Math 5111 (Algebra 1)

Lecture #23 of 24 $\sim$ December 3rd, 2020

Computing Galois Groups of Polynomials

- Quartic Polynomials
- Computing Galois Groups Over $\mathbb{Q}$

This material represents §4.4.4-4.4.5 from the course notes.

Quartic Polynomials, I

Last time, we analyzed the possible Galois groups of cubic polynomials and gave formulas for their roots.

- We may use similar techniques to analyze degree-4 polynomials, although because S_4 has many more subgroups than S_3, there are numerous possible Galois groups.
- As before, if the polynomial is reducible then we may reduce to lower-degree cases, so assume that the polynomial $f(t) = t^4 - a_1 t^3 + a_2 t^2 - a_3 t + a_4$ is an irreducible quartic polynomial in $F[t]$ with splitting field K.
- By making a substitution $y = t - a_1/4$, as with the cubic, we may equivalently analyze the polynomial $g(y) = y^4 + py^2 + qy + r$, which will have the same Galois group and discriminant as f.

Quartic Polynomials, II

A brief search will reveal that there are five possible isomorphism classes for the Galois group of $g(y) = y^4 + py^2 + qy + r$ as transitive subgroups of S_4:

1. S_4.
2. A_4.
3. $D_{2\cdot 4}$.
4. C_4.
5. V_4.

- Note C_4 is cyclic of order 4 while V_4 is the Klein 4-group.
- As explicit permutation groups, one can write $D_{2\cdot 4} = \langle (1\,2\,3\,4), (1\,3) \rangle$, $C_4 = \langle (1\,2\,3\,4) \rangle$, and $V_4 = \langle (1\,2)(3\,4), (1\,3)(2\,4) \rangle$, up to conjugacy.

By using the discriminant we can distinguish some possibilities.

- If the discriminant is a square, the Galois group is a subgroup of A_4, and there are two such subgroups: A_4 and V_4.
- If the discriminant is not a square, then the Galois group is one of the others: S_4, $D_{2\cdot 4}$, and C_4.

Quartic Polynomials, III

Here, unlike in the cubic case, the discriminant does not give enough information to determine the Galois group.

- To differentiate further between these possibilities, we may study other functions of the roots that are not fixed by all the elements in S_4.
- As first described by Lagrange, one method is to consider the elements $\theta_1 = (\beta_1 + \beta_2)(\beta_3 + \beta_4)$, $\theta_2 = (\beta_1 + \beta_3)(\beta_2 + \beta_4)$, and $\theta_3 = (\beta_1 + \beta_4)(\beta_2 + \beta_3)$.
- These elements are permuted by S_4, and the stabilizer of each individual element is a dihedral subgroup of S_4: for example, θ_2 is stabilized by the dihedral subgroup $\langle (1\,2\,3\,4), (1\,3) \rangle$ we wrote earlier, while the others are stabilized by appropriate conjugate subgroups. The stabilizer of all three elements is the Klein-four group V_4.

Quartic Polynomials, IV

We have $\theta_1 = (\beta_1 + \beta_2)(\beta_3 + \beta_4)$, $\theta_2 = (\beta_1 + \beta_3)(\beta_2 + \beta_4)$, and $\theta_3 = (\beta_1 + \beta_4)(\beta_2 + \beta_3)$.

- Since θ_1, θ_2, θ_3 are permuted by S_4, their elementary symmetric functions are fixed by S_4, and so the cubic polynomial whose roots are $\theta_1, \theta_2, \theta_3$ is fixed by the entire Galois group, so its coefficients lie in F.
- We may then compute $\theta_1 + \theta_2 + \theta_3 = 2s_2$, $\theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_3 = s_1 s_3 + s_2^2 - 4s_4$, and $\theta_1\theta_2\theta_3 = s_1^2 s_2 s_3 - s_1^2 s_4 - s_3^2$.
- Since $s_1 = 0$, this means that $\theta_1, \theta_2, \theta_3$ are the three roots of the polynomial $h(z) = z^3 - 2pz^2 + (p^2 - 4r)z + q^2$.

Quartic Polynomials, V

The cubic $h(z) = z^3 - 2pz^2 + (p^2 - 4r)z + q^2$, is called the resolvent cubic of $g(y)$.

- As we just noted, the roots of $h(z)$ are $\theta_1 = (\beta_1 + \beta_2)(\beta_3 + \beta_4)$, $\theta_2 = (\beta_1 + \beta_3)(\beta_2 + \beta_4)$, and $\theta_3 = (\beta_1 + \beta_4)(\beta_2 + \beta_3)$.
- Very conveniently, the discriminant of this cubic is the same as the discriminant of the quartic, since $(\theta_1 - \theta_2)^2 = (\beta_1 - \beta_4)^2(\beta_2 - \beta_3)^2$ and likewise for the other two squared differences. (In particular, we see that the elements θ_i are distinct as long as the β_i are.)
- If we can find the factorization of the resolvent cubic over F, then this will yield information about whether the elements θ_i are in F, which in turn gives information about the possible elements in the Galois group.

