Math 5111 (Algebra 1)

Lecture #24 of 24 $\sim$ December 7th, 2020

Solvability in Radicals

- Radical Extensions
- Solvable Groups
- The Abel-Ruffini Theorem on the Insolvability of the Quintic
- The Fundamental Theorem of Algebra

This material represents §4.4.6 from the course notes.

Radical Extensions, I

We have described ways to compute Galois groups for polynomials of moderate degree, and a natural followup is to try to find "formulas in radicals", similar to the cubic and quartic formulas, for the roots of these polynomials.

- Explicitly, we consider a formula in radicals to be one that is constructed via some combination of field operations (addition, subtraction, multiplication, division) and extraction of *n*th roots.

So, we need to study field extensions obtained by adjoining *n*th roots of elements.

Definition

If F is a field, the extension field K/F is a simple radical extension of K if $K = F(\beta)$ for some β with $\beta^n \in F$ for some n.

Radical Extensions, II

For any $a \in F$ we will write $a^{1/n}$ to denote an arbitrary choice of a root β of the polynomial $x^n - a$ in an algebraic closure of F.

- For an arbitrary F, the extension $F(a^{1/n})$ will not be Galois in general: its normal closure will be the splitting field of $x^n - a$ over F, which is only equal to $F(a^{1/n})$ when $F(a^{1/n})$ contains the nth roots of unity.
- In particular, if F itself contains the nth roots of unity, then $F(a^{1/n})$ will automatically be Galois over F for any $a \in F$, as long as $x^n - a$ is separable (which occurs precisely when n is not divisible by the characteristic of F and $a \neq 0$).
- In this case, any automorphism $\sigma \in \mathrm{Gal}(F(a^{1/n})/F)$ is uniquely determined by the value of $\sigma(a^{1/n}) = a^{1/n}\zeta$ for some nth root of unity ζ.
- We may then essentially compute the Galois group $\mathrm{Gal}(F(a^{1/n})/F)$, which turns out always to be cyclic.

Radical Extensions, III

More precisely, we have the following:

Theorem (Simple Radical Extensions)

Let F be a field of characteristic not dividing n that contains the nth roots of unity. Then for any $a \in F^{\times}$, the field $F(a^{1/n})/F$ is Galois and its Galois group is cyclic of order dividing n. Conversely, any cyclic Galois extension K/F of order dividing n has the form $K = F(a^{1/n})$ for some $a \in F$.

The main idea for the forward direction is to write down an injective map from the Galois group to the cyclic group of nth roots of unity.

Radical Extensions, IV

Proof (forward):

- First let $a \in F^\times$. Since F contains the nth roots of unity, $F(a^{1/n})$ is the splitting field of $x^n - a$ over F.
- Since $\mathrm{char}(F)$ does not divide n and $a \neq 0$, $x^n - a$ is separable, and so $F(a^{1/n})/F$ is Galois.
- If $G = \mathrm{Gal}(F(a^{1/n})/F)$, then for any $\sigma \in G$ we have $\sigma(a^{1/n}) = a^{1/n}\zeta_{(\sigma)}$ for some nth root of unity $\zeta_{(\sigma)}$.
- We therefore have a map $\varphi : G \to \mu_n$ from G to the cyclic group μ_n of nth roots of unity by setting $\varphi(\sigma) = \zeta_{(\sigma)} = \sigma(a^{1/n})/a^{1/n}$.

