Math 5111 (Algebra 1)

Lecture #22 of 24 $\sim$ November 30th, 2020

Cyclotomic and Abelian Extensions, Galois Groups of Polynomials

- Cyclotomic and Abelian Extensions
- Constructible Polygons
- Galois Groups of Polynomials
- Symmetric Functions and Discriminants
- Cubic Polynomials

This material represents §4.3.4-4.4.3 from the course notes.

Cyclotomic and Abelian Extensions, 0

Last time, we defined the general cyclotomic polynomials and showed they were irreducible:

Theorem (Irreducibility of Cyclotomic Polynomials)

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

We also computed the Galois group:

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 $\sigma_a(\zeta_n) = \zeta_n^a$.

Cyclotomic and Abelian Extensions, I

By using the structure of the Galois group we can in principle compute all of the subfields of $\mathbb{Q}(\zeta_n)$.

- In practice, however, this tends to be computationally difficult when the subgroup structure of $(\mathbb{Z}/n\mathbb{Z})^\times$ is complicated.
- The simplest case occurs when $n = p$ is prime, in which case (as we have shown already) the Galois group $G \cong (\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p - 1$.
- In this case, let σ be a generator of the Galois group, with $\sigma(\zeta_p) = \zeta_p^a$ where a is a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$.
- Then by the Galois correspondence, the subfields of $\mathbb{Q}(\zeta_p)$ are the fixed fields of σ^d for the divisors d of $p - 1$.

Cyclotomic and Abelian Extensions, II

We may compute an explicit generator for each of these fixed fields by exploiting the action of the Galois group on the basis $\{\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}\}$ for $\mathbb{Q}(\zeta_p)/\mathbb{Q}$.

- This set is obtained from the standard basis $\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$ using the relation $\zeta_p^{p-1} + \zeta_p^{p-2} + \cdots + \zeta_p + 1 = 0$ from the minimal polynomial of ζ_p.
- Since all of these basis elements are Galois conjugates, the action of any element of the Galois group permutes them.

Cyclotomic and Abelian Extensions, III

For any subgroup H of G, define the element $\alpha_H = \sum_{\sigma \in H} \sigma(\zeta_p)$.

- We claim that α_H is a generator for the fixed field of H.
- To see this, observe first that if $\tau \in H$, then $\tau(\alpha_H) = \alpha_H$ because τ merely permutes the elements $\sigma(\zeta_p)$ for $\sigma \in H$.
- Conversely, because the elements $\sigma(\zeta_p)$ for $\sigma \in G$ form a basis, if $\tau \in G$ has $\tau(\alpha_H) = \alpha_H$ then $\tau(\zeta_p)$ must equal $\sigma(\zeta_p)$ for some $\sigma \in H$. But then $\tau\sigma^{-1}$ acts as the identity on ζ_p and hence on all of $\mathbb{Q}(\zeta_p)$, so it must be the identity element: thus, $\tau = \sigma \in H$.
- We conclude that the automorphisms fixing α_H are precisely the elements of H, and so $\mathbb{Q}(\alpha_H)$ is the fixed field of H.

Cyclotomic and Abelian Extensions, IV

Example: Find generators for each of the subfields of $\mathbb{Q}(\zeta_7)$.

- We know that $G = \mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/7\mathbb{Z})^\times$. By trial and error we can see that $\overline{3}$ has order 6 in $(\mathbb{Z}/7\mathbb{Z})^\times$, so it is a generator. The corresponding automorphism generating G is the map σ with $\sigma(\zeta_7) = \zeta_7^3$.
- The subgroups of G are then $\langle\sigma\rangle = \{e, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5\}$, $\langle\sigma^2\rangle = \{e, \sigma^2, \sigma^4\}$, $\langle\sigma^3\rangle = \{e, \sigma^3\}$, and $\langle\sigma^6\rangle = \{e\}$.
- A generator of the fixed field of $\langle\sigma\rangle$ is given by $\zeta_7 + \sigma(\zeta_7) + \sigma^2(\zeta_7) + \sigma^3(\zeta_7) + \sigma^4(\zeta_7) + \sigma^5(\zeta_7) = \zeta_7 + \zeta_7^3 + \zeta_7^2 + \zeta_7^6 + \zeta_7^4 + \zeta_7^5$.
- Similarly, the fixed field of $\langle\sigma^2\rangle$ is generated by $\zeta_7 + \sigma^2(\zeta_7) + \sigma^4(\zeta_7) = \zeta_7 + \zeta_7^2 + \zeta_7^4$, while the fixed field of $\langle\sigma^3\rangle$ is generated by $\zeta_7 + \sigma^3(\zeta_7) = \zeta_7 + \zeta_7^6$.

Cyclotomic and Abelian Extensions, V

Example: Find generators for each of the subfields of $\mathbb{Q}(\zeta_7)$.

- We can also use the Galois action to compute the minimal polynomials of each of these elements, since we may compute all of these elements' Galois conjugates.
- For example, the element $\zeta_7 + \zeta_7^2 + \zeta_7^4$ has one other Galois conjugate inside $\mathbb{Q}(\zeta_7)$, namely $\zeta_7^3 + \zeta_7^5 + \zeta_7^6$.
- Then their common minimal polynomial is $m(x) = [x - (\zeta_7 + \zeta_7^2 + \zeta_7^4)] \cdot [x - (\zeta_7^3 + \zeta_7^5 + \zeta_7^6)] = x^2 + x + 2$, as follows from multiplying out and simplifying the coefficients.
- Solving the quadratic yields an explicit formula $\zeta_7 + \zeta_7^2 + \zeta_7^4 = \frac{-1-\sqrt{-7}}{2}$, and thus the corresponding fixed field $\mathbb{Q}(\zeta_7 + \zeta_7^2 + \zeta_7^4) = \mathbb{Q}(\sqrt{-7})$.

Cyclotomic and Abelian Extensions, VI

Example: Find generators for each of the subfields of $\mathbb{Q}(\zeta_7)$.

- Similarly, the element $\zeta_7 + \zeta_7^6 = 2\cos(2\pi/7)$ has two other Galois conjugates, namely $\zeta_7^2 + \zeta_7^5 = 2\cos(4\pi/7)$ and $\zeta_7^3 + \zeta_7^4 = 2\cos(6\pi/7)$.
- Their common minimal polynomial is $m(x) = [x - (\zeta_7 + \zeta_7^6)] \cdot [x - (\zeta_7^2 + \zeta_7^5)][x - (\zeta_7^3 + \zeta_7^4)] = x^3 + x^2 - 2x - 1$.
- Our analysis indicates that the splitting field of this polynomial is $\mathbb{Q}(\zeta_7 + \zeta_7^6) = \mathbb{Q}(\zeta_7^2 + \zeta_7^5) = \mathbb{Q}(\zeta_7^3 + \zeta_7^4)$, that it has degree 3 over $\mathbb{Q}$, and that its Galois group is cyclic of order 3. is cyclic of order 3.

Cyclotomic and Abelian Extensions, VII

For other n, we can perform similar computations, although there is not usually as convenient a basis available.

