Math 5111 (Algebra 1)

Lecture #21 of 24 ∼ November 23rd, 2020

Finite Fields, Primitive Elements, and Composite Extensions

- Finite Fields and Irreducible Polynomials Mod p
- The Primitive Element Theorem
- Composite Extensions

This material represents §4.3.1-4.3.3 from the course notes.

Erstwhile

Theorem (Fundamental Theorem of Galois Theory)

Let K/F be a Galois extension and let $G = \mathrm{Gal}(K/F)$.

0. *There is an inclusion-reversing bijection between intermediate fields E of K/F and subgroups H of G, given by associating a subgroup H to its fixed field E.*
1. *Subgroup indices correspond to extension degrees, so that $[K : E] = |H|$ and $[E : F] = |G : H|$.*
2. *The extension K/E is always Galois, with Galois group H.*
3. *If $\overline{F}$ is a fixed algebraic closure of F, then the embeddings of E into $\overline{F}$ are in bijection with the left cosets of H in G.*
4. *E/F is Galois if and only if H is a normal subgroup of G, and in that case, $\mathrm{Gal}(E/F)$ is isomorphic to G/H.*
5. *Intersections of subgroups correspond to joins of fields, and joins of subgroups correspond to intersections of fields.*
6. *The lattice of subgroups of G is the same as the lattice of intermediate fields of K/F turned upside-down.*

Roadmap

We will now discuss a number of applications of the fundamental theorem of Galois theory (and its various related ideas) to the study of field extensions:

1. Finite fields and irreducible polynomials in $\mathbb{F}_p[x]$
2. Simple extensions and the primitive element theorem
3. Properties of composite extensions
4. Cyclotomic and abelian extensions

Then we will finish off the semester back where we started: by studying polynomials and their roots.

Finite Fields and Irreducible Polynomials in $\mathbb{F}_p[x]$, I

We will start by analyzing the structure of finite fields, so let p be a prime and n be a positive integer.

- As we have discussed, there is a unique (up to isomorphism) finite field $\mathbb{F}_{p^n}$ with p^n elements, and it is the splitting field of the separable polynomial $x^{p^n} - x$ over $\mathbb{F}_p$.
- We have also shown that the Galois group $G = \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is cyclic of order n and is generated by the Frobenius automorphism $\varphi_{(n)} : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ with $\varphi_{(n)}(x) = x^p$.

Finite Fields and Irreducible Polynomials in $\mathbb{F}_p[x]$, II

Since $G = \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is cyclic of order n, its subgroups are of the form $\langle \varphi^d \rangle$ for the divisors d of n.

- Because G is abelian, all of these subgroups are normal, so the corresponding fixed fields are all Galois.
- Since $\varphi_{(n)}^d(x) = x^{p^d}$, the fixed field of φ^d is the set of solutions to the equation $x^{p^d} - x = 0$ inside $\mathbb{F}_{p^n}$, so the fixed field is the splitting field of $x^{p^d} - x$, which is $\mathbb{F}_{p^d}$.
- Thus, by the fundamental theorem of Galois theory, the subfields of $\mathbb{F}_{p^n}$ are the fields $\mathbb{F}_{p^d}$ for d dividing n.
- Furthermore, the Galois group $\mathrm{Gal}(\mathbb{F}_{p^d}/\mathbb{F}_p)$ is generated by the image of $\varphi_{(n)}$ inside the quotient group $G/\langle \varphi^d \rangle$. This map is simply the pth power map on elements, which is $\varphi_{(d)} : \mathbb{F}_{p^d} \to \mathbb{F}_{p^d}$. (In other words, the restriction of the Frobenius map from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^d}$ is the Frobenius map on $\mathbb{F}_{p^d}$.)

Finite Fields and Irreducible Polynomials in $\mathbb{F}_p[x]$, III

We can also use these observations to prove a useful result on irreducible polynomials over $\mathbb{F}_p$:

Theorem (Factorization of $x^{p^n} - x$ in $\mathbb{F}_p[x]$)

For any prime p and any positive integer n, the polynomial $x^{p^n} - x$ factors in $\mathbb{F}_p[x]$ as the product of all monic irreducible polynomials over $\mathbb{F}_p$ of degree dividing n.

Examples:

1. Over $\mathbb{F}_2$, $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
2. Over $\mathbb{F}_2$, $x^{16} - x = x(x+1)(x^2+x+1)(x^4+x^3+1)(x^4+x+1)(x^4+x^3+x^2+x+1)$.
3. Over $\mathbb{F}_3$, $x^9 - x = x(x+1)(x+2)(x^3+2x+1)(x^3+2x+2)$.

Finite Fields and Irreducible Polynomials in $\mathbb{F}_p[x]$, IV

Proof:

- Let $q(x) = x^{p^n} - x$. As we have noted previously, $q(x)$ is separable and its roots are the elements of $\mathbb{F}_{p^n}$.
- If $f(x)$ is any monic irreducible factor of $x^{p^n} - x$, then $\mathbb{F}_p[x]/f(x)$ is a subfield of $\mathbb{F}_{p^n}$, hence must be $\mathbb{F}_{p^d}$ for some d dividing n. Since $\deg(f) = d$ this means $\deg(f)$ divides n.
- Conversely, if $f(x) \in \mathbb{F}_p[x]$ is monic irreducible of degree d dividing n, then $\mathbb{F}_p[x]/(f(x))$ is a finite field with p^d elements, and is therefore (isomorphic to) $\mathbb{F}_{p^d}$.
- Then any root α of $f(x)$ is contained in $\mathbb{F}_{p^d}$ hence lies in $\mathbb{F}_{p^n}$ and is thus a root of $q(x)$. Since $f(x)$ is separable (since it is irreducible over a finite field) this means $f(x)$ divides $q(x)$.
- Thus, the irreducible factors of $x^{p^n} - x$ are precisely the monic irreducible polynomials of degree dividing n, and since no factor can be repeated, $x^{p^n} - x$ must simply be their product.