Radical Extensions, IV

Proof (forward, more):

- We have a map $\varphi : G \to \mu_n$ from G to the cyclic group μ_n of nth roots of unity by setting $\varphi(\sigma) = \zeta_{(\sigma)} = \sigma(a^{1/n})/a^{1/n}$.
- Then $\varphi(\sigma\tau) = \sigma(\tau(a^{1/n}))/a^{1/n} = \sigma(a^{1/n}\zeta_{(\tau)})/a^{1/n} = \sigma(a^{1/n})\zeta_{(\tau)}/a^{1/n} = \zeta_{(\sigma)}\zeta_{(\tau)} = \varphi(\sigma)\varphi(\tau)$ for any $\sigma, \tau \in G$, so φ is a group homomorphism.
- Furthermore, $\ker \varphi$ consists of the automorphisms fixing $a^{1/n}$, hence is trivial.
- Thus, by the first isomorphism theorem, we see that φ yields an isomorphism of G with its image inside μ_n.
- Since $\mathrm{im}\,\varphi$ is a subgroup of μ_n, it is cyclic of order dividing n as claimed.

Radical Extensions, V

Proof (reverse):

- For the converse, suppose K/F is cyclic Galois of order dividing n, where F contains the nth roots of unity and $\mathrm{char}(F)$ does not divide n.
- Let σ be a generator of $G = \mathrm{Gal}(K/F)$ and ζ be a primitive nth root of unity.
- Then because the automorphisms $1, \sigma, \sigma^2, \dots, \sigma^{n-1}$ are linearly independent, there exists an $\alpha \in K$ such that $\beta = \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha)$ is nonzero.

Radical Extensions, V

Proof (reverse, more):

- With $\beta = \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha)$, we have $\zeta\sigma(\beta) = \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha) + \zeta^n\sigma^n(\alpha) = \beta$, since both ζ and σ have order dividing n.
- This implies $\sigma(\beta) = \zeta^{-1}\beta$, and so iterating this yields $\sigma^k(\beta) = \zeta^{-k}\beta$. In particular, since $\beta \neq 0$ we see that β is not fixed by any nonidentity element of G, and so $K = F(\beta)$.
- Finally, we have $\sigma(\beta^n) = \zeta^{-n}\beta^n = \beta^n$ so β^n is fixed by σ hence by all of G, and thus $\beta^n = a$ is an element of F.
- This means $K = F(a^{1/n})$ for some $a \in F$, as claimed.

Remark: The element β is called a Lagrange resolvent. We can find it by looking for an element of K with the property that $\sigma(\beta) = \zeta^{-1}\beta$: if we write $\beta = \alpha + c_1\sigma(\alpha) + \cdots + c_n\sigma^{n-1}(\alpha)$, we can then compute the coefficients c_i using the action of σ.

Radical Extensions, VI

Now that we have characterized the extensions obtained by adjoining nth roots of individual elements, we can give a precise definition for solving an equation in radicals:

Definition

If $\alpha \in F$, we say α can be expressed in radicals of α is an element of some tower of simple radical extensions, namely, if there exist extensions $F = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_d = K$ such that $\alpha \in K$ and K_{i+1}/K_i is a simple radical extension for each i, and we say K/F is a root extension. We also say a polynomial $f(x) \in F[x]$ is solvable in radicals if each of its roots can be expressed in radicals.

Radical Extensions, VII

Examples:

1. The algebraic number $\sqrt[3]{2+7\sqrt{2+\sqrt{5}}-8\sqrt[9]{17}}$ can be expressed in radicals over $\mathbb{Q}$.
2. Any element of a cubic or quartic polynomial can be expressed in radicals, since we gave explicit constructions for the roots of these polynomials.
3. Any root of unity can be expressed in radicals, since by definition any nth root of unity is an nth root of 1.
4. Any constructible number can be expressed in radicals, since (as we proved) the constructible numbers are those which are contained in some tower of quadratic extensions.