- In general, the primitive nth roots of unity form a basis for $\mathbb{Q}(\zeta_n)$ precisely when n is squarefree.
- When n is prime, the main computational requirement is finding a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$.
- For other n, we can simplify some of these computations by writing $\mathbb{Q}(\zeta_n)$ as a composite of smaller cyclotomic fields.

Cyclotomic and Abelian Extensions, VIII

We can essentially reduce most computations down to working in the individual prime-power cyclotomic fields:

Proposition (Composites of Cyclotomic Extensions)

If a and b are relatively prime integers, then the composite of $\mathbb{Q}(\zeta_a)$ and $\mathbb{Q}(\zeta_b)$ is $\mathbb{Q}(\zeta_{ab})$, the intersection is $\mathbb{Q}$, and $\mathrm{Gal}(\mathbb{Q}(\zeta_{ab})/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_a)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_b)/\mathbb{Q})$.

In particular, if the prime factorization of n is $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, then $\mathbb{Q}(\zeta_n)$ is the composite of the fields $\mathbb{Q}(\zeta_{p_i^{a_i}})$ for $1 \leq i \leq k$, and $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{p_1^{a_1}})/\mathbb{Q}) \times \cdots \times \mathrm{Gal}(\mathbb{Q}(\zeta_{p_k^{a_k}})/\mathbb{Q})$.

More generally, for any a and b, the composite of $\mathbb{Q}(\zeta_a)$ and $\mathbb{Q}(\zeta_b)$ is $\mathbb{Q}(\zeta_{\mathrm{lcm}(a,b)})$ and the intersection is $\mathbb{Q}(\zeta_{\gcd(a,b)})$.

Cyclotomic and Abelian Extensions, IX

Proof:

- Observe that $\zeta_{ab}^{b} = \zeta_a$ and $\zeta_{ab}^{a} = \zeta_b$, so both ζ_a and ζ_b are in $\mathbb{Q}(\zeta_{ab})$: thus, the composite field is contained in $\mathbb{Q}(\zeta_{ab})$.
- Also, since a and b are relatively prime, there exist integers s and t with $sa + tb = 1$. Then $\zeta_b^s \cdot \zeta_a^t = \zeta_{ab}^{as+bt} = \zeta_{ab}$, and so ζ_{ab} is contained in the composite field of $\mathbb{Q}(\zeta_a)$ and $\mathbb{Q}(\zeta_b)$.
- Hence the composite field is $\mathbb{Q}(\zeta_{ab})$. Also since $[\mathbb{Q}(\zeta_{ab}) : \mathbb{Q}] = \varphi(ab) = \varphi(a)\varphi(b) = [\mathbb{Q}(\zeta_a) : \mathbb{Q}] \cdot [\mathbb{Q}(\zeta_b) : \mathbb{Q}]$, by the formula for the degree of a composite extension we must have $[\mathbb{Q}(\zeta_a) \cap \mathbb{Q}(\zeta_b) : \mathbb{Q}] = 1$ so $\mathbb{Q}(\zeta_a) \cap \mathbb{Q}(\zeta_b) = \mathbb{Q}$.
- The statement about the Galois group of $\mathbb{Q}(\zeta_{ab})/\mathbb{Q}$ follows immediately from our result on the Galois group of a composite of Galois extensions.
- The second statement then follows by a trivial induction by breaking n into the individual prime power factors.

Cyclotomic and Abelian Extensions, X

By using this decomposition of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, we can show that every abelian group appears as a Galois group over $\mathbb{Q}$:

Theorem (Abelian Galois Groups over $\mathbb{Q}$)

If G is an abelian group, then there exists an extension $K/\mathbb{Q}$ with Galois group isomorphic to G.

For general finite groups G, it is still an open problem whether G is the Galois group of some extension $K/\mathbb{Q}$.

- The problem of computing which groups occur as Galois groups over $\mathbb{Q}$, or more generally over an arbitrary field F, is known as the inverse Galois problem.

Cyclotomic and Abelian Extensions, XI

Proof:

- By the classification of finite abelian groups, G is isomorphic to a direct product of cyclic groups, say as $G \cong (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_k\mathbb{Z})$.
- By a theorem of Dirichlet, for any positive integer m there exist infinitely many primes congruent to 1 modulo m. In particular, we may choose distinct primes p_i such that $p_i \equiv 1$ mod m_i for each i.
- Then since m_i divides $|\mathrm{Gal}(\mathbb{Q}(\zeta_{p_i})/\mathbb{Q}| = p_i - 1$ and $\mathrm{Gal}(\mathbb{Q}(\zeta_{p_i})/\mathbb{Q}$ is cyclic, there exists a subgroup of index m_i.

Cyclotomic and Abelian Extensions, XII

Proof (continued):

- If K_i represents the corresponding fixed field, then $K_i/\mathbb{Q}$ is Galois (since $\mathrm{Gal}(\mathbb{Q}(\zeta_{p_i})/\mathbb{Q}$ is abelian, so every subgroup is normal) and by the fundamental theorem of Galois theory we see that its Galois group is cyclic of order m_i.
- By our results on cyclotomic fields, since the p_i are distinct primes, the intersection of any two of the fields $\mathbb{Q}(\zeta_{p_i})$ is $\mathbb{Q}$, so the same holds for the fields K_i.
- Hence by our results on Galois groups of composites, we see that the Galois group of $K = K_1K_2\cdots K_k$ over $\mathbb{Q}$ is isomorphic to $\mathrm{Gal}(K_1/\mathbb{Q}) \times \mathrm{Gal}(K_2/\mathbb{Q}) \times \cdots \times \mathrm{Gal}(K_k/\mathbb{Q}) \cong (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_k\mathbb{Z}) \cong G$, as desired.

Cyclotomic and Abelian Extensions, XIII

Perhaps surprisingly, the converse of this theorem is also true (although much harder to prove):

Theorem (Kronecker-Weber)

If $K/\mathbb{Q}$ is a Galois extension with abelian Galois group, then K is contained in a cyclotomic extension of $\mathbb{Q}$.

- This theorem was originally stated and mostly proven by Kronecker in the 1850s (his argument contained gaps in the case where the Galois group had order a power of 2), and Weber gave another proof in the 1880s (which also contained some gaps).

Cyclotomic and Abelian Extensions, XIV

In general, if $\mathrm{Gal}(K/F)$ is abelian, we say that K/F is an abelian extension.

- Since abelian groups are (in a sense) the least complicated finite groups, abelian extensions tend to be particularly well-behaved: for example, all of their intermediate fields are Galois.
- The problem of understanding the structure of all abelian extensions of other finite-degree extensions of $\mathbb{Q}$ falls under the branch of number theory known as class field theory, which generalizes and combines many threads from classical number theory, and has in turn been generalized and extended in other ways.

Cyclotomic and Abelian Extensions, XV

As a final remark, we note that it is also possible to apply most of these results to study the roots of unity over an arbitrary field F.