Quartic Polynomials, VI

Theorem (Galois Groups of Quartics)

Suppose F has characteristic not 2 or 3, and let $f(y) = y^4 + py^2 + qy + r$ be an irreducible separable quartic over F with associated resolvent cubic $g(z) = z^3 - 2pz^2 + (p^2 - 4r)z + q^2$ and discriminant $\Delta = \Delta(f) = \Delta(g)$. Then the Galois group of f is one of S_4, A_4, $D_{2\cdot 4}$, C_4, and V_4:

1. *The Galois group is V_4 if and only if Δ is a square in F and the resolvent cubic splits completely over F.*
2. *The Galois group is A_4 if and only if Δ is a square in F and the resolvent cubic has no roots in F.*
3. *The Galois group is S_4 if and only if Δ is not a square in F and the resolvent cubic has no roots in F.*
4. *The Galois group is C_4 if and only if Δ is not a square in F, the resolvent cubic has exactly one root r' in F, and the polynomials $x^2 + r'$ and $x^2 + (r' - p)x + r$ both split over $F(\sqrt{\Delta})$.*
5. *The Galois group is $D_{2\cdot 4}$ if and only if Δ is not a square in F, the resolvent cubic has exactly one root in F, and at least one of the polynomials $x^2 + r'$ and $x^2 + (r' - p)x + r$ is irreducible in $F(\sqrt{\Delta})$.*

Quartic Polynomials, VII

Some remarks:

- The condition differentiating C_4 and $D_{2\cdot 4}$ is a result due to Kappe and Warren from 1989. There is a more classical condition (specifically, whether the quartic $f(y)$ splits over $F(\sqrt{\Delta})$) that is harder to check that can also tell these groups apart.
- Implicit in our characterization is the fact that no other scenarios (e.g., Δ being a square and the resolvent cubic having exactly one root in F) can occur.
- The most efficient way to compute the discriminant Δ is to use the formula for the discriminant of the cubic $g(z)$.

Quartic Polynomials, VIII

Proof:

- As we have shown above, if $\beta_1, \beta_2, \beta_3, \beta_4$ are the roots of $f(y)$, then the roots of the resolvent cubic $g(z)$ are $\theta_1 = (\beta_1 + \beta_2)(\beta_3 + \beta_4)$, $\theta_2 = (\beta_1 + \beta_3)(\beta_2 + \beta_4)$, and $\theta_3 = (\beta_1 + \beta_4)(\beta_2 + \beta_3)$, and that $\Delta(p) = \Delta(g)$.
- As we have also noted, up to conjugacy the only transitive subgroups of S_4 are S_4, A_4, $D_{2\cdot 4}$, C_4, and V_4, so the Galois group G must be one of these.
- We will analyze the two cases where Δ is a square first (these are the cases of A_4 and V_4), and then treat the remaining three cases where Δ is not a square (these are the cases of S_4, $D_{2\cdot 4}$ and C_4).

Quartic Polynomials, IX

Proof (Δ square):

- First suppose that Δ is a square: then the Galois group is one of A_4 and V_4.
- If the resolvent cubic has all its roots in F, then all three of the θ_i are in F, meaning that they are fixed by G. Since the only elements of S_4 fixing each of $\theta_1, \theta_2, \theta_3$ are the elements of the Klein 4-group V_4, this means $G \subseteq V_4$, hence $G = V_4$.
- If the resolvent cubic does not have all its roots in F, then the only possibility is to have $G = A_4$. In this case, none of the θ_i is fixed by all of G (since the stabilizer of any given θ_i is a dihedral group of order 8), and so none of them lies in F.

Quartic Polynomials, X

Proof (Δ nonsquare):

- Now suppose Δ is not a square: then the Galois group is one of S_4, $D_{2\cdot 4}$, and C_4.
- If the resolvent cubic has no roots in F and $\Delta(g)$ is not a square, the Galois group of the resolvent cubic is S_3: thus, the degree $[K : F]$ is divisible by 6, meaning that $|G|$ is divisible by 6. The only possibility here is that $G = S_4$.
- It is not possible for the resolvent cubic to split completely over F, since then the Galois group would stabilize each of the θ_i hence be contained in V_4.