Radical Extensions, VIII

We make a few basic observations about root extensions:

- The composite of two root extensions of F is also a root extension of F. Explicitly, if $F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_d = K$ and $F = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_k = L$ are two towers of simple radical extensions, then so is $F = K_0L_0 \subseteq K_1L_0 \subseteq K_2L_0 \subseteq \cdots \subseteq K_dL_0 \subseteq K_dL_1 \subseteq \cdots \subseteq K_dL_k = KL$.
- In particular, the set of all elements in the algebraic closure $\overline{F}$ that can be expressed in radicals is a subfield of $\overline{F}$.
- Also, if α can be expressed in radicals and $\sigma(\alpha)$ is any Galois conjugate, then $\sigma(\alpha)$ can also be expressed in radicals, because $F = K_0 \subseteq \sigma(K_1) \subseteq \cdots \subseteq \sigma(K_d) = \sigma(K)$ is also a tower of simple radical extensions.

Radical Extensions, IX

We would like to characterize the elements $\alpha \in \overline{F}$ that can be expressed in radicals, which (by our observation about Galois conjugates) is equivalent to characterizing the polynomials in $F[x]$ that are solvable in radicals.

- We would like to be able to give a statement requiring information only about the minimal polynomial of α, but in order to do this we first need to see that α is contained in a Galois root extension.

Proposition (Elements Expressible in Radicals)

If α can be expressed in radicals over F, then α is contained in a root extension L having a tower $F = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_k = L$ where L is Galois over F and each intermediate extension L_{i+1}/L_i is Galois with cyclic Galois group.

Radical Extensions, X

Proof:

- Suppose α can be expressed in radicals over F.
- Then by our observation earlier, all Galois conjugates $\sigma(\alpha)$ can also be expressed in radicals over F, and so the splitting field K of the minimal polynomial of α is a root extension of F.
- This means that there is a tower of simple radical extensions $F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_d = K$, where K_{i+1}/K_i is obtained by extracting an n_ith root.
- If we let E be the field obtained by adjoining all n_ith roots of unity to F, then E/F is a simple radical extension of F, since it is obtained by adjoining a root of the polynomial $x^{n_1 n_2 \cdots n_{d-1}} - 1$.

Radical Extensions, XI

Proof (continued):

- We have a tower $F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_d = K$ of simple radical extensions, and also, E is the field obtained by adjoining all n_ith roots of unity to F. Now consider the tower $F \subseteq E = EK_0 \subseteq EK_1 \subseteq \cdots \subseteq EK_d = EK$.
- Each extension EK_{i+1}/EK_i is a simple radical extension obtained by extracting an n_ith root of unity, and since all of these roots of unity are in E (hence in EK_i), by our characterization of simple radical extensions, these extensions are all Galois with cyclic Galois group.
- Now just set $L_1 = E$ and $L_{i+1} = EK_i$ for $i \geq 1$, with $L = EK$. Then L is Galois over F (since it is the composite of two Galois extensions E/F and K/F) and each extension L_{i+1}/L_i is Galois with cyclic Galois group, as required.

Radical Extensions, XII

By applying the fundamental theorem of Galois theory to the tower constructed in the last proof, we obtain a necessary condition on the Galois group of L/F in order for L/F to be a Galois root extension.

- Explicitly, let G_i be the subgroup of $G = \mathrm{Gal}(L/F)$ associated to the intermediate extension L_i.
- Then the Galois correspondence yields a chain of subgroups $G = G_0 \geq G_1 \geq \cdots \geq G_k = \{e\}$ such that G_{i+1} is normal in G_i and the quotient group G_i/G_{i+1} is cyclic for each i.
- We now switch perspective from fields to groups, and study groups that have a chain of subgroups of this form.

Solvable Groups, I

Here is the requisite property of groups that we want to study:

Definition

A finite group G is solvable if there exists a chain of subgroups $G = G_0 \geq G_1 \geq \cdots \geq G_k = \{e\}$ such that G_{i+1} is normal in G_i and the quotient group G_i/G_{i+1} is cyclic for each $0 \leq i \leq k-1$.

We emphasize in the definition that G_{i+1} is only required to be a normal subgroup of the previous subgroup G_i, and does not have to be a normal subgroup of G itself.