- Since the polynomials $\Phi_n(x)$ are monic and have integer coefficients, the primitive nth roots of unity will still be the roots of $\Phi_n(x)$, although $\Phi_n(x)$ may no longer be irreducible or separable over F.
- Indeed, $x^n - 1$ (and, essentially equivalently, $\Phi_n(x)$) is separable over F if and only if $\mathrm{char}(F)$ does not divide n.
- In general, if ζ_n is any primitive nth root of unity, then $F(\zeta_n)/F$ is the splitting field of $\Phi_n(x)$ and if $\Phi_n(x)$ is separable, it will be Galois with cyclic Galois group.
- The inseparable case is also easy: if $p = \mathrm{char}(F)$ does divide n, there is only one p-power root of unity over F (namely, 1).

Constructible Numbers, I

Using the fundamental theorem of Galois theory, we can also give another characterization of constructible numbers, which will serve as a prototype for our work next week on solvability in radicals:

Theorem (Constructible Numbers)

The number $\alpha \in \mathbb{C}$ is constructible over $\mathbb{Q}$ if and only if the Galois group of the splitting field of its minimal polynomial over $\mathbb{Q}$ has order a power of 2.

To prove this result we will require a lemma, which I had intended to put in the group theory chapter but forgot:

Lemma

If G is a finite p-group, then there exists a chain of subgroups $G = G_0 \geq G_1 \geq \cdots \geq G_n = \{e\}$ such that $[G_i : G_{i+1}]$ has order p for each i.

Constructible Numbers, II

Proof (of lemma):

- We induct on n. The base case $n = 1$ is trivial, since we have the obvious chain $G = G_0 \geq G_1 = \{e\}$.
- For the inductive step, recall that p-groups have nontrivial centers. By taking an appropriate power we may assume $z \in Z(G)$ has order p: then the subgroup $\langle z \rangle$ has order p and is normal in G (since it is contained in the center).
- The quotient group $\overline{G} = G/\langle z \rangle$ therefore has order p^{n-1} so by the inductive hypothesis it has a chain of subgroups $\overline{G} \geq \overline{G_1} \geq \cdots \geq \overline{G_{n-1}} = \{\overline{e}\}$ where $[\overline{G_i} : \overline{G_{i+1}}] = p$ for each i.
- By the fourth isomorphism theorem, we may lift each of the $\overline{G_i}$ to a subgroup G_i of G containing $\langle z \rangle$ with $G_i/G_{i+1} \cong \overline{G_i}/\overline{G_{i+1}}$. We then have a chain of subgroups $G = G_0 \geq G_1 \geq \cdots \geq G_{n-1} = \langle z \rangle \geq G_n = \{e\}$ with $[G_i : G_{i+1}] = p$ for each i, as required.

Constructible Numbers, III

Proof (of theorem):

- Suppose the minimal polynomial α over $\mathbb{Q}$ is $m(x)$. Let $m(x)$ have splitting field $K/\mathbb{Q}$ and suppose $\mathrm{Gal}(K/\mathbb{Q}) = G$.
- If α is constructible, we have a tower of quadratic extensions $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_d$ with $[K_{i+1} : K_i] = 2$ and $\alpha \in K_d$.
- If L is any Galois extension of $\mathbb{Q}$ containing K_d, then $KL/\mathbb{Q}$ is also Galois. For any $\sigma \in \mathrm{Gal}(KL/\mathbb{Q})$, we have a tower of quadratic extensions $\mathbb{Q} = \sigma(K_0) \subseteq \sigma(K_1) \subseteq \cdots \subseteq \sigma(K_d)$ with $[\sigma(K_{i+1}) : \sigma(K_i)] = 2$ and $\sigma(\alpha) \in K_d$.
- Thus, all Galois conjugates of α over $\mathbb{Q}$ are constructible. It is then an easy induction to see that if $\alpha_1, \ldots, \alpha_n$ are the roots of $m(x)$, then $[\mathbb{Q}(\alpha_1, \ldots, \alpha_k) : \mathbb{Q}(\alpha_1, \ldots, \alpha_{k-1})]$ is a power of 2 for each k, and hence $|G| = [K : \mathbb{Q}] = [\mathbb{Q}(\alpha_1, \ldots, \alpha_n) : \mathbb{Q}]$ is also a power of 2, as claimed.

Constructible Numbers, IV

Proof (of theorem) (continued) (parentheses):

- For the converse, suppose the Galois group G has $|G| = 2^n$.
- By the lemma with $p = 2$, we have a chain of subgroups $G = G_0 \geq G_1 \geq \cdots \geq G_n = \{e\}$ such that $[G_i : G_{i+1}]$ has order 2 for each i.
- Now apply the fundamental theorem of Galois theory to this chain of subgroups: we obtain a chain of subfields $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = K$ with $[K_{i+1} : K_i] = 2$ for each i. Since $\alpha \in K$, this shows α lies in a tower of quadratic extensions and is therefore constructible, as claimed.

Constructible Numbers, V

As an immediate application we can characterize the constructible regular n-gons:

Corollary (Constructible n-gons)

The regular n-gon is constructible by straightedge and compass if and only if $\varphi(n)$ is a power of 2, if and only if n is a power of 2 times a product of distinct primes of the form $2^{2^k}+1$ for some integer k.

You essentially proved one direction of this result on the midterm.

- The general statement is a quite famous theorem of Gauss, who proved the constructibility of the 17-gon ($k=2$) in 1796, when he was 19.
- He then established the general result above five years later, although he never gave an explicit proof of necessity (which was done 35 years later by Wantzel).

Constructible Numbers, VI

Proof:

- As we showed, the regular n-gon is constructible if and only if $\cos(2\pi/n) = \zeta_n + \zeta_n^{-1}$ is constructible, and since $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = 2$, we see $\cos(2\pi/n)$ is constructible if and only if ζ_n is constructible.
- Then since $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is a Galois extension with Galois group $(\mathbb{Z}/n\mathbb{Z})^\times$ of order $\varphi(n)$, the previous result implies ζ_n is constructible precisely when $\varphi(n)$ is a power of 2.
- For the rest, consider the prime factorization $n = p_1^{a_1} \cdots p_k^{a_k}$: since $\varphi(n) = \varphi(p_1^{a_1}) \cdots \varphi(p_k^{a_k})$ we see $\varphi(p_i^{a_i}) = p_i^{a_i - 1}(p_i - 1)$ must be a power of 2, which requires either $p_i = 2$ or $a_i = 1$ and $p_i - 1$ to be a power of 2.
- If $p = 2^k + 1$, then if k has an odd prime factor d then $2^k + 1$ is divisible by $2^d + 1$ and is therefore not prime. So the only primes of this form are $2^{2^k} + 1$ for some integer k, as claimed.

Constructible Numbers, VII

The primes of the form $p_n = 2^{2^n} + 1$ are called Fermat primes.

- Fermat conjectured that all of these numbers were prime based on the fact that $p_0 = 3$, $p_1 = 5$, $p_2 = 17$, $p_3 = 257$, and $p_4 = 65537$ are prime.
- However, p_5 was shown to be composite by Euler.
- Euler's observation was that any prime divisor of $2^{2^n} + 1$ must be congruent to 1 modulo 2^{n+1}, so this narrows the search for divisors of $p_5 = 2^{32} + 1$ quite considerably.
- The numbers p_6 through p_{32} have subsequently been proven composite, and it is now unknown whether there are any other Fermat primes at all!