Finite Fields and Irreducible Polynomials in $\mathbb{F}_p[x]$, V

We can use the factorization of $x^{p^n} - x$ to give an exact count of the monic irreducible polynomials in $\mathbb{F}_p[x]$:

- Let $f_p(n)$ be the number of monic irreducible polynomials of exact degree n in $\mathbb{F}_p[x]$.
- The theorem says that $p^n = \sum_{d|n} df_p(d)$, since both sides count the total degree of the product of all irreducible polynomials of degree dividing n.
- Using this recursion, we can compute the first few values:

n	1	2	3	4	5	6	7
$f_p(n)$	p	$\frac{p^2-p}{2}$	$\frac{p^3-p}{3}$	$\frac{p^4-p^2}{4}$	$\frac{p^5-p}{5}$	$\frac{p^6-p^3-p^2+p}{6}$	$\frac{p^7-p}{7}$

- For example, we see that there are $(2^7-2)/2 = 63$ monic irreducible polynomials of degree 7 over $\mathbb{F}_2$.

Finite Fields and Irreducible Polynomials in $\mathbb{F}_p[x]$, VI

In fact, using a tool from elementary number theory, we can use the recursion to write down a general formula:

Definition

The Möbius function is defined as

$$\mu(n) = \begin{cases} 0 & \text{if } n \text{ is divisible by the square of any prime} \\ (-1)^k & \text{if } n \text{ is the product of } k \text{ distinct primes} \end{cases}.$$

In particular, $\mu(1) = 1$.

For example, $\mu(5) = -1$, $\mu(6) = 1$, $\mu(30) = -1$, and $\mu(12) = 0$.

Proposition (Möbius Inversion)

If $f(n)$ *is any sequence satisfying a recursive relation of the form* $g(n) = \sum_{d|n} f(d)$, *for some function* $g(n)$, *then* $f(n) = \sum_{d|n} \mu(d) g(n/d)$.

Finite Fields and Irreducible Polynomials in $\mathbb{F}_p[x]$, VII

Proof:

- First, we claim $\sum_{d|n} \mu(d)$ is 1 if $n = 1$ and 0 if $n \neq 0$.
- To see this, if $n = p_1^{a_1} \cdots p_k^{a_k}$, the only terms that will contribute to the sum $\sum_{d|n} \mu(d)$ are those values of $d = p_1^{b_1} \cdots p_k^{b_k}$ where each b_i is 0 or 1. If $k > 0$, then half of these 2^k terms will have $\mu(d) = 1$ and the other half will have $\mu(d) = -1$, so the sum is zero. Otherwise, $k = 0$ means that $n = 1$, in which case the sum is clearly 1.
- Now we prove the desired result by induction. It clearly holds for $n = 1$, so now suppose the result holds for all $k < n$.
- Then $\sum_{d|n} \mu(d) g(n/d) = \sum_{d|n} \mu(d) \sum_{d'|(n/d)} f(d') = \sum_{dd'|n} \mu(d) f(d') = \sum_{d'|n} f(d') \sum_{d|(n/d')} \mu(d)$ by induction and reordering the sum.
- But the last sum is simply $f(n)$, because $\sum_{d|(n/d')} \mu(d)$ is zero unless n/d' is equal to 1.

Finite Fields and Irreducible Polynomials in $\mathbb{F}_p[x]$, VIII

By applying Möbius inversion to $f_p(n)$, we immediately obtain the following:

Corollary (Number of Monic Irreducible Polynomials in $\mathbb{F}_p[x]$)

The number of monic irreducible polynomials of degree n in $\mathbb{F}_p[x]$ is $f_p(n) = \dfrac{1}{n} \sum_{d|n} p^{n/d} \mu(d)$.

Examples:

- The number of monic irreducibles of degree 18 in $\mathbb{F}_2[x]$ is $\frac{1}{18}(2^{18} - 2^9 - 2^6 + 2^3) = 14532$.
- The number of monic irreducibles of degree 30 in $\mathbb{F}_2[x]$ is $\frac{1}{30}(2^{30} - 2^{15} - 2^{10} - 2^6 + 2^5 + 2^3 + 2^2 - 2^1) = 35790267$.

Finite Fields and Irreducible Polynomials in $\mathbb{F}_p[x]$, IX

From this corollary, we see that $f_p(n) = \frac{1}{n}p^n + O(p^{n/2})$, where the "big-$O$" notation means that the error is of size bounded above by a constant times $p^{n/2}$ as $n \to \infty$.

- This has the following interesting reinterpretation: let X be the number of polynomials in $\mathbb{F}_p[x]$ of degree less than n. Clearly, $X = p^n$.
- Now we ask: of all these X polynomials, how many of them are "prime" (i.e., irreducible)?
- This is simply $f_p(n) = \dfrac{1}{n}p^n + O(p^{n/2}) = \dfrac{X}{\log_p(X)} + O(\sqrt{X})$.
- In other words: the number of "primes less than X" is equal to $\dfrac{X}{\log_p(X)}$, up to a bounded error term.

Finite Fields and Irreducible Polynomials in $\mathbb{F}_p[x]$, X

Compare the result $f_p(n) = \dfrac{X}{\log_p(X)} + \mathcal{O}(\sqrt{X})$ to the Prime Number Theorem in $\mathbb{Z}$:

Theorem (Prime Number Theorem)

If $\pi(n)$ is the number of primes in the interval $[1, n]$, then $\pi(n) \sim \dfrac{n}{\log(n)}$, in the sense that $\displaystyle\lim_{n\to\infty} \frac{\pi(n)}{n/\log(n)} = 1$.

So in fact, we have just proven the analogue of the Prime Number Theorem for the ring $\mathbb{F}_p[x]$.

Finite Fields and Irreducible Polynomials in $\mathbb{F}_p[x]$, XI

Any of the irreducible polynomials $f(x)$ of degree n yields gives a model for $\mathbb{F}_{p^n}$, namely as $\mathbb{F}_p[x]/(f(x))$.

- Thus, if f_1 and f_2 are both irreducible of degree n, then $F_1 = \mathbb{F}_p[x]/(f_1(x))$ and $F_2 = \mathbb{F}_p[y]/(f_2(y))$ are both isomorphic to $\mathbb{F}_{p^n}$.
- To compute an isomorphism between them, we simply observe that $f_1(x)$ splits completely over F_2, and if $\alpha(y)$ represents any root, then the map sending $\overline{x}$ in F_1 to $\alpha(y)$ in F_2 extends to an isomorphism of F_1 with F_2. (In other words, we map a root x of f_1 in F_1 to a root $\alpha(y)$ of f_1 in F_2.)
- In practice, it can be rather cumbersome to compute the roots by hand, although there do exist efficient factorization algorithms over finite fields, one of which is known as Berlekamp's algorithm.