Solvable Groups, II

Examples:

1. Any finite abelian group is solvable, since every finite abelian group is a direct product of cyclic groups.
2. The dihedral group $D_{2 \cdot n}$ is solvable, since the subgroup $G_1 = \langle r \rangle$ is cyclic and the quotient group $D_{2 \cdot n}/G_1$ is also cyclic (it has order 2 and is generated by $\overline{s}$).
3. The symmetric group S_4 is solvable, via the chain $S_4 \geq A_4 \geq V_4 \geq \langle (1\,2)(3\,4) \rangle \geq \{e\}$, where $V_4 = \langle (1\,2)(3\,4), \, (1\,3)(2\,4) \rangle$. Note that V_4 is normal in A_4 since it is in fact normal in S_4, and each successive quotient is cyclic because it has prime order (either 2 or 3).
4. Any non-cyclic simple group is *not* solvable, because it has no nontrivial normal subgroups (and thus there is no way to start the chain).

Solvable Groups, III

Here are some of the fundamental properties of solvable groups:

Proposition (Properties of Solvable Groups)

Let G be a group.

1. *If G is solvable, then any subgroup H is solvable and any quotient group G/N is solvable.*
2. *If N is a normal subgroup of G such that N and G/N are solvable, then G is solvable.*
3. *G is solvable if and only if G has a chain of subgroups $G = G_0 \geq G_1 \geq \cdots \geq G_k = \{e\}$ such that G_{i+1} is normal in G_i and the quotient group G_i/G_{i+1} is abelian.*
4. *Finite p-groups are solvable, as are finite nilpotent groups, and direct and semidirect products of solvable groups.*

Solvable Groups, IV

1. If G is solvable, then any subgroup H is solvable and any quotient group G/N is solvable.

Proof (subgroups):

- Suppose G is solvable with a chain $G = G_0 \geq G_1 \geq \cdots \geq G_k = \{e\}$ such that G_{i+1} is normal in G_i and G_i/G_{i+1} is cyclic.
- If H is a subgroup of G, let $H_i = G_i \cap H$ for each i.
- Then $H_{i+1} = H_i \cap G_{i+1}$, so by the second isomorphism theorem, we see that H_{i+1} is normal in H_i and $H_i/H_{i+1} = H_i/(H_i \cap G_{i+1}) \cong H_iG_{i+1}/G_{i+1}$.
- But since H_iG_{i+1} is a subgroup of G_i, the latter is a subgroup of G_i/G_{i+1} and hence cyclic. Hence we obtain a chain $H = H_0 \geq H_1 \geq \cdots \geq H_k = \{e\}$ such that H_{i+1} is normal in H_i and H_i/H_{i+1} is cyclic, so H is solvable.

Solvable Groups, V

1. If G is solvable, then any subgroup H is solvable and any quotient group G/N is solvable.

Proof (quotients):

- Suppose G is solvable with a chain $G = G_0 \geq G_1 \geq \cdots \geq G_k = \{e\}$ such that G_{i+1} is normal in G_i and G_i/G_{i+1} is cyclic.
- If N is a normal subgroup of G, let $\overline{G_i} = G_i/(G_i \cap N) \cong G_iN/N$ be the image of G_i in G/N.
- Then by the second and third isomorphism theorems, $(G_iN/N)/(G_{i+1}N/N) \cong G_iN/G_{i+1}N$, and the latter is isomorphic to a quotient of G_i/G_{i+1} by the second isomorphism theorem, hence is cyclic.
- Hence the chain $G/N = \overline{G_0} \geq \overline{G_1} \geq \cdots \geq \overline{G_k} = \{\overline{e}\}$ has the property that $\overline{G_{i+1}}$ is normal in $\overline{G_i}$ and $\overline{G_i}/\overline{G_{i+1}}$ is cyclic, so G/N is solvable.