Galois Groups of Polynomials, I

If K/F is a Galois extension and we have an explicit description of the action of $\mathrm{Gal}(K/F)$ on the elements of K, we have described in detail how to use the fundamental theorem of Galois theory to compute intermediate fields and minimal polynomials of elements.

- However, all of this discussion presupposes our ability to compute the Galois group and its action on K.
- If K is described only as the splitting field of a polynomial $p(x) \in F[x]$, it is not generally obvious how to determine the Galois group nor even how to compute the degree K/F.
- Our next goal is to describe methods for computing Galois groups of general polynomials (recall that the Galois group of $p(x)$ over F is simply the Galois group of the splitting field).
- This can become quite difficult when the degree is large, so we focus primarily on low-degree polynomials.

Galois Groups of Polynomials, II

As we have previously noted, if $p(x) \in F[x]$ is a separable polynomial of degree n with splitting field K, any $\sigma \in \mathrm{Gal}(K/F)$ is completely determined by its permutation of the roots of p.

- If we fix an ordering of the roots, we get an injective homomorphism from $\mathrm{Gal}(K/F)$ into the symmetric group S_n.
- We may then view the Galois group interchangeably with its image in S_n.
- In general, if we pick a different ordering of the roots, we will obtain a different homomorphism from $\mathrm{Gal}(K/F)$ into S_n.
- However, the resulting subgroups will be the same up to relabeling the elements of the underlying set.
- Per our understanding of conjugacy in S_n as acting via relabeling, this is just saying that the image of G in S_n is determined up to conjugacy inside S_n.

Galois Groups of Polynomials, III

Example: Suppose $p(x) = (x^2 - 2)(x^2 - 3)(x^2 - 6)$ over $\mathbb{Q}$.

- Then the splitting field of p is $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ with Galois group generated by the automorphisms σ and τ with $\sigma(\sqrt{2}, \sqrt{3}) = (-\sqrt{2}, \sqrt{3})$ and $\tau(\sqrt{2}, \sqrt{3}) = (\sqrt{2}, -\sqrt{3})$.
- If we label the six roots $\{\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}, \sqrt{6}, -\sqrt{6}\}$ as $\{1, 2, 3, 4, 5, 6\}$, then σ corresponds to the permutation $(1\,2)(5\,6)$, τ corresponds to the permutation $(3\,4)(5\,6)$, and $\sigma\tau$ corresponds to the permutation $(1\,2)(3\,4)$.
- We can compute the other elements in the Galois group in the same way.
- If we pick a different labeling, then the effect will be to give a conjugate subgroup of this one.

Galois Groups of Polynomials, IV

We also observe that automorphisms must act as permutations on the roots of the irreducible factors of $p(x)$.

- Thus, we may study the action of each element of $\mathrm{Gal}(K/F)$ on the roots of each irreducible factor of $p(x)$ separately.
- If $q(x)$ is an irreducible factor of $p(x)$ of degree m, then as we have shown, the roots of $q(x)$ are all Galois conjugates of one another.
- Thus, the Galois group permutes the roots of $q(x)$ transitively, meaning that for any roots α, β of $q(x)$, there is some $\sigma \in \mathrm{Gal}(K/F)$ with $\sigma(\alpha) = \beta$.
- In particular, if $p(x)$ is itself irreducible, then $\mathrm{Gal}(K/F)$ must be a transitive subgroup of S_n. This information reduces (rather substantially) the number of possibilities for what $\mathrm{Gal}(K/F)$ can be inside S_n.

Galois Groups of Polynomials, V

What we will now do is study these possible transitive subgroups of S_n, and identify properties of polynomials that allow us to determine what their Galois group structure is.

- We will start by analyzing the Galois group of a "generic" polynomial (i.e., whose coefficients are elements of a function field, rather than specific numbers).
- Then we will discuss some related properties of symmetric functions and discriminants of polynomials.
- We will then treat in detail the cases of cubic and quartic polynomials, and then give an overview of some results in moderately larger degrees (5, 6, 7, 8) and how to compute Galois groups over $\mathbb{Q}$ in those cases.
- Finally, we will classify polynomials that are solvable in radicals based on the structure of their Galois groups.

Galois Groups of Polynomials, VI

So, consider a "generic" monic polynomial $p(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0$.

- If its roots are $x_1, x_2, \ldots, x_n$, then we have the obvious factorization $p(t) = (t - x_1)(t - x_2)\cdots(t - x_n)$.
- Expanding out and comparing coefficients shows that
  $a_{n-1} = -(x_1 + x_2 + \cdots + x_n)$,
  $a_{n-2} = x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + \cdots + x_{n-1}x_n$,
  $\vdots$
  and $a_0 = (-1)^n x_1x_2\cdots x_n$.
- These formulas for the coefficients of the polynomial in terms of its roots are often called Vieta's formulas (or if you prefer his actual name in French, Viète's formulas).

Galois Groups of Polynomials, VII

The functions of the x_i appearing in the coefficients are symmetric functions in the roots:

Definition

If $x_1, \ldots, x_n$ are fixed indeterminates, then for $1 \leq k \leq n$, the kth elementary symmetric function s_k in $x_1, \ldots, x_n$ is given by the sum of all products of the x_i taken k at a time. Explicitly, we have

$$\begin{aligned}
s_1 &= x_1 + x_2 + x_3 + \cdots + x_n \\
s_2 &= x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + \cdots + x_{n-1}x_n \\
s_3 &= x_1x_2x_3 + \cdots + x_{n-2}x_{n-1}x_n \\
&\vdots \quad \vdots \quad \vdots \\
s_n &= x_1x_2x_3 \cdots x_n
\end{aligned}$$

Galois Groups of Polynomials, VIII

Thus, if $p(t)$ is monic and has roots $x_1, x_2, \ldots, x_n$, then $p(t) = (t - x_1)(t - x_2)\cdots(t - x_n) = t^n - s_1 t^{n-1} + s_2 t^{n-2} + \cdots + (-1)^n s_n$.

- If F is any field, this means that the field $F(x_1, x_2, \ldots, x_n)$ is a Galois extension of $F(s_1, s_2, \ldots, s_n)$, since it is the splitting field of $p(t) = t^n - s_1 t^{n-1} + s_2 t^{n-2} + \cdots + (-1)^n s_n$.

Our first goal is to determine the Galois group of this extension:

Proposition (Generic Galois Group)

Suppose $x_1, \ldots, x_n$ are independent indeterminates and s_k is the kth elementary symmetric function of the x_i. Then the field $F(x_1, x_2, \ldots, x_n)$ is a Galois extension of $F(s_1, s_2, \ldots, s_n)$ whose degree is $n!$ and whose Galois group is isomorphic to S_n. Explicitly, the isomorphism is provided by the group action of S_n on $F(x_1, x_2, \ldots, x_n)$ via index permutation.