Finite Fields and Irreducible Polynomials in $\mathbb{F}_p[x]$, XII

Example: Compute an explicit isomorphism of the field $\mathbb{F}_3[x]/(x^3 + 2x + 1)$ with the field $\mathbb{F}_3[y]/(y^3 + y^2 + 2)$.

- Note that both $x^3 + 2x + 1$ and $y^3 + y^2 + 2$ are irreducible over $\mathbb{F}_3$ because they are degree-3 and have no roots in $\mathbb{F}_3$.
- To compute an isomorphism, we search for a root of $x^3 + 2x + 1$ in $\mathbb{F}_3[y]/(y^3 + y^2 + 2)$.
- Checking the various possibilities eventually reveals that $2y^2 + 2y$ is a root of $x^3 + 2x + 1$, and therefore the map $\varphi : \mathbb{F}_3[x]/(x^3 + 2x + 1) \to \mathbb{F}_3[y]/(y^3 + y^2 + 2)$ with $\varphi(x) = 2y^2 + 2y$ is such an isomorphism.

Finite Fields and Irreducible Polynomials in $\mathbb{F}_p[x]$, XIII

As a final remark, we will observe that the simple structure of finite field extensions also yields a nice description of the algebraic closure $\overline{\mathbb{F}_p}$.

- Explicitly, if $\alpha \in \overline{\mathbb{F}_p}$ then α (being algebraic over $\mathbb{F}_p$) is contained in a finite-degree extension of $\mathbb{F}_p$, namely, one of the fields $\mathbb{F}_{p^n}$.
- But notice that the fields $\mathbb{F}_{p^n}$ for $n \geq 1$ are partially ordered under inclusion, and that any two of them are contained in another (namely, $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^m}$ are both contained in $\mathbb{F}_{p^{mn}}$).
- Thus, the union of these fields (technically, the colimit) is well defined, and by the above, it contains every element α algebraic over $\mathbb{F}_p$, meaning that it is the algebraic closure.

Finite Fields and Irreducible Polynomials in $\mathbb{F}_p[x]$, XIV

Symbolically, $\overline{\mathbb{F}_p} = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$.

- Furthermore, since the Frobenius maps on the various $\mathbb{F}_{p^n}$ are all consistent under restriction, we see that they extend to a Frobenius map $\varphi : \overline{\mathbb{F}_p} \to \overline{\mathbb{F}_p}$ on the algebraic closure, defined explicitly via $\varphi(x) = x^p$.
- Note that φ has infinite order as an element of $\mathrm{Aut}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$, but one may show in fact that $\mathrm{Aut}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ is uncountably infinite (and thus φ is not a generator, since the cyclic subgroup it generates is only countably infinite).

The Primitive Element Theorem, I

We can use the fundamental theorem of Galois theory to determine (in a large number of cases) when an arbitrary finite-degree extension K/F is simple, which is to say, when $K = F(\alpha)$ for some $\alpha \in K$. The easiest case is when F is finite:

Proposition (Finite Fields are Simple)

Suppose K/F is a finite-degree extension and F is finite. Then K is a simple extension of F.

Proof:

- If K/F has finite degree and F is finite, then K is also finite.
- As we have shown, the multiplicative group $K^{\times}$ of any finite field is cyclic.
- If α is any generator, then every nonzero element of K is a power of α, and thus $F(\alpha) = F[\alpha] = K$.

The Primitive Element Theorem, II

Next we prove a characterization of simple extensions in terms of their subfields:

Proposition (Simple Extensions and Subfields)

Suppose K/F is a finite-degree extension. Then $K = F(\alpha)$ for some $\alpha \in K$ if and only if K/F has finitely many intermediate fields.

If F is finite then the result follows immediately from the previous proposition, so for the proof we can assume that F is infinite.

The Primitive Element Theorem, III

Proof:

- First suppose $K = F(\alpha)$ is a simple extension and suppose E is an intermediate field of K/F.
- Let $m(x) \in F[x]$ be the minimal polynomial for α over F and $p(x) \in E[x]$ be the minimal polynomial for α over E, and note that $p(x)$ divides $m(x)$ in $E[x]$.
- If we let E' be the field generated over F by the coefficients of $p(x)$, then clearly $E' \subseteq E$, and the minimal polynomial for α over E' is also $p(x)$. But since $[K : E] = \deg p = [K : E']$, this means $E' = E$.
- We conclude that E is generated over F by the coefficients of some monic polynomial dividing $m(x)$ in $F[x]$. Since there are only finitely many such factors (explicitly, there are at most 2^n such factors where n is the number of roots of $m(x)$), there are finitely many such subfields.

The Primitive Element Theorem, IV

Proof (continued):

- For the converse, suppose K/F has finite degree and finitely many intermediate fields. Then $K = F(\alpha_1, \dots, \alpha_n)$ for some algebraic $\alpha_i \in K$, so it suffices to show that $F(\beta, \gamma)$ is a simple extension for any algebraic β, γ, since then the result for K follows immediately by induction.
- To show this, consider the subfields $F(\beta + x\gamma)$ for $x \in F$: since F is infinite by hypothesis and there are only finitely many intermediate fields of K/F, there must exist distinct $x, y \in F$ such that $F(\beta + x\gamma) = F(\beta + y\gamma)$. Call this field E.
- Then $E \subseteq F(\beta, \gamma)$, and since E contains $\beta + x\gamma$ and $\beta + y\gamma$ it also contains $(x - y)\gamma$, hence γ, since $x - y$ is a nonzero element of F. Then E clearly also contains $\beta = (\beta + x\gamma) - x\gamma$, and so $E = F(\beta, \gamma)$.
- Thus, $E = F(\beta + x\gamma)$ is a simple extension of F, so we win.

The Primitive Element Theorem, V

Using the Galois correspondence, we can then see immediately that a finite-degree Galois extension has finitely many intermediate subfields, since these are in bijection with subgroups of the Galois group (which is a finite group), and is therefore simple. We may extend this result to any separable extension:

Theorem (Primitive Element Theorem)

If K/F is a finite-degree separable extension, then $K = F(\alpha)$ for some $\alpha \in K$. In particular, any finite-degree extension of characteristic-0 fields is a simple extension.