Solvable Groups, VI

2. If N is a normal subgroup of G such that N and G/N are solvable, then G is solvable.

Proof:

- Suppose that N has a chain $N = N_0 \geq N_1 \geq \cdots \geq N_d = \{e\}$ and G/N has a chain $G/N = \overline{G_0} \geq \overline{G_1} \geq \cdots \geq \overline{G_k} = \{\overline{e}\}$.
- Then by the fourth isomorphism theorem we may lift each of the $\overline{G_i}$ to a subgroup G_i of G containing N with $G_i/G_{i+1} \cong \overline{G_i}/\overline{G_{i+1}}$.
- Then the chain $G = G_0 \geq G_1 \geq \cdots \geq G_k = N = N_0 \geq N_1 \geq \cdots \geq N_d = \{e\}$ shows G is solvable.

Solvable Groups, VII

3. G is solvable if and only if G has a chain of subgroups $G = G_0 \geq G_1 \geq \cdots \geq G_k = \{e\}$ such that G_{i+1} is normal in G_i and the quotient group G_i/G_{i+1} is abelian.

Proof:

- If G is solvable then it clearly has such a chain (since cyclic groups are abelian).
- For the converse, we induct on k. The base case $k = 1$ is trivial since abelian groups are solvable as noted above.
- For the inductive step, suppose we have a chain $G = G_0 \geq G_1 \geq \cdots \geq G_k = \{e\}$ such that G_{i+1} is normal in G_i and the quotient group G_i/G_{i+1} is abelian.
- Then G_1 is solvable by the inductive hypothesis, and G/G_1 is also solvable (since it is abelian). Hence by (2), G is solvable.

Remark: This property is often taken as the definition of a solvable group, rather than ours (where successive quotients are cyclic).

Solvable Groups, VIII

4. Finite p-groups are solvable, as are finite nilpotent groups, and direct and semidirect products of solvable groups.

Proof:

- For p-groups of order p^n, we induct on n. The base case $n = 1$ is trivial. For the inductive step, we note that any p-group has a nontrivial center.
- If $G = Z(G)$ then the result is trivial since G is abelian.
- Otherwise, both $Z(G)$ and $G/Z(G)$ are p-groups of order less than p^n, so by the inductive hypothesis they are both solvable. Then G is solvable by (2).
- Direct and semidirect products of solvable groups are also solvable by (2), since the two components in the semidirect product are solvable by assumption.
- Finally, nilpotent groups are direct products of p-groups, so they are also solvable.

Solvability in Radicals, I

From our properties of solvable groups, we see that if $f(x)$ is solvable in radicals, then each of its roots is contained in a Galois extension L/F whose Galois group $\mathrm{Gal}(L/F)$ is solvable.

- The Galois group of $f(x)$ is $\mathrm{Gal}(K/F)$ where K is the splitting field for f.
- Since this is a quotient group of $\mathrm{Gal}(L/F)$ and quotient groups of solvable groups are solvable, $\mathrm{Gal}(K/F)$ is solvable.

Solvability in Radicals, II

Our central result is that the converse is true also.

Theorem (Solvability in Radicals)

Let F be a field and $f(x) \in F[x]$ be a polynomial of degree n, where the characteristic of F does not divide $n!$ (in particular, if F has characteristic 0). Then $f(x)$ is solvable in radicals if and only if the Galois group of f is a solvable group.

This result (at least for $F = \mathbb{Q}$) is essentially due to Galois, and was the historical motivation for his development of Galois theory.

- Galois's use of groups here, viewed as permutations of the roots of a polynomial, was actually one of the fundamental motivations for the development of abstract group theory by Jordan and Cayley in the late 1800s.

Solvability in Radicals, III

Proof (forward):

- Note that any irreducible factor of f has degree at most n, hence dividing $n!$, so all irreducible factors of f are separable.
- By replacing f with the least common multiple of its irreducible factors (which does not change the roots), we may therefore assume f is separable.
- Now suppose f is solvable in radicals, and let K be the splitting field of f, with $G = \mathrm{Gal}(K/F)$.
- If α is any root of f, then α is expressible in radicals, and so by our proposition, there exists a Galois extension L_α/F containing α such that $\mathrm{Gal}(L_\alpha/F)$ is solvable.