Quartic Polynomials, XI

Proof (Δ nonsquare, more):

- Thus, the only remaining case is that the resolvent cubic factors over F as the product of a degree-1 and an irreducible degree-2 polynomial (i.e., it has exactly one root in F), and in this case the Galois group is either $D_{2\cdot 4}$ or C_4.
- To distinguish between $D_{2\cdot 4}$ and C_4, note $F(\sqrt{\Delta})$ is the fixed field of $G \cap A_4$ by the fundamental theorem of Galois theory.
- Now let r' be the root of g in F and assume that G contains the 4-cycle $(1\,2\,3\,4)$, so that it is either $C_4 = \langle (1\,2\,3\,4) \rangle$ or $D_{2\cdot 4} = \langle (1\,3), (1\,2\,3\,4) \rangle$: then $r' = (\beta_1 + \beta_3)(\beta_2 + \beta_4)$ since this is the only θ_i fixed by $(1\,2\,3\,4)$.

Quartic Polynomials, XII

Proof (Δ nonsquare, more more):

- If the Galois group is C_4 then the unique quadratic subfield of K/F is $F(\sqrt{\Delta})$, and is also the fixed field of the subgroup $\langle(1\,3)(2\,4)\rangle$. Then the roots of the two polynomials $(x-(\beta_1+\beta_3))(x-(\beta_2+\beta_4)) = x^2+r'$ and $(x-\beta_1\beta_3)(x-\beta_2\beta_4) = x^2+(r'-p)+r$ are both fixed by this subgroup, and hence lie in $F(\sqrt{\Delta})$. In other words, these polynomials both split over $F(\sqrt{\Delta})$.
- If the Galois group is $D_{2\cdot 4}$ then $F(\beta_1) = F(\beta_3)$ is the fixed field of $\langle(2\,4)\rangle$ and $F(\sqrt{\Delta})$ is the fixed field of $\langle(1\,2)(3\,4),\,(1\,3)(2\,4)\rangle$, since the given elements are fixed by the indicated subgroups (the latter because it lies inside A_4) and the fields have the correct degrees.

Quartic Polynomials, XIII

Proof (Δ nonsquare, more more more):

- Now consider the two polynomials $(x-(\beta_1+\beta_3))(x-(\beta_2+\beta_4))$ and $(x-\beta_1\beta_3)(x-\beta_2\beta_4)$: we claim that at least one is irreducible over $F(\sqrt{\Delta})$.
- Otherwise, both $\beta_1+\beta_3$ and $\beta_1\beta_3$ would be elements of $F(\sqrt{\Delta})$, and then $F(\sqrt{\Delta})$ would be a subfield of $F(\beta_1)=F(\beta_3)$. But this cannot occur because the fixing subgroup of $F(\sqrt{\Delta})$, namely $\langle(1\,2)(3\,4),(1\,3)(2\,4)\rangle$, does not contain the fixing subgroup of $F(\beta_1)=F(\beta_3)$, namely $\langle(2\,4)\rangle$.
- Thus, if the Galois group is $D_{2\cdot4}$, at least one of the polynomials x^2+r' and $x^2+(r'-p)+r$ is irreducible in $F(\sqrt{\Delta})$.
- The converse conditions are immediate since all our cases are disjoint. We have analyzed all of the cases, we are done.

Quartic Polynomials, XIV

So, to summarize, here is the algorithm for finding the Galois group of a quartic polynomial $p(t)$:

0. Check p is irreducible. Substitute $y = t - a_1/4$ to convert $p(t) = t^4 - a_1 t^3 + a_2 t^2 - a_3 t + a_4$ into $f(y) = y^4 + py^2 + qy + r$.
1. Find the resolvent cubic $g(z) = z^3 - 2pz^2 + (p^2 - 4r)z + q^2$.
2. Factor g and compute discriminant $\Delta = \Delta(f) = \Delta(g)$.
3. If Δ is a square and g splits completely, group is V_4. If Δ is a square otherwise, group is A_4. If g is irreducible, group is S_4.
4. If g has a single root r', consider $x^2 + r'$ and $x^2 + (r' - p)x + r$. If both split over $F(\sqrt{\Delta})$, group is C_4. Otherwise, group is $D_{2\cdot 4}$.

