n)$, then by the remainder theorem, any subfield of K in which p splits completely must contain $r_1, \dots, r_n$, hence $F(r_1, \dots, r_n)$.
- On the other hand, clearly $p(x)$ does split completely over $F(r_1, \dots, r_n)$, so saying that p splits completely in K but not over any proper subfield is equivalent to saying that $K = F(r_1, r_2, \dots, r_n)$.
- In particular, the definition is well-posed. (Phew!)

Splitting Fields, X

For any $p \in F[x]$, a splitting field for p always exists:

- Specifically, we run through the construction detailed a few slides ago to find an extension L/F in which $p(x)$ splits completely as $p(x) = c(x - r_1)(x - r_2) \cdots (x - r_n)$.
- Then we just take $K = F(r_1, r_2, \dots, r_n)$.
- By the discussion on the last slide, K is then a splitting field for p.

Splitting Fields, XI

Examples:

1. $\mathbb{Q}(\sqrt{D})$ is a splitting field for the polynomial $p(x) = x^2 - D$ over $\mathbb{Q}$.
   - This follows immediately because $p(x) = (x + \sqrt{D})(x - \sqrt{D}) \in \mathbb{Q}(\sqrt{D})[x]$ and $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{D}, -\sqrt{D})$.
2. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a splitting field for the polynomial $p(x) = (x^2 - 2)(x^2 - 3)$ over $\mathbb{Q}$.
   - We can see that $p(x)$ splits completely over $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ because $p(x) = (x - \sqrt{2})(x + \sqrt{2})(x - \sqrt{3})(x + \sqrt{3})$ in $K[x]$.
   - Furthermore, $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3})$, so K is indeed a splitting field.

Splitting Fields, XII

We can give an upper bound on the degree of a splitting field by formalizing the arguments we gave earlier:

Proposition (Degree of Splitting Fields)

For any field F and any (nonzero) polynomial $p \in F[x]$ of degree n, there exists a splitting field K/F for p, and $[K : F] \leq n!$.

The idea is simply to keep track of the degrees of the extensions in the construction we described earlier.

Splitting Fields, XIII

Proof:

- Induct on n: for the base case $n = 1$ with $p(x) = ax + b = a(x + b/a)$, we have a single root $r_1 = -b/a \in F$. Thus, $K = F$ is a splitting field.
- For the inductive step, assume that any polynomial of degree $n - 1$ over any field has a splitting field extension of degree at most $(n - 1)!$, and let $p \in F[x]$ have degree n.
- Choose any irreducible factor (in $F[x]$) q of p of degree $k \leq n$ and set $K_1 = F[t]/q(t)$. Then $[K_1 : F] = k$ by our results on simple extensions.

Splitting Fields, XIV

Proof (continued):

- Furthermore, $q(\overline{t}) = 0$ in K_1, so since q divides p we have $p(\overline{t}) = 0$ in K_1.
- So by the factor theorem we may write $p(x) = (x - \overline{t}) \cdot p_1(x)$ for a polynomial $p_1(x) \in K_1[x]$ of degree $n - 1$ and some element $r_1 \in K_1$.
- By the induction hypothesis, there exists a splitting field L for $p_1(x)$ over K_1 of degree at most $(n-1)!$.
- Then $[L : F] = [L : K_1] \cdot [K_1 : F] \leq (n-1)! \cdot k \leq n!$, and $p(x)$ splits completely in L, say as $p(x) = c(x - r_1)(x - r_2) \cdots (x - r_n)$.
- The subfield $F(r_1, r_2, \dots, r_n)$ of L is then a splitting field for p, and its degree is at most $[L : F] \leq n!$, as required.

Splitting Fields, XV

We would now like to analyze the relationships between "different" possible splitting fields for a given polynomial.

- We saw that $\mathbb{C}$ is a splitting field for $x^2 + 4$ over $\mathbb{R}$, since $x^2 + 4 = (x + 2i)(x - 2i)$ in $\mathbb{C}[x]$, and $\mathbb{C} = \mathbb{R}(2i, -2i)$.
- But the field $K = \mathbb{R}[t]/(t^2 + 4)$ is also a splitting field for $x^2 + 4$ over $\mathbb{R}$, since $x^2 + 4 = (x - \overline{t})(x + \overline{t})$ in $K[x]$.
- But notice: these two fields are isomorphic, with an explicit isomorphism being the one that associates $\overline{t}$ with $2i$ (extended in the natural way).
- Thus, both of these splitting fields have the same structure. This turns out to be true for arbitrary splitting fields, although it is actually easier to prove a slightly stronger result.