Solvability in Radicals, IV

Proof (forward more):

- Then the composite L of all the L_α over all roots α of f is also Galois over F, and its Galois group is a subgroup of the direct product of the $\mathrm{Gal}(L_\alpha/F)$ by our results on Galois groups of composite extensions.
- Since the direct product of solvable groups is solvable, and subgroups of solvable groups are solvable, this means the Galois group of L/F is solvable.
- Since L contains all roots of f, it contains K, and so by the fundamental theorem of Galois theory $G = \mathrm{Gal}(K/F)$ is a quotient of $\mathrm{Gal}(L/F)$.
- Thus G is a quotient of a solvable group, hence is solvable as claimed.

Solvability in Radicals, V

Proof (converse):

- For the converse, suppose G is solvable and has a chain $G = G_0 \geq G_1 \geq \cdots \geq G_k = \{e\}$ such that G_{i+1} is normal in G_i and G_i/G_{i+1} is cyclic of order n_i.
- By the fundamental theorem of Galois theory, the corresponding fixed fields $F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_k = K$ such that K_{i+1}/K_i is Galois with cyclic Galois group of order n_i.
- Now let E be the extension of F containing all of the n_ith roots of unity for each i, then E/F is Galois and a simple radical extension (as we have noted).

Solvability in Radicals, VI

Proof (converse more):

- We have a tower $F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_k = K$ such that K_{i+1}/K_i is Galois with cyclic Galois group of order n_i, and E is the extension of F containing all the necessary roots of unity.
- Then EK_{i+1}/EK_i is also Galois with cyclic Galois group of order dividing n_i by the "sliding-up" property of the Galois extension K_{i+1}/K_i.
- Then since E contains the n_ith roots of unity, we conclude that EK_{i+1}/EK_i is a simple radical extension.
- This means $F \subseteq E \subseteq EK_1 \subseteq EK_2 \subseteq \cdots \subseteq EK_k = EK$ is a tower of simple radical extensions containing all the roots of f, and so f is solvable in radicals as claimed.

The Simple Simplicity of A_n, I

Since we will need it imminently and I didn't actually prove the simplicity of A_n at any point, let me just do that right now:

Proposition (Simplicity of A_5)

The group A_5 is simple.

We show that the only nontrivial normal subgroup of A_5 is A_5 itself. We do this using a counting argument.

- The idea is that any normal subgroup of a group G consists of a union of conjugacy classes: normality requires that if one element of a conjugacy class is taken, then they all are.
- So we just have to find the conjugacy classes in A_5, and then show we cannot construct a proper subgroup using a union of some of them.

The Simple Simplicity of A_n, II

Proof:

- The conjugacy classes in A_n consist of elements having the same cycle type, since those are the conjugacy classes in S_n.
- By an orbit-stabilizer calculation, conjugacy classes in S_n either remain the same or split into two in A_n: more specifically, the number of classes in A_n equals $[S_n : A_n C_G(x)]$ for any x in the S_n-conjugacy class. This equals 1 if and only if x commutes with an odd permutation if and only if the cycle type of x consists of distinct odd integers.
- The only such elements in A_5 are the 5-cycles. Thus, the conjugacy classes in A_5 have sizes 1 (identity), 20 (3-cycles), 12 and 12 (5-cycles), and 15 (2,2-cycles).
- No sum of these numbers including 1 yields a divisor of 60 except the sum of all of them, so by Lagrange's theorem the only nontrivial normal subgroup of A_5 is A_5 itself.

The Simple Simplicity of A_n, III

Now we can establish the simplicity of A_n for larger n:

Theorem (Simplicity of A_n)

The group A_n is simple for all $n \geq 5$.