Quartic Polynomials, XV

Example: Find the Galois groups of each of the following quartic polynomials:

1. $f(y) = y^4 - 2$ over $\mathbb{Q}$. $[\Delta = -2048.]$
2. $f(y) = y^4 + 8y + 12$ over $\mathbb{Q}$. $[\Delta = 2^{12} \cdot 3^4.]$
3. $f(y) = y^4 + 2y - 2$ over $\mathbb{Q}$. $[\Delta = -2^4 \cdot 5 \cdot 31.]$
4. $f(y) = y^4 - 14y^2 + 9$ over $\mathbb{Q}$. $[\Delta = 2^{14} \cdot 3^2 \cdot 5^2.]$
5. $f(y) = y^4 + 5y + 5$ over $\mathbb{Q}$. $[\Delta = 5^3 \cdot 11^2.]$

- And also for your convenience: the resolvent cubic of $f(y) = y^4 + py^2 + qy + r$ is $g(z) = z^3 - 2pz^2 + (p^2 - 4r)z + q^2$.
- If g has a single root r', consider $x^2 + r'$ and $x^2 + (r' - p)x + r$ over $F(\sqrt{\Delta})$.

Quartic Polynomials, XVI

Example: Find the Galois groups of each of the following quartic polynomials:

1. $f(y) = y^4 - 2$ over $\mathbb{Q}$. $[\Delta = -2048.]$

- This polynomial is irreducible by Eisenstein.
- Resolvent cubic is $g(z) = z^3 + 8z$ with $\Delta = -4 \cdot 8^3 = -2048$.
- Since the discriminant is not a square and the resolvent cubic factors as $g(z) = z(z^2 + 8)$ we see that the Galois group is either C_4 or $D_{2\cdot 4}$.
- To determine which of these it is, we see that the root of $g(z)$ is $r' = 0$, so we must test the reducibility of $x^2 + r' = x^2$ and $x^2 + (r' - p)x + r = x^2 - 2$ over $\mathbb{Q}(\sqrt{-2048}) = \mathbb{Q}(\sqrt{-2})$.
- Although the first polynomial is reducible, the second is irreducible over $\mathbb{Q}(\sqrt{-2})$. Hence the Galois group is $\boxed{D_{2\cdot 4}}$ (as we have shown previously by computing the action explicitly on the splitting field).

Quartic Polynomials, XVII

Example: Find the Galois groups of each of the following quartic polynomials:

2. $f(y) = y^4 + 8y + 12$ over $\mathbb{Q}$. $[\Delta = 2^{12} \cdot 3^4.]$

- One may verify by direct calculation that f is irreducible (it has no roots by the rational root test, and also does not factor as the product of two integral quadratics).
- Resolvent cubic is $g(z) = z^3 - 48z + 64$, with $\Delta = -4(-48)^3 - 27(64)^2 = 2^{14} \cdot 3^3 - 3^3 \cdot 2^{12} = 2^{12} \cdot 3^4$.
- The discriminant is a square, and the resolvent cubic has no rational roots via the rational root test.
- So we conclude that the Galois group is $\boxed{A_4}$.

Quartic Polynomials, XVIII

Example: Find the Galois groups of each of the following quartic polynomials:

3. $f(y) = y^4 + 2y - 2$ over $\mathbb{Q}$. $[\Delta = -2^4 \cdot 5 \cdot 31.]$

- This polynomial is irreducible by Eisenstein, and its resolvent cubic is $g(z) = z^3 + 8z + 4$ with discriminant $\Delta = -4 \cdot 8^3 - 27 \cdot 4^2 = -2^4 \cdot 5 \cdot 31$.
- Since the discriminant is not a square, and the resolvent cubic has no rational roots (via the rational root test), by our criterion we conclude that the Galois group is $\boxed{S_4}$.

Quartic Polynomials, XIX

Example: Find the Galois groups of each of the following quartic polynomials:

4. $f(y) = y^4 - 14y^2 + 9$ over $\mathbb{Q}$. [$\Delta = 2^{14} \cdot 3^2 \cdot 5^2$.]

- One may verify by direct calculation that f is irreducible (it has no roots by the rational root test, and also does not factor as the product of two integral quadratics).
- Resolvent cubic is $g(z) = z^3 + 28z^2 + 160z = z(z+8)(z+2)$, with discriminant $\Delta = 2^{14} \cdot 3^2 \cdot 5^2$.
- Since the discriminant is a square, and the resolvent cubic splits completely over $\mathbb{Q}$, by our criterion we conclude that the Galois group is $\boxed{V_4}$.
- In this case, we may compute the roots explicitly using the quadratic formula to solve for y^2 and then simplify the square root: the roots are $\pm\sqrt{2} \pm \sqrt{5}$.