Galois Groups of Polynomials, IX

Proof:

- As noted already, the extension is Galois because it is the splitting field of $p(t) = t^n - s_1 t^{n-1} + s_2 t^{n-2} + \cdots + (-1)^n s_n$.
- Let G be the Galois group.
- As we have discussed previously, S_n acts on $F[x_1, \ldots, x_n]$ via index permutation, with the action given by $\sigma \cdot p(x_1, \ldots, x_n) = p(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$. It is easy to see that this action is also well-defined on rational functions.
- Each of the elementary symmetric functions $s_1, s_2, \ldots, s_n$ is invariant under any permutation of the variable indices, so $F(s_1, s_2, \ldots, s_n)$ is fixed under this action, and therefore is an automorphism of $F(x_1, x_2, \ldots, x_n)/F(s_1, s_2, \ldots, s_n)$.
- This means S_n is (isomorphic to) a subgroup of G, since the only permutation map fixing $F(x_1, x_2, \ldots, x_n)$ is the identity permutation.

Galois Groups of Polynomials, X

Proof (continued):

- In particular, since S_n is isomorphic to a subgroup of G, that means $|G| \geq |S_n| = n!$, and therefore $[F(x_1, x_2, \ldots, x_n) : F(s_1, s_2, \ldots, s_n)] = |G| \geq n!$.
- On the other hand, because $F(x_1, x_2, \ldots, x_n)$ is the splitting field of the degree-n polynomial $p(t)$ over $F(s_1, s_2, \ldots, s_n)$, we see that $[F(x_1, x_2, \ldots, x_n) : F(s_1, s_2, \ldots, s_n)] \leq n!$ by our bounds on the degree of a splitting field.
- Therefore, we must have equality, so $[F(x_1, x_2, \ldots, x_n) : F(s_1, s_2, \ldots, s_n)] = n!$.
- Then $|G| = n! = |S_n|$, and thus we see that the elements of G are precisely the automorphisms induced by index permutations and that $G \cong S_n$.

Galois Groups of Polynomials, XI

As a corollary, we obtain the following classical result about symmetric functions:

Corollary (Symmetric Functions)

If $p(x_1, x_2, \ldots, x_n)$ is a rational function over a field F that is symmetric in the variables $x_1, x_2, \ldots, x_n$, then it is a rational function in the symmetric functions $s_1, s_2, \ldots, s_n$.

- As an example, the function $p(x_1, x_2, x_3) = x_1^3 + x_2^3 + x_3^3$ is symmetric in x_1, x_2, and x_3, and indeed one can verify that $p(x_1, x_2, x_3) = s_1^3 - 3s_1s_2 + 3s_3$.

Galois Groups of Polynomials, XII

Proof:

- Let $L = F(x_1, x_2, \ldots, x_n)$ and $K = F(s_1, s_2, \ldots, s_n)$. If $p(x_1, x_2, \ldots, x_n)$ is a rational function that is symmetric in $x_1, x_2, \ldots, x_n$, then it lies in the fixed field of $G = \mathrm{Gal}(L/K)$.
- But by our characterization of Galois extensions, the fixed field of G is simply the base field: thus, p is an element of K, meaning that it is a rational function in $s_1, s_2, \ldots, s_n$.

Remark: If $p(x_1, x_2, \ldots, x_n)$ is a polynomial that is symmetric in the x_i, then in fact one can show that p is necessarily also a polynomial function of the elementary symmetric functions.

Galois Groups of Polynomials, XIII

Our results above, loosely speaking, say that the Galois group of a "generic" degree-n polynomial is S_n, in the sense that if the s_i are indeterminates, then the Galois group of the polynomial $p(t) = t^n - s_1 t^{n-1} + \cdots + (-1)^n s_n$ is isomorphic to S_n.

- However, by itself, this result does not actually give any information about the Galois group for any specific values of the parameters s_i.
- We would like to be able to "specialize" the choices of the s_i by setting them equal to specific elements of the field F.
- But this is quite a bit more subtle than it may seem.

Galois Groups of Polynomials, XIV

Specifically, choosing values for the s_i may introduce algebraic relations between them that shrink the size of the Galois group.

- Over a finite field, for example, no matter what values we choose for the coefficients, the Galois group will always be cyclic, since every extension of finite fields is Galois with cyclic Galois group.
- Since S_n is not cyclic (or even abelian) for $n \geq 3$, that means for $n \geq 3$ we will always obtain substantial "collapsing" of the Galois group structure from S_n down to a cyclic group, regardless of what selection of coefficients we make.

Galois Groups of Polynomials, XV

In some situations, we can show that such collapsing will not occur.

- Over $\mathbb{Q}$ (or more generally finite extensions of $\mathbb{Q}$), however, a theorem of Hilbert known as Hilbert's irreducibility theorem gives a sufficient condition for specializations not to collapse, in the sense that the Galois group of the specialization will be isomorphic to the Galois group of the original "generic" family.
- In particular, by applying Hilbert's irreducibility theorem to the extension $F(x_1, x_2, \ldots, x_n)/F(s_1, s_2, \ldots, s_n)$, one may deduce that "most" specializations of the s_i at elements of $\mathbb{Q}$ will yield a polynomial with Galois group S_n.
- However, this is more subtle than it may seem, because, depending on the value of n and how one orders polynomials for counting purposes, it may not be the case that 100% of polynomials (probabilistically speaking) actually do have Galois group S_n, even over $\mathbb{Q}$.

Galois Groups of Polynomials, XVI

However, this is more subtle than it may seem: depending on the value of n and how one orders polynomials for counting purposes, it may not be the case that 100% of polynomials (probabilistically speaking) actually do have Galois group S_n, even over $\mathbb{Q}$.

- In fact (up to a little bit of finagling with counting fields versus counting polynomials) if one orders irreducible degree-4 polynomials by the absolute value of their discriminant (which we will discuss next) rather than by the sizes of their coefficients, then in fact a positive proportion of them will have Galois group $D_{2\cdot 4}$ rather than S_4.
- These, and other questions about counting fields and polynomials by discriminant, are a quite active area of research in number theory at the moment[1].

[1] Counting number fields is also the subject of my PhD thesis, in case you were wondering.

Discriminants of Polynomials, I

If F is a field of characteristic not equal to 2, then we may find the roots of a degree-2 polynomial in $F[x]$ via the usual procedure of completing the square.

- Explicitly, if $p(t) = at^2 + bt + c$, then $p(t) = 0$ is equivalent to $a(t + b/(2a))^2 + (c - b^2/(4a)) = 0$, and then rearranging and extracting the square root yields the usual quadratic formula $t = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.
- The nature of the roots is closely tied to the value of the discriminant $D = b^2 - 4ac$: for example, the polynomial has a repeated root (i.e., is inseparable) precisely when $D = 0$, and the roots generate the extension $F(\sqrt{D})$, which has special properties when D is a perfect square.
- In terms of the roots r_1 and r_2 themselves, we can see that when $p(t)$ is monic, $D = (r_1 - r_2)^2$.

Discriminants of Polynomials, II

We can generalize the idea of a discriminant to an arbitrary polynomial:

Definition

If $x_1, x_2, \ldots, x_n$ are arbitrary, we define the discriminant as

$$\Delta(x_1, \ldots, x_n) = \prod_{i=1}^{n} \prod_{j=i+1}^{n} (x_i - x_j)^2 = \prod_{i<j} (x_i - x_j)^2,$$

and we define the discriminant $\Delta(p)$ of the polynomial p with roots $r_1, \ldots, r_n$ (including multiplicities) to be $\Delta(r_1, \ldots, r_n)$.