We first observe that the 3-cycles generate A_n.

- This follows by writing any element of A_n as a product of an even number of transpositions, and then observing that any pair of unequal transpositions has product equal to a 3-cycle or a 2,2-cycle.
- But any 2,2-cycle is the product of two 3-cycles: $(a\,b)(c\,d) = (a\,c\,d)(a\,b\,d)$. Thus the 3-cycles generate A_n.

We now give our main argument, which will reduce to showing that a nontrivial normal subgroup of A_n must contain a 3-cycle (hence all of them).

The Simple Simplicity of A_n, IV

Proof:

- We induct on n. We just established the base case $n = 5$, so now assume $n \geq 6$.
- Suppose H is a nontrivial normal subgroup of $G = A_n$ and let G_i be the stabilizer of i under the permutation action of A_n on $\{1, 2, \ldots, n\}$.
- Then $G_i \cong A_{n-1}$ is simple by the induction hypothesis.
- By properties of normality, the intersection $H \cap G_i$ is a normal subgroup of G_i for each i. But since G_i is simple, the only possibilities are $H \cap G_i = e$ or $H \cap G_i = G_i$.
- If $H \cap G_i = G_i$ for any i, then since all of the G_i are conjugate, we see that H contains all of the G_i, hence $(1\,2)(3\,4) \in G_5$ along with all of its conjugates.
- Then all of the 3-cycles are in H, and so $H = G$ by our observation that the 3-cycles generate A_n.

The Simple Simplicity of A_n, V

Proof (continued):

- We are left with the case where $H \cap G_i = e$ for all i.
- This means that no nonidentity element of H can stabilize any element of $\{1, 2, \ldots, n\}$.
- Now pick a nonidentity element $\sigma \in H$.
- If σ has a cycle $(a_1 a_2 a_3 \ldots)$ of length ≥ 3, conjugate by the permutation $(a_3 a_4 a_5) \in A_n$ with $a_4, a_5 \neq a_1, a_2, a_3$ to obtain the permutation $\tau \in H$ having a cycle $(a_1 a_2 a_4 \ldots)$. Then $\sigma\tau^{-1} \in H$ fixes a_1 but not a_2, contradiction.
- Otherwise, every $\sigma \in H$ is a product only of 2-cycles.
- Then conjugating a permutation $\sigma = (a_1 a_2)(a_3 a_4)(a_5 a_6) \cdots \in H$ by $(a_1 a_2)(a_3 a_5) \in A_n$ yields $\tau = (a_1 a_2)(a_4 a_5)(a_3 a_6) \cdots \in H$, but then $\sigma\tau \in H$ fixes a_1 but not a_3, contradiction. (Note we need $n \geq 6$ here!)

The Simple Simplicity of A_n, VI

While we're here, I figured I might also show you a beautiful argument of Bender, communicated to me by R. Foote via D. Dummit, to show that A_5 is the unique simple group of order 60:

- Let G be a simple group of order 60.
- Then the number n_5 of Sylow 5-subgroups of G is congruent to 1 modulo 5 and divides 12. It cannot be 1 since G has no nontrivial normal subgroups, so it must be 6.
- Now, G acts on these six Sylow 5-subgroups by conjugation. This yields a homomorphism from G into S_6, which must be faithful because the kernel is a normal subgroup of G.
- If H is the image of this homomorphism, then $H \cap A_6$ is either H or a subgroup of H of index 2. But if the latter case held, then the inverse image of $H \cap A_6$ in G would be a subgroup of G of index 2, which would be normal by one of your homework problems.

The Simple Simplicity of A_n, VII

Therefore, the image $H \subseteq S_6$ of the conjugation action of G on its six Sylow 5-subgroups actually lies inside A_6.