Quartic Polynomials, XX

Example: Find the Galois groups of each of the following quartic polynomials:

5. $f(y) = y^4 + 5y + 5$ over $\mathbb{Q}$. $[\Delta = 5^3 \cdot 11^2.]$

- This polynomial is irreducible by Eisenstein. Resolvent cubic is $g(z) = z^3 - 20z + 25 = (z+5)(z^2 - 20z + 25)$ with discriminant $\Delta = -4 \cdot (-20)^3 - 27 \cdot 25^2 = 5^3 \cdot 11^2$.
- Since the discriminant is not a square, and the resolvent cubic has a root, the Galois group is either C_4 or $D_{2\cdot 4}$.
- To determine which of these it is, we see that the root of $g(z)$ is $r' = -5$, so we must test the reducibility of $x^2 + r' = x^2 - 5$ and $x^2 + (r' - p)x + r = x^2 - 10x + 5$ over $\mathbb{Q}(\sqrt{5^3 \cdot 11^2}) = \mathbb{Q}(\sqrt{5})$.
- These quadratics both factor over $\mathbb{Q}(\sqrt{5})$ since their roots are $\pm\sqrt{5}$ and $5 \pm 2\sqrt{5}$. Hence the Galois group is $\boxed{C_4}$.

Quartic Polynomials, XXI

By exploiting the resolvent cubic, we can extend Cardano's formulas to solve the general quartic as well.

- Explicitly, by Cardano's formulas, we may compute the solutions $\theta_1, \theta_2, \theta_3$ of the resolvent cubic.
- To find the roots $\beta_1, \beta_2, \beta_3, \beta_4$ of the original quartic, we must then solve the system $\theta_1 = (\beta_1 + \beta_2)(\beta_3 + \beta_4)$, $\theta_2 = (\beta_1 + \beta_3)(\beta_2 + \beta_4)$, and $\theta_3 = (\beta_1 + \beta_4)(\beta_2 + \beta_3)$.
- However, since $\beta_1 + \beta_2 + \beta_3 + \beta_4 = 0$, we see that $\theta_1 = -(\beta_1 + \beta_2)^2$, $\theta_2 = -(\beta_1 + \beta_3)^2$, and $\theta_3 = -(\beta_2 + \beta_3)^2$.
- Taking the square roots then yields $\beta_1 + \beta_2 = \pm\sqrt{-\theta_1}$, $\beta_1 + \beta_3 = \pm\sqrt{-\theta_2}$, and $\beta_2 + \beta_3 = \pm\sqrt{-\theta_3}$.
- The square roots are not independent, however, since we also have $(\beta_1 + \beta_2)(\beta_1 + \beta_3)(\beta_2 + \beta_3) = -q$, so the choice of any two determines the third. We can compute $\beta_1, \beta_2, \beta_3$ from the equations above, and then $\beta_4 = -\beta_1 - \beta_2 - \beta_3$.

Quartic Polynomials, XXII

In practice, the solutions obtained by this technique are sufficiently complicated that they are not especially useful (other than as a demonstration of the existence of a general formula for the roots).

- For example, for the quartic $g(y) = y^4 + 2y - 2$ with resolvent cubic $h(z) = z^3 + 8z + 4$, Cardano's formulas yield $A = \sqrt[3]{-2 + \sqrt{\frac{620}{27}}}$ and $B = \sqrt[3]{-2 - \sqrt{\frac{620}{27}}}$, with both cube roots real for concreteness.
- Then the three roots of g are $A + B$, $\zeta_3 A + \zeta_3^2 B$, and $\zeta_3^2 A + \zeta_3 B$, so we obtain an explicit root of f as

$$\frac{1}{2}\sqrt{\sqrt[3]{-2+\sqrt{\frac{620}{27}}}+\sqrt[3]{-2-\sqrt{\frac{620}{27}}}}+\frac{1}{2}\sqrt{\zeta_3\sqrt[3]{-2+\sqrt{\frac{620}{27}}}+\zeta_3^2\sqrt[3]{-2-\sqrt{\frac{620}{27}}}}$$

$$-\frac{1}{2}\sqrt{\zeta_3^2\sqrt[3]{-2+\sqrt{\frac{620}{27}}}+\zeta_3\sqrt[3]{-2-\sqrt{\frac{620}{27}}}} \approx 0.34845 - 1.24753i,$$

which one may confirm with a numerical root-finder.

Computing Galois Groups over $\mathbb{Q}$, I

We would like to extend our work on the Galois groups of cubic and quartic polynomials to higher degree.

- Unfortunately, there is a substantial computational obstruction to doing this, namely that we require a description of the transitive subgroups of S_n in order to analyze the possible Galois groups of an irreducible polynomial.
- When n is large or has many prime factors, there are very many transitive subgroups of S_n (since, for example, any subgroup containing an n-cycle is automatically transitive) and there is no obvious method for cataloguing them.

Computing Galois Groups over $\mathbb{Q}$, II

Let's assume we do have a list of the transitive subgroups of S_n.