Splitting Fields, XVI

Theorem (Uniqueness of Splitting Fields)

Let $\varphi : E \to F$ be an isomorphism of fields with $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in E[x]$, and set $q(x) = \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n \in F[x]$ to be the polynomial obtained by applying φ to the coefficients of p. If K/E is a splitting field for p, and L/F is a splitting field for q, then the isomorphism φ extends to an isomorphism $\sigma : K \to L$ (i.e., $\sigma|_E = \varphi$, or explicitly, for any $\alpha \in E$ we have $\sigma(\alpha) = \varphi(\alpha)$). In particular, any two splitting fields for p are isomorphic.

The argument here is mostly bookkeeping.

Splitting Fields, XVII

Proof:

- The second statement follows from the first by taking φ to be the identity map, since in that case the first statement says that if K/E and L/E are both splitting fields of p, then K and L are isomorphic.
- To prove the first statement, we induct on the degree n of p. For the base case $n = 1$, as we have already observed, the splitting field of any degree-1 polynomial over a field is simply the field itself. Thus, $K = E$ and $L = F$, so the desired map σ is simply φ.

Splitting Fields, XVIII

Proof (continued more):

- Now suppose the result holds for polynomials of degree $n-1$, and let p have degree n.
- Choose any monic irreducible factor $a(x) = c_0 + c_1 x + \cdots + c_m x^m$ of p, and set $b(x) = \varphi(c_0) + \varphi(c_1)x + \cdots + \varphi(c_m)x^m$.
- It is essentially trivial to see that $\varphi : E \to F$ extends to an isomorphism of $E[x]$ with $F[x]$. It therefore preserves factorizations and thus irreducibility.
- Thus, $b(x)$ divides $q(x)$, and $b(x)$ is irreducible in $F[x]$.
- Since every root of $a(x)$ is a root of $p(x)$ we see that K contains every root of a; similarly L contains every root of b.

Splitting Fields, XIX

Proof (continued even still more):

- Consider $\hat{\varphi} : F[x] \to E(s)$ defined by $\hat{\varphi}(p) = \varphi(p)(s)$, the composition of φ with the evaluation-at-s map.
- This map is a ring homomorphism that is clearly surjective, and its kernel is the ideal $(a(x))$.
- Thus, by the first isomorphism theorem, we obtain an isomorphism $\tilde{\varphi} : F(r) \to E(s)$.
- Explicitly, $\tilde{\varphi}$ maps the polynomial $d_0 + d_1 r + \cdots + d_{m-1} r^{m-1} \mapsto$ $\varphi(d_0) + \varphi(d_1)s + \cdots + \varphi(d_{m-1})s^{m-1}$ for $d_i \in F$.

Splitting Fields, XX

Proof (continued additionally even still yet more also further):

- By the factor theorem, since r is a root of p and s is a root of q, we may write $p(x) = (x-r)p'(x)$ and $q(x) = (x-s)q'(x)$ for some polynomials $p' = c(x-r_2)\cdots(x-r_n)$ and $q' = d(x-s_2)\cdots(x-s_n)$ of degree $n-1$.
- In particular, p' splits completely over K and q' splits completely over L.
- Since K is the splitting field of p, we see that $K = F(r, r_2, \ldots, r_n) = F(r)(r_2, \ldots, r_n)$, and so in fact K is the splitting field of p' over $F(r)$. Likewise, L is the splitting field of q' over $E(s)$.
- Finally, by the induction hypothesis, since we have an isomorphism $\tilde{\varphi} : F(r) \to E(s)$, we may lift it to obtain an isomorphism $\sigma : K \to L$, as required.

Splitting Fields, XXI

The point of that whole long argument was that splitting fields are unique up to isomorphism.

- The isomorphism between two splitting fields is the fairly natural one of "map the roots of the various equivalent irreducible factors to one another, taking care to ensure that everything stays well defined".
- Because splitting fields are unique up to isomorphism, we will usually commit the mild abuse of terminology of referring to "the" splitting field of $p(x)$ over F.

Splitting Fields, XXII

Let's write down some examples now.