In general, an element α generating the extension K/F is called a primitive element for K/F, whence the name "primitive element theorem".

The Primitive Element Theorem, VI

Proof:

- If K/F is a finite-degree separable extension, then $K = F(\alpha_1, \ldots, \alpha_n)$ for some algebraic $\alpha_1, \ldots, \alpha_n$.
- Let the minimal polynomial of α_i over F be $m_i(x)$, and define $m(x)$ to be the least common multiple of the polynomials $m_i(x)$.
- Then $m(x)$ cannot have any repeated roots, since by definition of the least common multiple this would require one of the m_i to have a repeated root, so $m(x)$ is separable.
- Let L be the splitting field of $m(x)$ over F: then L contains each of $\alpha_1, \ldots, \alpha_n$, hence contains K, and L/F is a Galois extension.

The Primitive Element Theorem, VII

Proof (continued):

- Let L be the splitting field of $m(x)$ over F: then L contains each of $\alpha_1, \dots, \alpha_n$, hence contains K, and L/F is a Galois extension.
- By the fundamental theorem of Galois theory, the intermediate fields of L/F are in bijection with the subgroups of $\mathrm{Gal}(L/F)$. Since $\mathrm{Gal}(L/F)$ is a finite group, it has finitely many subgroups, and so there are finitely many intermediate fields of L/F.
- Since K is a subfield of L/F, this means there are finitely many intermediate fields of K/F also. By the previous result, this means K/F is a simple extension, as claimed.
- The second statement follows immediately, since every extension of characteristic-0 fields is separable.

The Primitive Element Theorem, VIII

Per the proof of the primitive element theorem, if K/F is separable and has finite degree with $K = F(\alpha_1, \ldots, \alpha_n)$ and F is infinite, then we may always construct a primitive element as an F-linear combination of the generators $\alpha_1, \ldots, \alpha_n$.

- If in addition K/F is Galois, then to verify that $\beta \in K$ is a primitive element, we need only check that it is not fixed by any element of the Galois group $\mathrm{Gal}(K/F)$, since then it cannot be an element of any proper subfield of K/F.
- More generally, to determine whether an element β of a non-Galois separable extension K/F is a generator, we may compute all of its Galois conjugates (inside a Galois extension $L/K/F$): if the number of distinct Galois conjugates is equal to the degree $[K : F]$, then β will generate K/F.

The Primitive Element Theorem, IX

Example: If p is a prime, find the degree of the extension $\mathbb{Q}(3^{1/p}, \zeta_p)/\mathbb{Q}$, show it is Galois, and identify its automorphisms.

- Note that $\mathbb{Q}(3^{1/p}, \zeta_p)$ is the splitting field of the Eisenstein-irreducible polynomial $x^p - 3$ over $\mathbb{Q}$, and is also the composite of the fields $\mathbb{Q}(3^{1/p})$ and $\mathbb{Q}(\zeta_p)$, which have degrees p and $p-1$ over $\mathbb{Q}$. Thus, $[K : \mathbb{Q}] = p(p-1)$.
- Any element of the Galois group must map $3^{1/p}$ to one of its p Galois conjugates $3^{1/p}, 3^{1/p}\zeta_p, \dots, 3^{1/p}\zeta_p^{p-1}$ over $\mathbb{Q}$, and must also map ζ_p to one of its $p-1$ Galois conjugates $\zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}$ over $\mathbb{Q}$.
- Since this yields at most $p(p-1)$ choices, each must actually extend to an automorphism of $K/\mathbb{Q}$.
- Thus, the automorphisms are obtained by extending the maps $3^{1/p} \mapsto \{3^{1/p}, 3^{1/p}\zeta_p, \dots, 3^{1/p}\zeta_p^{p-1}\}$ and $\zeta_p \mapsto \{\zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}\}$ to the full field K.

The Primitive Element Theorem, X

Example: If p is a prime, find a primitive element for the Galois extension $\mathbb{Q}(3^{1/p}, \zeta_p)/\mathbb{Q}$.

- To compute a primitive element, let us try the easiest nontrivial linear combination of the generators, namely $\alpha = 3^{1/p} + \zeta_p$.
- We can see that applying all of the automorphisms in the Galois group to α yield the $p(p-1)$ elements $3^{1/p}\zeta_p^a + \zeta_p^b$ for $a \in \{0, 1, \ldots, p-1\}$ and $b \in \{1, 2, \ldots, p-1\}$.
- Since no automorphism fixes α, we conclude that $\alpha = 3^{1/p} + \zeta_p$ is a primitive element for $K/\mathbb{Q}$.
- There are, of course, many other possible choices.

The Primitive Element Theorem, XI

We will also remark that there do exist non-separable finite-degree extensions that are not simple.

- For example, consider the fields $K = \mathbb{F}_p(x^p, y^p)$ and $L = \mathbb{F}_p(x, y)$, where x and y are indeterminates. Then $[L : K] = [L : F(x^p, y)] \cdot [F(x^p, y) : F(x^p, y^p)] = p \cdot p = p^2$.
- On the other hand, there is no primitive element for L/K, because the pth power of every element of L lies in K: taking pth powers does not affect elements in $\mathbb{F}_p$ and respects addition and multiplication, so the result of taking the pth power of a rational function in L is simply to replace x with x^p and y with y^p.
- Therefore, every element of L satisfies a polynomial of degree p with coefficients in K. In particular, there does not exist any element α in L with $[K(\alpha) : K] = p^2$, and so L/K is not a simple extension.

The Primitive Element Theorem, XII

We can explicitly compute an infinite family of intermediate subfields for $L/K = \mathbb{F}_p(x, y)/\mathbb{F}_p(x^p, y^p)$.

- Specifically, we have the intermediate fields $E_n = K(x + y^{1+np})$ for positive integers n.
- Each of these fields is a degree-p extension of K, since $x + y^{1+ap} \notin K$ but as noted earlier its pth power is in K.
- Also, $E_a \neq E_b$ for $a \neq b$, because the composite of $K(x + y^{1+ap})$ and $K(x + y^{1+bp})$ contains the difference $y(y^{ap} - y^{bp})$ and hence y (since the second term is in K), and hence also x.
- This means the composite field of E_a and E_b is $K(x, y) = L$, but since $[L : K] = p^2$ this means the original fields could not have been equal.
- The existence of infinitely many intermediate fields again implies that L/K cannot be a simple extension.