- Then, assuming we have verified that a polynomial $f(t) \in F[t]$ is irreducible, the Galois group of f must be one of the groups on our list.
- If we can somehow glean enough information about the permutations in this subgroup, in principle we should be able to determine the Galois group exactly.

If F is a subfield of $\mathbb{R}$, one simple way we can obtain information is by looking at the action of complex conjugation on the roots of f.

- Since the roots of f necessarily come in complex conjugate pairs, complex conjugation will act as a product of k 2-cycles, where k is the number of conjugate pairs of roots.
- In some cases this is enough to show that the Galois group must actually be S_n.

Computing Galois Groups over $\mathbb{Q}$, III

But let's assume that we do have a list of all of the transitive subgroups of S_n. Generating such a list is a finite calculation for any fixed n and it only has to be done once.

- Then, assuming we have verified that a polynomial $f(t) \in F[t]$ is irreducible, the Galois group of f must be one of the groups on our list.
- If we can somehow glean enough information about the permutations in this subgroup, in principle we should be able to determine the Galois group exactly.

Computing Galois Groups over $\mathbb{Q}$, IV

Example: Show $f(t) = t^5 - 4t + 2$ has three real roots and two complex-conjugate roots over $\mathbb{Q}$.

- Since $f(-2) = -14$, $f(0) = 2$, $f(1) = -1$, and $f(2) = 18$, f has at least 3 real roots by the intermediate value theorem.
- On the other hand, since $f'(t) = 5t^4 - 4$, we see that there are two values at which $f'(t) = 0$ (namely $t = \pm\sqrt[4]{4/5}$) and therefore by Rolle's theorem f can have at most 3 real roots.
- Alternatively, we could use Descartes' rule of signs to see that f has at most 3 real roots.
- Hence f has exactly 3 real roots, and thus also has 2 complex-conjugate roots.

Computing Galois Groups over $\mathbb{Q}$, V

Example: Show $f(t) = t^5 - 4t + 2$ has Galois group S_5 over $\mathbb{Q}$.

- Since f has two complex-conjugate roots, complex conjugation is an element of the Galois group that acts as a transposition.
- Furthermore, since f is irreducible by Eisenstein's criterion, any root generates an extension of degree 5 over $\mathbb{Q}$.
- Thus by the fundamental theorem of Galois theory, the Galois group must have order divisible by 5, so by Cauchy's theorem, it must contain an element of order 5. But the only elements of order 5 in S_5 are 5-cycles, so G contains a 5-cycle.
- By relabeling we may assume the transposition is $(1\,2)$, and then by taking an appropriate power of the 5-cycle we may assume that 2 follows 1 in its cycle decomposition, and then by relabeling we may assume it is $(1\,2\,3\,4\,5)$.
- As you showed on the midterm, $(1\,2)$ and $(1\,2\,3\,4\,5)$ generate S_5, and so we must have $G = S_5$.

Computing Galois Groups over $\mathbb{Q}$, VI

We may obtain additional information about the cycle structures of elements in the Galois group by appealing to the following theorem from algebraic number theory:

Theorem (Dedekind-Frobenius)

If $f(t) \in \mathbb{Z}[t]$ is irreducible with Galois group G over $\mathbb{Q}$, then for any prime p not dividing the discriminant $\Delta(f)$, if the mod-p reduction of $f(t)$ factors over $\mathbb{F}_p$ as a product of terms having degrees $k_1, k_2, \ldots, k_d$, then G contains a permutation having a cycle decomposition of lengths $k_1, k_2, \ldots, k_d$.

There is a more general result about factorizations of ideals in Dedekind domains (which was, in fact, Dedekind's primary motivation for defining the general notion of an ideal of a ring) that contains this fact as a special case.

Computing Galois Groups over $\mathbb{Q}$, VII

Using the Dedekind-Frobenius theorem, we may therefore determine cycle types for elements of the Galois group by factoring $f(t)$ modulo p for many primes p.

- Furthermore, it follows from another theorem of algebraic number theory (the Chebotarev density theorem) that the asymptotic proportion of primes for which $f(t)$ factors into terms of degrees $k_1, k_2, \ldots, k_d$ is proportional to the number of permutations in G with cycle type $k_1, k_2, \ldots, k_d$.
- By computing the factorization of $f(t)$ modulo p for a reasonably large number of primes p and tallying the results, one may therefore identify an optimal candidate for the Galois group by comparing the proportions of cycle types observed to the proportion of cycle types in the possible transitive subgroups of S_n.

Computing Galois Groups over $\mathbb{Q}$, VIII

We will now list the transitive subgroups of S_n for some smaller values of n (along with the distribution of cycle types):

- There is a standard labeling of the transitive subgroups of S_n due to Conway, Hulpke, and McKay, which we include with the tables.
- We also remark that many subgroups have (isomorphic) conjugates inside S_n, and the list of generators is only one possibility among many.