- In general, it can be quite difficult to compute an explicit description of a splitting field, because it requires knowing information about the factorization and the precise nature of the roots of $p(x)$, along with any sort of algebraic relations among the roots.
- Indeed, attempting to do this in as much generality as possible quickly leads one in the direction of Galois theory, since that is precisely how one describes what the algebraic relations between the roots of a polynomial look like.
- But for the moment, we will primarily focus on finding splitting fields over $\mathbb{Q}$ where we can give an explicit description of the field, since we have irreducibility criteria that can apply to polynomials of arbitrarily large degree in $\mathbb{Q}[x]$, or of polynomials of low degree that we can analyze concretely.

Splitting Fields, XXIII

Example: Find the splitting field for $p(x) = x^2 + 1$ over $\mathbb{Q}$, over $\mathbb{F}_2$, and over $\mathbb{F}_3$.

- Over $\mathbb{Q}$, we can see that $\mathbb{Q}(i)$ is a splitting field because $p(x) = (x + i)(x - i) \in \mathbb{Q}[x]$ and $\mathbb{Q}(i) = \mathbb{Q}(i, -i)$.
- Over $\mathbb{F}_2$, the field $\mathbb{F}_2$ itself is actually already a splitting field because $p(x) = (x + 1)^2 \in \mathbb{F}_2[x]$.
- Over $\mathbb{F}_3$, the polynomial is irreducible (since it has degree 2 and no roots in $\mathbb{F}_3$), so any splitting field must be of degree at least 2 over $\mathbb{F}_3$.
- On the other hand, in the degree-2 field extension $K = \mathbb{F}_3[t]/p(t)$, we can factor $p(x)$ as $p(x) = (x - \overline{t})(x + \overline{t})$, and $K = \mathbb{F}_3(\overline{t}, -\overline{t})$, so we see that K is a splitting field for p.

Splitting Fields, XXIV

The observations from this last example hold in general for splitting fields of quadratic polynomials.

- For any quadratic polynomial $p(x) \in F[x]$, if p has a root in F, then both its roots are in F.
- This follows by observing that if $p(x) = (x - r_1)(x - r_2) = x^2 + ax + b$ then $r_2 = -a - r_1 \in F$.
- Thus, in this case F itself is the splitting field for p.
- Otherwise, if p is irreducible, then p does not split completely over F, but does split completely over the quadratic extension $F[t]/p(t)$: thus, $F[t]/p(t)$ will be a splitting field.

Splitting Fields, XXV

Example: Show that $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ is the splitting field for the polynomial $p(x) = x^3 - 2$ over $\mathbb{Q}$, where $\zeta_3 = e^{2\pi i/3} = (-1 + i\sqrt{3})/2$ denotes a nonreal cube root of unity.

- As we have mentioned previously, this field $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ is also equal to $\mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2})$, and has degree 6 over $\mathbb{Q}$.
- We can see that $p(x)$ splits completely over K because $p(x) = (x - \sqrt[3]{2})(x - \zeta_3\sqrt[3]{2})(x - \zeta_3^2\sqrt[3]{2})$ in $K[x]$.
- To see this, one may either compute the third remaining root of $p(x)$ using polynomial division once the roots $\sqrt[3]{2}$ and $\zeta_3\sqrt[3]{2}$ are identified, or by directly observing that $\zeta_3^2\sqrt[3]{2}$ is also a root.

Splitting Fields, XXVI

Example: Show that $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ is the splitting field for the polynomial $p(x) = x^3 - 2$ over $\mathbb{Q}$, where $\zeta_3 = e^{2\pi i/3} = (-1 + i\sqrt{3})/2$ denotes a nonreal cube root of unity.

- Thus, we see that $L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2})$ is a splitting field for $p(x)$ over $\mathbb{Q}$.
- Notice that L contains both generators $\sqrt[3]{2}$ and $\zeta_3 = (\zeta_3\sqrt[3]{2})/(\sqrt[3]{2})$ of $K/\mathbb{Q}$, so L contains K.
- On the other hand, K contains all three generators $\sqrt[3]{2}$, $\zeta_3\sqrt[3]{2}$, and $\zeta_3^2\sqrt[3]{2}$ of $L/\mathbb{Q}$, so K contains L.
- Thus, $K = L$ is a splitting field for $p(x)$ as claimed.