The Primitive Element Theorem, XIII

In fact, the example we gave is essentially the simplest possible non-simple field extension.

- Explicitly, a non-simple extension must be inseparable, so its degree can be reduced to a power of p by taking its purely inseparable part.
- Furthermore, every extension of degree p is simple, as you showed on the midterm exam (it is generated by any element of K not in F).
- Thus, a non-simple field extension of minimal degree must be a purely inseparable extension of degree p^2 over a field of characteristic p.
- This means it has to be of the form $F(\alpha^{1/p}, \beta^{1/p})$ for some $\alpha, \beta \in F$, since if it were generated by taking a p^2 root, it would be simple.

Composite Extensions, I

Next we consider the question of computing Galois groups of composite extensions. The main result is as follows:

Proposition ("Sliding-Up" Galois Extensions)

Suppose K/F is a Galois extension and L/F is any extension. Then the extension KL/L is Galois, and its Galois group is isomorphic to the subgroup $\mathrm{Gal}(K/K \cap L)$ of $\mathrm{Gal}(K/F)$.

Composite Extensions, II

Proof:

- By our characterization of Galois extensions, K is the splitting field of a separable polynomial $p(x)$ over F: explicitly, $K = F(r_1, r_2, \ldots, r_n)$ where the r_i are the roots of $p(x)$ in K.
- Then KL is the splitting field of $p(x)$ over L, since $KL = L(r_1, r_2, \ldots, r_n)$, and so KL/L is Galois.
- Now suppose σ is any automorphism of KL/L: observe that the restriction $\sigma|_K$ of σ to K is an automorphism of K, since $\sigma|_K(K)$ is a Galois conjugate field of K, hence must equal K since K/F is Galois.
- We obtain a well-defined map $\varphi : \mathrm{Gal}(KL/L) \to \mathrm{Gal}(K/F)$ given by restricting an automorphism of KL/L to K/F.
- Trivially, φ is a homomorphism. Also, $\ker \varphi$ consists of automorphisms of KL fixing both L and K, but the only such map is the identity.

Composite Extensions, III

Proof (continued):

- We have a homomorphism $\varphi : \mathrm{Gal}(KL/L) \to \mathrm{Gal}(K/F)$ given by restricting an automorphism of KL/L to K/F.
- For $\mathrm{im}\,\varphi$, observe that every element in $\mathrm{im}(\varphi)$ must fix the elements of L inside K, hence $\mathrm{im}(\varphi) \leq \mathrm{Gal}(K/K \cap L)$.
- Now let E be the fixed field of $\mathrm{im}(\varphi)$: then the observation above shows that E contains $K \cap L$.
- Also, EL is fixed by $\mathrm{Gal}(KL/L)$, since any $\sigma \in \mathrm{Gal}(KL/L)$ fixes L and its restriction to K fixes E (by definition).
- Thus, by the fundamental theorem of Galois theory, we see that $EL = L$, and hence $E \subseteq L$. Since $E \subseteq K$ this means $E \subseteq K \cap L$, and so we must have $E = K \cap L$.
- Hence again by the fundamental theorem of Galois theory, we conclude that $\mathrm{im}(\varphi) = \mathrm{Gal}(K/E) = \mathrm{Gal}(K/K \cap L)$.

Composite Extensions, IV

As a corollary, we obtain a useful formula for the degree of a composite extension where at least one of the fields is Galois:

Corollary (Degree of Composite)

Suppose K/F is a Galois extension and L/F is any finite-degree extension. Then $[KL : F] = \dfrac{[K : F] \cdot [L : F]}{[K \cap L : F]}$.

Proof:

- From the previous result, we know that $\mathrm{Gal}(KL/L) \cong \mathrm{Gal}(K/K \cap L)$, and therefore by the fundamental theorem of Galois theory, $[KL : L] = [K : K \cap L]$.
- Then $[KL : F] = [KL : L] \cdot [L : F] = [K : K \cap L] \cdot [L : F] = \dfrac{[K : F] \cdot [L : F]}{[K \cap L : F]}$, as claimed.

Composite Extensions, V

We may also say more about the Galois group of the composite of two Galois extensions:

Proposition (Galois Groups of Composites)

If K_1/F and K_2/F are Galois, then K_1K_2/F is also Galois and its Galois group is isomorphic to the subgroup of $\mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$ consisting of elements whose restrictions to $K_1 \cap K_2$ are equal.

In particular, if $K_1 \cap K_2 = F$, then $\mathrm{Gal}(K_1K_2/F) \cong \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$.

Composite Extensions, VI

Proof:

- If K_1 and K_2 are Galois over F then they are splitting fields of some separable polynomials $p_1(x)$ and $p_2(x)$.
- Then the composite field K_1K_2 is the splitting field of the least common multiple of $p_1(x)$ and $p_2(x)$, which as we have previously noted is also separable.
- Therefore, K_1K_2/F is also Galois.
- To compute the Galois group, observe that the action of any automorphism on K_1K_2/F is completely determined by its actions on K_1/F and K_2/F (since the elements of K_1 and K_2 generate K_1K_2), and so we have a homomorphism $\varphi : \mathrm{Gal}(K_1K_2)/F \to \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$ given by $\varphi(\sigma) = (\sigma_{K_1}, \sigma_{K_2})$.
- This map φ is clearly injective, since any automorphism fixing both K_1 and K_2 fixes K_1K_2.