Computing Galois Groups over $\mathbb{Q}$, IX

In degree 5, there are 5 transitive subgroups of S_5, with generators and cycle types as follows:

	#	Name	Generators	1	2	2,2	3	2,3	4	5
5T1	5	C_5	(1 2 3 4 5)	1						4
5T2	10	$D_{2\cdot 5}$	(1 2 3 4 5), (1 5)(2 4)	1		5				4
5T3	20	F_{20}	(1 2 3 4 5), (1 2 4 3)	1		5			10	4
5T4	60	A_5	(1 2 3), (3 4 5)	1		15	20			24
5T5	120	S_5	(1 2 3 4 5), (1 2)	1	10	15	20	20	30	24

Computing Galois Groups over $\mathbb{Q}$, X

In degree 6, there are 16 transitive subgroups of S_6:

	#	Name	1	2	2,2	2,3	2,4	2,2,2	3	3,3	4	5	6
6T1	6	C_6	1					1		2			2
6T2	6	S_3	1					3		2			
6T3	12	$S_3 \times C_2$	1		3			4		2			2
6T4	12	A_4	1		3					8			
6T5	18	F_{18}	1					3	4	4			6
6T6	24	$A_4 \times C_2$	1	3	3			1		8			8
6T7	24	S_4 (a)	1		9		6			8			
6T8	24	S_4 (b)	1		3			6		8	6		
6T9	36	$S_3 \times S_3$	1		9			6	4	4			12
6T10	36	F_{36}	1		9		18		4	4			
6T11	48	$S_4 \times C_2$	1	3	9		6	7		8	6		8
6T12	60	A_5	1		15					20		24	
6T13	72	$F_{36} \rtimes C_2$	1	6	9	12	18	6	4	4			12
6T14	120	S_5	1		15			10		20	30	24	20
6T15	360	A_6	1		45		90		40	40		144	
6T16	720	S_6	1	15	45	120	90	15	40	40	90	144	120

Computing Galois Groups over $\mathbb{Q}$, XI

For degree 7, there are 7 transitive subgroups of S_7 (for any cycle type not listed, S_7 is the only transitive subgroup containing it):

	#	Name	1	2,2	2,4	2,2,2	2,2,3	3	3,3	5	6	7
7T1	7	C_7	1									6
7T2	14	$D_{2\cdot 7}$	1			7						6
7T3	21	F_{21}	1						14			6
7T4	42	F_{42}	1			7			14		14	6
7T5	168	$PSL_2(\mathbb{F}_7)$	1	21	42				56			48
7T6	2520	A_7	1	105	630		210	70	280	504		720
7T7	5040	S_7	1	105	630	105	210	70	280	504	840	720

You have encountered the group F_{42} on one of your homework assignments.

Computing Galois Groups over $\mathbb{Q}$, XII

For degree 8, there are 50 transitive subgroups of S_8.

- We will not list these, although we will mention that there are two subgroups of order 96 (specifically, groups 8T32 and 8T33) that have the same collection of cycle types appearing with the same frequencies.
- Here are the numbers of transitive subgroups of S_n for the values of n up through 21 (taken from John Jones' database of transitive groups at https://hobbes.la.asu.edu/Groups/):

n	9	10	11	12	13	14	15	16	17	18	19	20	21
# Groups	34	45	8	301	9	63	104	1954	10	983	8	1117	164

Computing Galois Groups over $\mathbb{Q}$, XIII

We can use these tables to compute probable Galois groups for irreducible polynomials of degree ≤ 7.

- What we do is compute the factorization of the polynomial modulo primes not dividing its discriminant and listing the corresponding cycles that must appear in its Galois group.
- We can also check whether the discriminant is a square, which will tell us whether G is a subgroup of A_n.
- In most cases, the result will not provably establish the Galois group (except generally for A_n and S_n).
- But, once we have identified a candidate for the Galois group, we can construct resolvent polynomials (similar to the resolvent cubic we used for the quartic) and then use information about their roots and factorizations to eliminate all of the other possible Galois groups.

Computing Galois Groups over $\mathbb{Q}$, XIV

For example, to establish that a particular polynomial of degree 5 has Galois group $D_{2\cdot 5} = \langle (1\,2\,3\,4\,5), (1\,5)(2\,4) \rangle$ requires eliminating the possibility that the Galois group is $A_5 = \langle (1\,2\,3), (3\,4\,5) \rangle$.