- When the terms are clear from context, we will often write the discriminant merely as Δ.
- Example: For $p(t) = t^3 + at^2 + bt + c$, we have $\Delta = -27c^2 + 18abc - 4b^3 - 4a^3c + a^2b^2$.

Discriminants of Polynomials, III

Note that $\Delta(x_1, \ldots, x_n) = \prod_{i=1}^{n} \prod_{j=i+1}^{n} (x_i - x_j)^2 = \prod_{i<j} (x_i - x_j)^2$ is a symmetric polynomial in the x_i, and is thus an element of $F[s_1, \ldots, s_n]$.

- In particular, this means that $\Delta(p)$ is a polynomial function in the coefficients of p. However, since the total degree of Δ in the x_i is $n(n-1)$, for large n the resulting expressions will be quite complicated.
- For $n = 4$, for example, the discriminant of $p(t) = t^4 + at^4 + bt^2 + ct + d$ is $\Delta = -27a^4d^2 + 18a^3bcd - 4a^3c^3 - 4a^2b^3d + a^2b^2c^2 + 144a^2bd^2 - 6a^2c^2d - 80ab^2cd + 18abc^3 - 192acd^2 + 16b^4d - 4b^3c^2 - 128b^2d^2 + 144bc^2d - 27c^4 + 256d^3$.

Discriminants of Polynomials, IV

We have already encountered the discriminant in our analysis of the alternating group A_n.

- Specifically, we showed that the square root of the discriminant $\sqrt{\Delta} = \prod_{i<j}(x_i - x_j)$ has the property that $\sigma(\sqrt{\Delta}) = \sqrt{\Delta}$ for $\sigma \in A_n$, and $\sigma(\sqrt{\Delta}) = -\sqrt{\Delta}$ for $\sigma \notin A_n$.
- If the characteristic of F is not equal to 2, this means $\sqrt{\Delta}$ is not fixed by all of S_n, but its square is: thus, $\sqrt{\Delta}$ generates a degree-2 extension of $F(s_1, s_2, \ldots, s_n)$.
- Since $[S_n : A_n] = 2$, by the fundamental theorem of Galois theory, we conclude that $\sqrt{\Delta}$ generates the fixed field of A_n.

Discriminants of Polynomials, V

By applying this to specific polynomials, we obtain the following very useful fact:

Proposition (A_n and Discriminants)

If F is a field of characteristic not 2, and $p(x) \in F[x]$ is any separable polynomial, then the Galois group of $p(x)$ is a subgroup of A_n if and only if $\sqrt{\Delta(p)} \in F$.

Discriminants of Polynomials, VI

Proof:

- As we noted already, $\Delta = \Delta(p)$ is symmetric in the roots of p, hence is fixed by every element of the Galois group G of p.
- If we fix an ordering of the roots $r_1, \ldots, r_n$ of p, then $\sqrt{\Delta(p)} = \prod_{i<j}(r_i - r_j)$ is an element of the splitting field K.
- Then if σ is any element of the Galois group, we see that $\sigma(\sqrt{\Delta}) = \epsilon(\sigma) \cdot \sqrt{\Delta}$, where $\epsilon(\sigma)$ is the sign of the permutation that σ induces on the roots.
- Since the characteristic of F is not 2 (so that $\sqrt{\Delta} \neq -\sqrt{\Delta}$) we see that σ fixes $\sqrt{\Delta}$ if and only if $\sigma \in A_n$.
- Thus, the Galois group is a subgroup of A_n if and only if every element of the Galois group fixes $\sqrt{\Delta}$, which is in turn equivalent to saying that $\sqrt{\Delta} \in F$.

Cubic Polynomials, I

We now study degree-3 polynomials using the tools we have developed so far.

- If $f(t) \in F[t]$ is a reducible degree-3 polynomial, everything reduces to the case of lower degree.
- If $f(t)$ factors either as a product of 3 degree-1 terms, then the splitting field of f is F and the Galois group is trivial.
- If $f(t)$ factors as a product of a degree-1 term and an irreducible degree-2 term, then the splitting field of p is a quadratic extension of F (obtained by solving the quadratic equation) and the Galois group is $\mathbb{Z}/2\mathbb{Z}$.

Cubic Polynomials, II

The interesting case is for an irreducible polynomial, so suppose $f(t) = t^3 - a_1 t^2 + a_2 t - a_3$ is an irreducible cubic polynomial in $F[t]$ with splitting field K.

- If f has roots $\beta_1, \beta_2, \beta_3$, then since $a_1 = s_1$ is the sum of the roots, we have $\beta_3 = a_1 - \beta_1 - \beta_2$. Thus, $K = F(\beta_1, \beta_2, \beta_3) = F(\beta_1, \beta_2)$.
- We get a tower $F \subset F(\beta_1) \subseteq F(\beta_1, \beta_2) = K$, where $[F(\beta_1) : F] = 3$ and $[K : F(\beta_1)] \leq 2$.
- Since p is irreducible, the Galois group of f is a transitive subgroup of S_3.
- It is easy to see that there are only two such subgroups, namely S_3 and A_3, and we can tell these cases apart by looking at the discriminant as long as the characteristic of F is not 2.

Cubic Polynomials, III

So we have two possible cases:

1. When the Galois group is A_3, this means that if α is any root of f in K, then $K = F(\alpha)$. (In particular, the other roots of f will be polynomials in α.) Furthermore, there are no proper nontrivial intermediate fields of K/F since A_3 has no nontrivial proper subgroups.
2. When the Galois group is S_3, there are nontrivial proper subgroups, which (by the Galois correspondence) correspond to intermediate fields: specifically, there is the quadratic subfield of K fixed by A_3 (which by our discussion is generated by the square root of the discriminant), and also the three cubic subfields of K each fixed by a transposition (each of which will be generated by one of the three roots of f).

Cubic Polynomials, IV

We summarize these observations in the following proposition:

Proposition (Galois Groups of Cubics)

If F is a field of characteristic not equal to 2 and $f(t) = t^3 - a_1 t^2 + a_2 t - a_3$ is an irreducible cubic polynomial in $F[t]$, then the Galois group of f is either A_3 or S_3, and it is A_3 precisely when the discriminant $\Delta(p) = -27a_3^2 + 18a_1a_2a_3 - 4a_2^3 - 4a_1^3a_3 + a_1^2a_2^2$ is a square in F.

Cubic Polynomials, IV

Proof:

- If f is irreducible then the Galois group is a transitive subgroup of S_3, hence is either S_3 or A_3. By our results on discriminants, it is A_3 precisely when the discriminant is a square in F.
- The only thing left is to compute the formula for the discriminant.
- If the characteristic of F is not 3, we may make a change of variables $y = t - a_1/3$ and then analyze the polynomial $g(y) = y^3 + py + q$ where $p = a_2 - a_1^3/3$ and $q = (-2/27)a_1^3 + a_1 a_2/3 - a_3$ are F-rational polynomials in the original coefficients.
- Since the roots of g are translates of the roots of f, the discriminants of f and g are the same (since the discriminant only involves the pairwise differences of the roots).