It should be relatively obvious that the fields $\mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2})$ and $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ are the same: the point is that you can construct the generators of each extension inside the other one.

Splitting Fields, XXVII

Example: Find the splitting field for $p(x) = x^4 + 64$ over $\mathbb{Q}$.

- As it happens, this polynomial factors over $\mathbb{Q}$ as $p(x) = (x^2 - 4x + 8)(x^2 + 4x + 8)$.
- Using the quadratic formula, we can see that the roots of these two quadratics are $\pm 2 \pm 2i$.
- Therefore, we can see that $\mathbb{Q}(i)$ is a splitting field for p, since it is the subfield of $\mathbb{C}$ generated by the roots of p.
- Notice in particular that, although $p(x)$ has degree 4, the degree of the splitting field is only 2. (You should think about why this can only happen because p factors over $\mathbb{Q}$.)

Splitting Fields, XXVIII

As an aside, I wanted to mention that another way to compute the roots of $p(x) = x^4 + 64$ in this last example is to write the corresponding complex numbers in polar form.

- This is something I assume you have seen before, but since it's useful and we will use it repeatedly when we start working more with roots of unity, I want to review it now.
- The point is that the solutions to the equation $z^n = re^{i\theta}$ in $\mathbb{C}$, where r is a nonnegative real number, are $z = r^{1/n}e^{i(\theta+2k\pi)/n}$ for $k = 0, 1, \dots, n-1$.
- We can also use Euler's identity $e^{i\theta} = \cos\theta + i\sin\theta$ to write down the real and imaginary parts explicitly.
- The solutions to $z^n = 1$ are the complex nth roots of unity, of the form $e^{2\pi ik/n} = \cos(2\pi k/n) + i\sin(2\pi k/n)$. We will discuss them more later.

Splitting Fields, XXIX: Later Is Now

Example: If n is a positive integer, show that the splitting field of the polynomial $x^n - 1$ over $\mathbb{Q}$ is of the form $\mathbb{Q}(\zeta_n)$ where ζ_n is the complex number $\zeta_n = e^{2\pi i/n} = \cos(2\pi/n) + i\sin(2\pi/n)$.

- As I just noted, $\zeta_n = e^{2\pi i/n}$ has the property that $\zeta_n^n = e^{2\pi i} = 1$, and so ζ_n is a root of $q(x)$ over $\mathbb{C}$.
- Furthermore, for each integer k with $0 \leq k \leq n-1$, we see that $\zeta_n^k = e^{2\pi ik/n} = \cos(2\pi k/n) + i\sin(2\pi k/n)$ also has the property that $(\zeta_n^k)^n = 1^k = 1$ and so ζ_n^k is also a root of $q(x)$ over $\mathbb{C}$.
- The n complex numbers ζ_n^k for $0 \leq k \leq n-1$ are distinct as elements of $\mathbb{C}$ (geometrically, they represent n equally spaced points around the unit circle $|z| = 1$ in the complex plane).

Splitting Fields, XXX: After Dark (Literally)

Example: If n is a positive integer, show that the splitting field of the polynomial $x^n - 1$ over $\mathbb{Q}$ is of the form $\mathbb{Q}(\zeta_n)$ where ζ_n is the complex number $\zeta_n = e^{2\pi i/n} = \cos(2\pi/n) + i\sin(2\pi/n)$.

- So we have the factorization $q(x) = (x-1)(x-\zeta_n)(x-\zeta_n^2)\cdots(x-\zeta_n^{n-1})$.
- Thus, the splitting field for $q(x)$ over $\mathbb{Q}$ is $\mathbb{Q}(1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1})$.
- This field clearly contains $\mathbb{Q}(\zeta_n)$, but since $\mathbb{Q}(\zeta_n)$ contains each of the generators $1, \zeta_n, \dots, \zeta_n^{n-1}$, it is equal to $\mathbb{Q}(\zeta_n)$ as claimed.

Splitting Fields, XXXI

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.

It is a nontrivial problem (and one to which we will return later) 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 $\mathbb{Q}$.

But I will spoil the answer now and tell you that the degree is $\varphi(n)$, where φ is the Euler φ-function. Next time I will prove that this is the correct degree when $n = p$ is a prime.

Summary

We discussed some classical constructions from Euclidean geometry.

We introduced splitting fields and established a number of their properties.

Next lecture: More with splitting fields, algebraic closures