Composite Extensions, VII

Proof (continued):

- We have $\varphi : \mathrm{Gal}(K_1K_2)/F \to \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$ given by $\varphi(\sigma) = (\sigma_{K_1}, \sigma_{K_2})$.
- To compute $\mathrm{im}(\varphi)$, first observe that $\mathrm{im}(\varphi)$ is certainly contained in the subgroup H of $\mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$ consisting of elements whose restrictions to $K_1 \cap K_2$ are equal.
- Furthermore, notice that for any fixed $\tau \in \mathrm{Gal}(K_2/F)$, there are $|\mathrm{Gal}(K_1/K_1 \cap K_2)|$ automorphisms $\sigma \in \mathrm{Gal}(K_1/F)$ such that $\sigma|_{K_1 \cap K_2} = \tau|_{K_1 \cap K_2}$, and so $|H| =$ $|\mathrm{Gal}(K_2/F)| \cdot |\mathrm{Gal}(K_1/K_1 \cap K_2)| = [K_2 : F] \cdot [K_1 : K_1 \cap K_2]$.
- By the sliding-up result, $\mathrm{Gal}(K_1K_2/K_2) \cong \mathrm{Gal}(K_1/K_1 \cap K_2)$ and thus $[K_1K_2 : K_2] = [K_1 : K_1 \cap K_2]$.
- Hence $|\mathrm{im}(\varphi)| = |\mathrm{Gal}(K_1K_2)/F| = [K_1K_2 : F]$ $= [K_1K_2 : K_2] \cdot [K_2 : F] = [K_1 : K_1 \cap K_2] \cdot [K_2 : F]$.
- Thus we see that $|H| = |\mathrm{im}(\varphi)|$.

Composite Extensions, VIII

Proof (continued more):

- We have $\varphi : \mathrm{Gal}(K_1K_2)/F \to \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$ given by $\varphi(\sigma) = (\sigma_{K_1}, \sigma_{K_2})$.
- Since $|H| = |\mathrm{im}(\varphi)|$, that means $H = \mathrm{im}\,\varphi$.
- Therefore, since $\ker\varphi$ is trivial, we see that $\mathrm{Gal}(K_1K_2/F)$ is isomorphic to the subgroup of $\mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$ consisting of elements whose restrictions to $K_1 \cap K_2$ are equal, as claimed.
- In particular, if $K_1 \cap K_2 = F$, then every element (σ, τ) in the direct product has $\sigma|_{K_1 \cap K_2} = \tau|_{K_1 \cap K_2}$.
- Then $\mathrm{Gal}(K_1K_2/F) \cong \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$.

Composite Extensions, IX

In cases where we can compute $K_1 \cap K_2$, this allows us to determine Galois groups for composite fields explicitly.

- For general fields K_1 and K_2, of course, computing the field intersection can be difficult, since it is not always obvious what kinds of algebraic relations may exist between the generators.
- Our main basic tools are to use properties of extension degrees and to exploit the fact that some elements are real and others are not.

Composite Extensions, X

Example: Find the degree of $\mathbb{Q}(2^{1/3}, 3^{1/2}, \zeta_3)/\mathbb{Q}$ and describe its Galois group.

Composite Extensions, X

Example: Find the degree of $\mathbb{Q}(2^{1/3}, 3^{1/2}, \zeta_3)/\mathbb{Q}$ and describe its Galois group.

- Observe that $L = \mathbb{Q}(2^{1/3}, 3^{1/2}, \zeta_3)$ is the composite of the Galois extensions $K_1 = \mathbb{Q}(2^{1/3}, \zeta_3)$ and $K_2 = \mathbb{Q}(3^{1/2})$.
- Now observe that K_1 has a unique quadratic subfield, namely $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$, which is not equal to K_2. Hence we have $K_1 \cap K_2 = \mathbb{Q}$.
- Then by the degree formula we have $[K_1 K_2 : \mathbb{Q}] = \dfrac{[K_1 : \mathbb{Q}] \cdot [K_2 : \mathbb{Q}]}{[K_1 \cap K_2 : \mathbb{Q}]} = 12.$
- The Galois group is simply the direct product $\mathrm{Gal}(K_1/\mathbb{Q}) \times \mathrm{Gal}(K_2/\mathbb{Q}) \cong S_3 \times (\mathbb{Z}/2\mathbb{Z})$.

Composite Extensions, XI

Example: Find the degree of $\mathbb{Q}(2^{1/3}, 3^{1/3}, \zeta_3)/\mathbb{Q}$ and describe its Galois group.

- Observe that $L = \mathbb{Q}(2^{1/3}, 3^{1/3}, \zeta_3)$ is the composite of the Galois extensions $K_1 = \mathbb{Q}(2^{1/3}, \zeta_3)$ and $K_2 = \mathbb{Q}(3^{1/3}, \zeta_3)$.
- Then $K_1 \cap K_2$ certainly contains $\mathbb{Q}(\zeta_3)$ and is contained in K_1, so since $[K_1 : \mathbb{Q}(\zeta_3)] = 3$ we must have either $K_1 \cap K_2 = K_1$ or $K_1 \cap K_2 = \mathbb{Q}(\zeta_3)$.
- If $K_1 \cap K_2 = K_1$ then we would also have $K_1 \cap K_2 = K_2$ by degree considerations, and then K_1 would equal K_2.
- But this is not possible, because it would imply that $3^{1/3} \in \mathbb{Q}(2^{1/3})$, which is not true.

Composite Extensions, XI

<u>Example</u>: Find the degree of $\mathbb{Q}(2^{1/3}, 3^{1/3}, \zeta_3)/\mathbb{Q}$ and describe its Galois group.

- It is intuitively obvious that $3^{1/3} \notin \mathbb{Q}(2^{1/3})$.
- But for completeness, here is a rigorous argument.
- First observe that any element σ of the Galois group has the property that $\sigma(3^{1/3})/3^{1/3}$ is a 3rd root of unity.
- Now note that the only elements $z \in \mathbb{Q}(2^{1/3})$ with $\sigma(z)/z$ equal to a third root of unity for all $\sigma \in \mathrm{Gal}(K_1/\mathbb{Q})$ are rational multiples of $\{1, 2^{1/3}, 4^{1/3}\}$.
- Finally, $3^{1/3}$ is not equal to any of these, since none of $3^{1/3}$, $6^{1/3}$, $12^{1/3}$ are rational (and this follows by the rational root test or Eisenstein's criterion).

Composite Extensions, XII

Example: Find the degree of $\mathbb{Q}(2^{1/3}, 3^{1/3}, \zeta_3)/\mathbb{Q}$ and describe its Galois group.