Cubic Polynomials, V

Proof (continued):

- Since $\Delta(g)$ is a symmetric polynomial of homogeneous degree 6 (i.e., every term has degree 6) in its roots r_1, r_2, r_3, it is a polynomial in s_1, s_2, s_3, and since $s_1 = 0$ we may ignore it.
- Since s_2 is homogeneous of degree 2 and s_3 is homogeneous of degree 3, we must have $\Delta(g) = c_1 \cdot s_2^3 + c_2 \cdot s_3^2$ since these are the only homogeneous polynomials in s_1, s_2, s_3 of degree 6.
- We may compute c_1 and c_2 by picking values for r_1, r_2, r_3 and then comparing the value of $\Delta(s)$ to $c_1 \cdot s_2^3 + c_2 \cdot s_3^2$. Choosing, for example, $(r_1, r_2, r_3) = (-1, 0, 1)$ and $(-2, 1, 1)$ leads to the equations $4 = c_1(-1)^3 + c_2(0)$ and $0 = c_1(-3)^3 + c_2(-2)^2$, whence $c_1 = -4$ and $c_2 = -27$.
- Hence $\Delta(f) = \Delta(g) = -4p^3 - 27q^2$, and then plugging back in for a_1, a_2, a_3 and simplifying eventually yields the given formula (which in fact is also correct in characteristic 3).

Cubic Polynomials, VI

There are two useful techniques employed in the proof just given.

- The first idea was to make a change of variables to simplify the form of the cubic equation.
- Making a sufficiently artful change of variables of this nature can allow us to reduce (sometimes, greatly) the amount of computation required in examples.
- The other idea was the technique for determining a formula for a symmetric polynomial in terms of the elementary symmetric functions by writing down the general form (based on degree) and then plugging in specific values to find the coefficients.

Cubic Polynomials, VII

Example: Find the Galois group of $f(t) = t^3 - 3t + 1$ over $\mathbb{Q}$ and identify all subfields of its splitting field.

- This cubic is irreducible over $\mathbb{Q}$ since it has no roots by the rational root test.
- Using the formula from the (proof of) the proposition, we see that $\Delta(f) = 4 \cdot 3^3 - 27 = 81$. Since this is a perfect square in $\mathbb{Q}$, the Galois group is A_3.
- Since the splitting field has degree 3, its only subfields are itself and $\mathbb{Q}$.
- After some effort, one may show that if α is a root of f then so is $\alpha^2 - 2$. Hence, if α is one root of f, then the others are $\alpha^2 - 2$ and $(\alpha^2 - 2)^2 - 2 = -\alpha^2 - \alpha - 2$.

Cubic Polynomials, VIII

Example: Find the Galois group of $f(t) = t^3 + t + 1$ over $\mathbb{Q}$ and identify all subfields of its splitting field.

- This cubic is is irreducible over $\mathbb{Q}$ since it has no roots by the rational root test.
- Using the formula from the (proof of) the proposition, we see that $\Delta(f) = -4 \cdot 1^3 - 27 = -31$.
- Since this is not a perfect square in $\mathbb{Q}$, the Galois group is S_3.
- Another way of seeing that the Galois group must be S_3 is that by calculus, the polynomial has one real root and two (necessarily) complex-conjugate roots.
- Therefore, complex conjugation is an element of the Galois group that transposes two of the roots (hence has order 2), so the Galois group must be S_3.

Cubic Polynomials, IX

Example: Find the Galois group of $f(t) = t^3 + t + 1$ over $\mathbb{Q}$ and identify all subfields of its splitting field.

- In comparison to the A_3 example, computing the subfields here takes a bit more work (but not too much, since S_3 does not have many subgroups).
- By the fundamental theorem of Galois theory, there is a unique quadratic subfield of the splitting field, namely $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{-31})$: this is the fixed field of the order-3 subgroup of S_3.
- There are also three conjugate degree-3 subfields, namely, $\mathbb{Q}(\beta_1)$, $\mathbb{Q}(\beta_2)$, and $\mathbb{Q}(\beta_3)$ where $\beta_1, \beta_2, \beta_3$ are the three roots of f. These are the fixed fields of the three order-2 subgroups of S_3.

Cubic Polynomials, X

Although we have computed the Galois group of an arbitrary cubic, the results do not actually give us an explicit description of the fields of interest, since we do not have formulas for the roots.

- The problem of finding a general formula for the roots of a cubic equation was considered by the ancient Egyptians and Greeks.
- Indeed, one aspect of their work was the attempt to construct cube roots using straightedge and compass (the fruitlessness of which we have previously discussed!).
- The search for a "cubic formula" was taken up by many mathematicians in antiquity, but no general solution was found until the 1500s.

Cubic Polynomials, XI

Ultimately, the story of how the cubic formula was eventually publicized is rather convoluted. Since it is quite a fascinating story, I will briefly summarize it.

- Minimal progress was made on solving the cubic until the early 1500s, when del Ferro discovered a method for solving cubics of the form $t^3 + pt = q$.
- However, due to the nature of Renaissance patronage, del Ferro did not publicize his method, but only taught it to his student Fior.

Cubic Polynomials, XII

Pictured: Tartaglia (courtesy Wikipedia)

In 1535, Fior in turn challenged another scholar, Niccolo Fontana (nicknamed Tartaglia due to a physical deformity), who eventually (re)discovered the solution to the cubic. Again, as was normal at the time, Tartaglia kept it a secret.

Cubic Polynomials, XIII

Pictured: Cardano (courtesy Wikipedia)

Eventually, Gerolamo Cardano (an avid astrologer and gambler who at one time was one of the most well-regarded physicians in Europe, who was eventually jailed for heresy and then pardoned by the Pope) was able, after repeated entreaties and vows never to reveal Tartaglia's method, to coax Tartaglia into revealing it.

Cubic Polynomials, XIV

Pictured: A Ferrari (courtesy USA Today)

Cardano was then able to extend Tartaglia's method to solve the general cubic equation, and eventually took a student, Ludovico Ferrari, who was able to extend Cardano's techniques to solve degree-4 equations. Cardano and Ferrari eventually discovered that del Ferro had solved the cubic prior to Tartaglia's discovery of the solution, and published his generalization in 1545 in his famous *Ars Magna*, giving credit to del Ferro, Fior, and Tartaglia.

Cubic Polynomials, XV

However, as seems to happen with many major mathematical and scientific discoveries, this did not sit well with all parties.

- Despite receiving proper attribution, Tartaglia nonetheless felt betrayed by Cardano, despite the fact that del Ferro had developed the technique prior to Tartaglia.
- Cardano attempted to stay out of the dispute. However, Ferrari charged that Tartaglia had built his reputation on the stolen work of others, and then challenged him to a public debate on mathematics.
- Eventually Tartaglia took a teaching position in Cardano's hometown, and (apparently) a debate eventually took place. It, unsurprisingly, quickly devolved into a shouting match.

Cubic Polynomials, XVI

Anyway.... to finish off the day, we will present a solution of the cubic similar to Cardano's (and presumably, also to Tartaglia's).