- One way to do this is to compute the resolvent polynomial whose roots are the S_5-permutations of $\beta_1\beta_2 + \beta_2\beta_3 + \beta_3\beta_4 + \beta_4\beta_5 + \beta_5\beta_1$, which in this case has degree 12 (there are 11 other possible results of permuting the indices, like $\beta_1\beta_3 + \beta_2\beta_4 + \beta_3\beta_5 + \beta_4\beta_1 + \beta_5\beta_2$). This will differentiate between $D_{2\cdot 5}$ and A_5 since $D_{2\cdot 5}$ fixes several of these elements (so the resolvent polynomial will have a rational root) but A_5 does not.
- Notice that, unlike the case of the resolvent cubic for the quartic, the resolvent polynomial for $D_{2\cdot 5}$ has degree 12, which much larger than the degree of the original quintic polynomial. (This is a typical phenomenon when $n \geq 5$.)

Computing Galois Groups over $\mathbb{Q}$, XV

Example: Determine the probable Galois group of $f(t) = t^5 - t^2 - 2t - 3$, with discriminant $\Delta = 17^2 \cdot 29^2$.

- Computing the factorization of $f(t)$ modulo p for the 100 smallest primes excluding 17 and 29 yields the following cycles:

Factorization Type	1	2	2,2	3	2,3	4	5
# Appearances	1		20	30			49

- The only transitive subgroup contained in A_5 having these cycle types is A_5 itself, so in fact we have proven that the Galois group of this polynomial is A_5.
- Note that the distribution of the factorization types matches fairly closely with the distribution of cycle types in A_5, as should be expected.

Computing Galois Groups over $\mathbb{Q}$, XVI

Example: Determine the probable Galois group of $f(t) = t^5 - 5t^2 - 3$ of discriminant $\Delta = 3^2 \cdot 5^6$.

- The Galois group is a subgroup of A_5.
- Computing the factorization of $f(t)$ modulo p for the 100 smallest primes excluding 3 and 5 yields the following cycles:

Factorization Type	1	2	2,2	3	2,3	4	5
# Appearances	8		54				38

- The only transitive subgroups contained in A_5 having these cycle types are $D_{2\cdot 5}$ and A_5.
- Since $D_{2\cdot 5}$ has no 3-cycles (in contrast to A_5, $1/3$ of whose elements are 3-cycles) we would expect no factorizations to have a 3-cycle if the Galois group were $D_{2\cdot 5}$, but about $1/3$ of them if the Galois group were A_5.
- Since no 3-cycles appear in the computed factorizations, it seems overwhelmingly likely that the Galois group is $D_{2\cdot 5}$.

Computing Galois Groups over $\mathbb{Q}$, XVII

Example: Determine the probable Galois group of $f(t) = t^6 - t^5 - t^2 + t + 1$, of discriminant $\Delta = -3^3 \cdot 433$.

- The Galois group is not a subgroup of A_6.
- Computing the factorization of $f(t)$ modulo p for the 100 smallest primes excluding 3 and 433 yields the following cycles:

Type	1	2	2,2	2,3	2,4	2,2,2	3	3,3	4	5	6
#	1	4	14	17	29	6	8	3			18

- There are only two transitive subgroups that contain cycles of each of these types: the subgroup 6T13 of order 72 and the subgroup 6T16 (which is S_6).
- Since 6T16 has no 4-cycles or 5-cycles (in contrast to S_6, roughly $1/3$ of whose elements are 4-cycles or 5-cycles), and no 4-cycles or 5-cycles appear in the computed factorizations, it seems overwhelmingly likely that the Galois group is 6T13.

Computing Galois Groups over $\mathbb{Q}$, XVIII

Example: Determine the probable Galois group of $f(t) = t^7 - 7t + 3$, of discriminant $\Delta = 3^8 \cdot 7^8$.

- The Galois group is a subgroup of A_7.
- Computing the factorization of $f(t)$ modulo p for the 100 smallest primes excluding 3 and 7 yields the following cycles:

Type	1	2,2	2,4	2,2,2	2,2,3	3	3,3	5	6	7
#		15	32				32			21

- There are only two transitive subgroups contained in A_7 that contain cycles of each of these types: $PSL_2(\mathbb{F}_7)$ and A_7.
- As above, since the observed factorization types match the cycles of $PSL_2(\mathbb{F}_7)$ very closely (in contrast to A_7, which also has 3-cycles, 2,2,3-cycles, and 5-cycles), the probable Galois group is $PSL_2(\mathbb{F}_7)$.

Summary

We analyzed the Galois groups of quartic polynomials and described how to find their roots.

We discussed some methods for computing Galois groups of polynomials of degrees 5 through 7 over $\mathbb{Q}$.

Next lecture: Solvability in radicals, Abel's theorem on the insolvability of the quintic.