- Hence $K_1 \cap K_2 = \mathbb{Q}(\zeta_3)$, and so by the degree formula we see that $[K_1 K_2 : \mathbb{Q}] = \dfrac{[K_1 : \mathbb{Q}] \cdot [K_2 : \mathbb{Q}]}{[K_1 \cap K_2 : \mathbb{Q}]} = \dfrac{6 \cdot 6}{2} = 18$.
- The Galois group is the subgroup of $\mathrm{Gal}(K_1/\mathbb{Q}) \times \mathrm{Gal}(K_2/\mathbb{Q}) \cong S_3 \times S_3$ of pairs (σ, τ) where $\sigma|_{\mathbb{Q}(\zeta_3)} = \tau|_{\mathbb{Q}(\zeta_3)}$.
- These are the maps $\varphi(2^{1/3}, 3^{1/3}, \zeta_3) = (2^{1/3}\zeta_3^a,\ 3^{1/3}\zeta_3^b,\ \zeta_3^c)$ where $a \in \{0, 1, 2\}$, $b \in \{0, 1, 2\}$, and $c \in \{1, 2\}$.
- It is easy to see that every element in the Galois group must be of this form, and conversely since $|\mathrm{Gal}(K_1 K_2/\mathbb{Q})| = 18$, each of these 18 choices does extend to an automorphism.
- This group is also a semidirect product $(C_3 \times C_3) \rtimes C_2$ (the C_3 factors are the maps on the cube roots of 2 and 3, while the C_2 is complex conjugation).

Composite Extensions, XIII

One may extend the arguments we gave here to analyze general "radical extensions" obtained by adjoining various roots of elements.

- The study of such extensions is generally referred to as Kummer theory.
- In general, the structures of these extensions have a similar form to the ones we described in the last two examples, and the Galois groups will be obtained as (iterated) semidirect products.
- In order to study these general radical extensions, the first step is to look at cyclotomic extensions, which are obtained by adjoining roots of unity.

Cyclotomic Extensions, I

Our first goal is to compute the degree and the Galois group of the cyclotomic extension $\mathbb{Q}(\zeta_n)$ for an arbitrary positive integer n.

- To do this, we require some facts about the nth roots of unity.
- As we have observed previously, the group $\mu_n = \{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\}$ of nth roots of unity is cyclic of order n and generated by ζ_n. We have an explicit isomorphism of μ_n with $\mathbb{Z}/n\mathbb{Z}$ given by associating ζ_n^k with $\overline{k}$.
- From properties of order, we see that the order of ζ_n^k is $n/\gcd(n, k)$, so in particular ζ_n^k has order n precisely when k is relatively prime to n (equivalently, when k is a unit modulo n).
- If ζ is an nth root of unity of order n, we call it a <u>primitive</u> nth root of unity: by the above remarks, the number of primitive nth roots of unity is $\#(\mathbb{Z}/n\mathbb{Z})^\times$.

Cyclotomic Extensions, II

The number of units modulo n is an important quantity that often shows up in number theory:

Definition

If n is a positive integer, the Euler φ-function $\varphi(n)$, also sometimes called the Euler totient function, is the number of units in $\mathbb{Z}/n\mathbb{Z}$. Equivalently, $\varphi(n)$ is the number of positive integers k with $1 \leq k \leq n$ that are relatively prime to n.

Examples:

1. $\varphi(6) = 2$ since there are 2 units modulo 6, namely $\overline{1}$ and $\overline{5}$.
2. $\varphi(p) = p - 1$ if p is prime since $\mathbb{Z}/p\mathbb{Z}$ has $p - 1$ units.
3. $\varphi(20) = 8$ as the units mod 20 are $\overline{1}$, $\overline{3}$, $\overline{7}$, $\overline{9}$, $\overline{11}$, $\overline{13}$, $\overline{17}$, $\overline{19}$.

Cyclotomic Extensions, III

We can give an explicit formula for the value of $\varphi(n)$:

Proposition (Value of $\varphi(n)$)

If p is a prime, then $\varphi(p^k) = p^k - p^{k-1}$, and for any relatively prime integers a and b we also have $\varphi(ab) = \varphi(a)\varphi(b)$. Thus, if n has prime factorization $n = \prod_i p_i^{a_i}$, we have $\varphi(n) = \prod_i p_i^{a_i-1}(p_i - 1) = n \cdot \prod_i (1 - 1/p_i)$.

Examples:

1. $\varphi(60) = \varphi(2^2 \cdot 3 \cdot 5) = \varphi(2^2)\varphi(3)\varphi(5) = 2 \cdot 2 \cdot 4 = 16$.
2. $\varphi(2000) = \varphi(2^4 5^3) = \varphi(2^4)\varphi(5^3) = (2^4 - 2^3)(5^3 - 5^2) = 800$.

Cyclotomic Extensions, IV

Proof:

- If p is a prime, then $\varphi(p^k) = p^k - p^{k-1}$, since the integers with $1 \leq k \leq p^k$ not relatively prime to p^k are simply the multiples of p, of which there are p^{k-1}.
- For the second statement, by the Chinese remainder theorem we know $(\mathbb{Z}/ab\mathbb{Z})^\times$ and $(\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times$ are isomorphic.
- Comparing cardinalities shows that $\varphi(ab) = \varphi(a)\varphi(b)$ for any relatively prime integers a and b.
- For the last statement, we simply write n as a product of prime powers and then apply the two results we have just established to conclude that $\varphi(n) = \prod_i p_i^{a_i - 1}(p_i - 1)$.
- The second formula $\varphi(n) = n \cdot \prod_i (1 - 1/p_i)$. follows by pulling out a factor of $p_i^{a_i}$ from each term.

Cyclotomic Extensions, V

Definition

The <u>nth cyclotomic polynomial</u> $\Phi_n(x)$ is the monic polynomial of degree $\varphi(n)$ whose roots are the primitive nth roots of unity: $\Phi_n(x) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - \zeta_n^k)$.

Observe that the roots of $x^n - 1$ are all of the nth roots of unity.

- So, if we group together all of the primitive dth roots of unity for each $d|n$, we see that $x^n - 1 = \prod_{d|n} \Phi_d(x)$. (Computing the degree of both sides also establishes the identity $n = \sum_{d|n} \varphi(d)$ for the Euler φ-function.)
- This yields a recursion that we can use to compute $\Phi_n(x)$: for example, $x^6 - 1 = \Phi_6(x)\Phi_3(x)\Phi_2(x)\Phi_1(x)$, so
$$\Phi_6(x) = \frac{x^6 - 1}{(x^2 + x + 1)(x + 1)(x - 1)} = x^2 - x + 1.$$

Cyclotomic Extensions, VI

In fact, we can use a multiplicative version of Möbius inversion to solve $x^n - 1 = \prod_{d|n} \Phi_d(x)$ for the cyclotomic polynomials.