Theorem (del Ferro / Fior / Tartaglia / Cardano Formulas)

If the characteristic of F is not 2 or 3, and the polynomial $g(t) = t^3 + pt + q$ is irreducible and separable over F, then for $A = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$ *and* $B = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$ *with cube roots chosen so that $AB = -p/3$, the three roots of g are*

$$A + B,\ \zeta_3 A + \zeta_3^2 B,\ \text{and}\ \zeta_3^2 A + \zeta_3 B,$$

where $\zeta_3 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ is a primitive 3rd root of unity over F.

Cubic Polynomials, XVII

Proof:

- From the algebraic identity $(x+y)^3 - 3xy(x+y) = x^3 + y^3$, we can see that if we take $x+y=t$, $3xy=-p$, and $x^3+y^3=-q$, then the identity becomes $t^3+pt+q=0$.
- The equation $3xy=-p$ implies $y=-p/(3x)$.
- Then $x^3+y^3=-q$ becomes $x^3 - p^3/(27x^3) = -q$, whence $x^6 + qx^3 - \frac{p^3}{27} = 0$. (Note that we need the characteristic not to be 3, in order to divide by 27.)
- This is a quadratic in x^3, so solving yields $x^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$, $y^3 = -q - x^3 = -\frac{q}{2} \mp \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$. (Note that we are using the fact the characteristic is not 2 to invoke the quadratic formula here.)

Cubic Polynomials, XVIII

Proof (continued):

- Since we may interchange x and y, let us assume $x^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$ and $y^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$.
- Then there are three possible values for x, namely $x = \zeta_3^k \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$, and since we must also have $3xy = p$, any choice of x yields a unique value for y, namely $y = \zeta_3^{2k} \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$.
- Thus, we obtain the claimed solutions $t = \zeta_3^k \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \zeta_3^{2k} \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$ for $k \in \{0, 1, 2\}$.

Cubic Polynomials, XIX

Example: Find the roots of the cubic $f(t) = t^3 + t + 1$ over $\mathbb{Q}$.

- By Cardano's formulas, we compute
  $A = \sqrt[3]{-\frac{1}{2} + \sqrt{\frac{31}{108}}}$ and $B = \sqrt[3]{-\frac{1}{2} + \sqrt{\frac{31}{108}}}$.
- Thus, the three roots of f are
  $A + B$, $\zeta_3 A + \zeta_3^2 B$, and $\zeta_3^2 A + \zeta_3 B$.

Cubic Polynomials, XIX

Example: Find the roots of the cubic $f(t) = t^3 + t + 1$ over $\mathbb{Q}$.

- By Cardano's formulas, we compute
  $$A = \sqrt[3]{-\frac{1}{2} + \sqrt{\frac{31}{108}}} \text{ and } B = \sqrt[3]{-\frac{1}{2} + \sqrt{\frac{31}{108}}}.$$
- Thus, the three roots of f are
  $A + B$, $\zeta_3 A + \zeta_3^2 B$, and $\zeta_3^2 A + \zeta_3 B$.
- What, were you expecting something else? This cubic is irreducible, so its roots aren't going to magically look any nicer than that!

Cubic Polynomials, XX

Example: Find the roots of the cubic $f(t) = t^3 - 3t + 1$ over $\mathbb{Q}$.

- By Cardano's formulas, we compute
  $A = \sqrt[3]{-\frac{1}{2} + \sqrt{-\frac{3}{4}}}$ and $B = \sqrt[3]{-\frac{1}{2} - \sqrt{-\frac{3}{4}}}$.
- So the roots of f are $A + B$, $\zeta_3 A + \zeta_3^2 B$, and $\zeta_3^2 A + \zeta_3 B$.

Cubic Polynomials, XX

Example: Find the roots of the cubic $f(t) = t^3 - 3t + 1$ over $\mathbb{Q}$.

- By Cardano's formulas, we compute
$$A = \sqrt[3]{-\frac{1}{2} + \sqrt{-\frac{3}{4}}} \text{ and } B = \sqrt[3]{-\frac{1}{2} - \sqrt{-\frac{3}{4}}}.$$
- So the roots of f are $A + B$, $\zeta_3 A + \zeta_3^2 B$, and $\zeta_3^2 A + \zeta_3 B$.
- For this polynomial we can compute more explicit descriptions of the roots, since the term under the cube root for A is $-\frac{1}{2} + \frac{\sqrt{-3}}{2} = \zeta_3$ and the term under the cube root for B is ζ_3^2.
- Then we have $A = \sqrt[3]{\zeta_3} = \zeta_9$ while $B = \zeta_9^8$ (note that we must choose the cube roots so that $AB = 1$).
- Hence the roots are in fact $A + B = \zeta_9 + \zeta_9^8 = 2\cos(2\pi/9)$, $\zeta_3 A + \zeta_3^2 B = \zeta_9^4 + \zeta_9^5 = 2\cos(8\pi/9)$, and $\zeta_3^2 A + \zeta_3 B = \zeta_9^7 + \zeta_9^2 = 2\cos(4\pi/9)$.

Cubic Polynomials, XXI

In the second example, notice that the expressions for the roots from Cardano's formulas involved complex numbers, even though all of the roots are real. In fact, this will always be the case when the polynomial has three real roots.

- If all three roots are real, then $\sqrt{\Delta}$ is also clearly real (it is a polynomial in the roots), so Δ is a nonnegative real number.
- But in Cardano's formulas, we have $A, B = \sqrt[3]{-\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} = \sqrt[3]{-\frac{q}{2} + \sqrt{-\Delta}}$: note the $\sqrt{-\Delta}$.
- On the other hand, if the polynomial has two complex-conjugate roots, then in fact Δ will always be negative: to see this, suppose the roots are $x + iy$, $x - iy$, w with x, y, w real. Then $\sqrt{\Delta} = (2iy)(x + iy - w)(x - iy - w) = (2iy)[(x - w)^2 + y^2]$ is purely imaginary, and so Δ is negative.

Cubic Polynomials, XXII

As a coda to the tortuous history of the cubic, we will remark that it is this perplexing appearance of square roots of negative numbers in the formulas for real solutions to cubic equations that led to the initial development of complex numbers in mathematics.

- To illustrate, for the cubic $p(t) = t^3 - 15t - 4$, Cardano's formulas give $A = \sqrt[3]{2 + \sqrt{-121}}$ and $B = \sqrt[3]{-2 + \sqrt{-121}}$, even though one may verify that the three roots of this cubic are the real numbers 4 and $-2 \pm \sqrt{3}$.
- To resolve this difficulty, Bombelli in 1572 observed that one may formally compute $(2 \pm \sqrt{-1})^3 = \pm 2 + \sqrt{-121}$, and so one may take $A = 2 + \sqrt{-1}$ and $B = 2 - \sqrt{-1}$ to obtain the correct root $A + B = 4$.
- One cannot give general formulas involving only real radicals for the solutions of irreducible cubics with $\Delta < 0$, so this issue can only be resolved by working with non-real numbers.

Summary

We discussed more about cyclotomic and abelian extensions.

We classified the constructible regular polygons.

We introduced Galois groups of polynomials, and discussed symmetric functions and discriminants of polynomials.

We discussed the history and solution of the cubic equation, and some related facts.

Next lecture: Quartic polynomials, computing Galois groups over $\mathbb{Q}$.