- Recall that if $f(n)$ is any sequence satisfying a recursive relation of the form $g(n) = \sum_{d|n} f(d)$, for some function $g(n)$, then $f(n) = \sum_{d|n} \mu(d) g(n/d)$.
- Exponentiating both sides and replacing f and g with their exponentials yields the multiplicative version: if $g(n) = \prod_{d|n} f(d)$, then $f(n) = \prod_{d|n} [g(n/d)]^{\mu(d)}$.
- Thus, we see $\Phi_n(x) = \prod_{d|n} [x^{n/d} - 1]^{\mu(d)}$.
- <u>Example</u>:
$$\Phi_{20}(x) = \frac{(x^{20}-1)(x^2-1)}{(x^{10}-1)(x^4-1)} = x^8 - x^6 + x^4 - x^2 + 1.$$
- From this recursion we can see by induction on n and Gauss's lemma that $\Phi_n(x)$ will always have integer coefficients.

Cyclotomic Extensions, VII

We have previously shown that if p is prime, then $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible over $\mathbb{Q}$. We now extend this result to all of the polynomials $\Phi_n(x)$:

Theorem (Irreducibility of Cyclotomic Polynomials)

For any positive integer n, the cyclotomic polynomial $\Phi_n(x)$ is irreducible over $\mathbb{Q}$, and therefore $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

Cyclotomic Extensions, VIII

Proof:

- Suppose we have an irreducible monic factor of $\Phi_n(x)$ in $\mathbb{Q}[x]$.
- By Gauss's lemma, this yields a factorization $\Phi_n(x) = f(x)g(x)$ where $f(x), g(x) \in \mathbb{Z}[x]$ are monic and $f(x)$ is irreducible.
- Let ω be a primitive nth root of unity that is a root of f, and let p be any prime not dividing n. Since f is irreducible, this means f is the minimal polynomial of ω.
- By properties of order, we see that ω^p is also a primitive nth root of unity, hence is a root of either f or of g.
- We will show it is in fact a root of f.

Cyclotomic Extensions, IX

Proof (continued):

- So suppose ω^p is a root of g: then $g(\omega^p) = 0$.
- This means ω is a root of $g(x^p)$, and so since f is the minimal polynomial of ω, it must divide $g(x^p)$: say $f(x)h(x) = g(x^p)$ for some $h(x) \in \mathbb{Z}[x]$.
- Modulo p, this says $\overline{f}(x)\overline{h}(x) = \overline{g}(x^p) = \overline{g}(x)^p$.
- By unique factorization in $\mathbb{F}_p[x]$, we see that $\overline{f}(x)$ and $\overline{g}(x)$ have a nontrivial common factor in $\mathbb{F}_p[x]$.
- Then since $\Phi_n(x) = f(x)g(x)$, reducing modulo p yields $\overline{\Phi_n}(x) = \overline{f}(x)\overline{g}(x)$ and so $\overline{\Phi_n}(x)$ would have a repeated factor, hence so would $x^n - 1$.
- But this is a contradiction because since $x^n - 1$ is separable in $\mathbb{F}_p[x]$ (its derivative is nx^{n-1}, which is relatively prime to $x^n - 1$ because p does not divide n).
- Thus, ω^p is not a root of g, so it must be a root of f.

Cyclotomic Extensions, X

Proof (continued more):

- So: for any primitive nth root of unity ω, and any prime p not dividing n, we see that ω^p is a root of f.
- Therefore, we see that for any $a = p_1 p_2 \cdots p_k$ that is relatively prime to n, then $\omega^a = ((\omega^{p_1})^{p_2})^{\cdots p_n}$ is a root of f.
- But this means every primitive nth root of unity is a root of f, and so $\Phi_n = f$ is irreducible as claimed.
- Then the fact that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ follows immediately, because $\Phi_n(x)$ is then the minimal polynomial of ζ_n, so $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg(\Phi_n) = \varphi(n)$.

Cyclotomic Extensions, XI

We can now easily compute the Galois group of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$:

Theorem (Galois Group of $\mathbb{Q}(\zeta_n)$)

The extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois with Galois group isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$. Explicitly, the elements of the Galois group are the automorphisms σ_a for $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ acting via $\sigma_a(\zeta_n) = \zeta_n^a$.

The argument is essentially the same one we used to compute the Galois group of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. The only missing piece of information here was that the degree of $\mathbb{Q}(\zeta_n)$ is equal to $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$.

The only remaining computational aspect to writing down the Galois group structure is to find the structure of the abelian group $(\mathbb{Z}/n\mathbb{Z})^\times$, which you will do on Homework 11.

Cyclotomic Extensions, XII

Proof:

- Since $K = \mathbb{Q}(\zeta_n)$ is the splitting field of $x^n - 1$ (or $\Phi_n(x)$) over $\mathbb{Q}$ it is Galois, and $|\mathrm{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}] = \varphi(n)$.
- Any automorphism σ must map ζ_n to one of its Galois conjugates over $\mathbb{Q}$, which are the roots of $\Phi_n(x)$: explicitly, these are the $\varphi(n)$ values ζ_n^a for a relatively prime to n.
- Since there are in fact $\varphi(n)$ possible automorphisms, each of these choices must extend to an automorphism of $K/\mathbb{Q}$.
- Hence the elements of the Galois group are the maps σ_a as claimed. Since $\sigma_a(\sigma_b(\zeta_n)) = \sigma_a(\zeta_n^b) = \zeta_n^{ab}$, the composition of automorphisms is the same as multiplication of the indices in $(\mathbb{Z}/n\mathbb{Z})^\times$, and since this association is a bijection, the Galois group is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$.

Summary

We discussed finite fields and irreducible polynomials mod p.

We proved the primitive element theorem.

We discussed some properties of composite extensions.

Next lecture: Cyclotomic extensions, symmetric functions, discriminants, cubic polynomials.