- Since H is isomorphic to G (the kernel is trivial), it has order 60 inside of A_6, which has order $6!/2 = 360$.
- Equivalently, H has index 6 inside A_6.
- Now, A_6 acts on the six left cosets of H by permutation.
- This yields a homomorphism from A_6 into S_6.
- Since A_6 is simple, by the same argument as on the previous slide, the kernel is trivial and the image must lie inside A_6, so it is an isomorphism of A_6 with itself.
- But now H is the stabilizer of the left coset eH, meaning that H is a point stabilizer inside of A_6.
- If we label eH as 6, then H is the set of even permutations inside S_6 fixing 6, which is simply a description of A_5.
- Thus, H hence G is isomorphic to A_5, as claimed.

The Insolvability of The Quintic, I

We can now put these last results together to obtain the famed Abel-Ruffini theorem on the insolvability of the general quintic:

Corollary (Abel-Ruffini Theorem)

If $n \geq 5$, the general equation of degree n is not solvable in radicals.

Proof:

- By our results on solvability, an equation is solvable in radicals if and only if its Galois group is solvable.
- As we showed, the Galois group of the general equation of degree n is S_n.
- But S_n is not solvable for any $n \geq 5$: if it were, then its subgroup A_n would be solvable, and that is not the case because A_n is a non-cyclic simple group for $n \geq 5$.
- Thus, the general equation of degree n is not solvable in radicals for any $n \geq 5$.

The Insolvability of The Quintic, II

We can also give specific examples of polynomials that are not solvable in radicals using the methods we have described previously for computing Galois groups.

- For example, as we noted earlier, the polynomial $f(t) = t^5 - 4t + 2$ has Galois group S_5 over $\mathbb{Q}$, and is therefore not solvable in radicals.
- Likewise, we also showed (by analyzing factorizations over $\mathbb{F}_p$) that the polynomial $f(t) = t^5 - t^2 - 2t - 3$ has Galois group A_5 over $\mathbb{Q}$, hence also is not solvable in radicals.
- As a third example, the polynomial $f(t) = t^7 - 7t + 3$ can be shown to have Galois group $PSL_2(\mathbb{F}_7) \cong SL_3(F_2)$, which is a simple group of order 168. This polynomial is therefore also not solvable in radicals.

The Non-Insolvability of Some Quintics, I

For polynomials whose Galois group is solvable, there do exist formulas in radicals for the roots, although of course these may be challenging to compute explicitly.

- We briefly outline the situation for $n = 5$.
- The possible Galois groups here are C_5 (order 5), $D_{2\cdot 5}$ (order 10), F_{20} (order 20), A_5 (order 60), and S_5 (order 120).
- It is not hard to see that the first three are solvable while the last two are not.
- Indeed, since each of C_5, $D_{2\cdot 5}$, and F_{20} is contained in F_{20}, an irreducible quintic is solvable in radicals precisely when its Galois group is a subgroup of F_{20}.

The Non-Insolvability of Some Quintics, II

As detailed in a 1991 paper of D. Dummit[1], this may in turn be determined by determining whether an associated resolvent polynomial for F_{20} (of degree 6) has a rational root, and if so, one may give explicit formulas in radicals for the roots of the quintic.

- For the quintic $f(x) = x^5 + px + q$ in particular, the resolvent sextic is $f_{20}(x) = x^6 + 8px^5 + 40p^2x^4 + 160p^3x^3 + 400p^4x^2 + (512p^5 - 3125q^4)x + (256p^6 - 9375pq^4)$, and the quintic $f(x)$ is solvable in radicals if and only if the resolvent sextic has a rational root.
- Example: For $f(x) = x^5 + 120x - 1344$ of discriminant $\Delta = 2^{11} \cdot 3^4 \cdot 5^6$, the resolvent sextic has a rational root $x = 1440$, and therefore f is solvable. Since the discriminant is not a square, its Galois group is not contained in A_5, and must therefore be F_{20}.

[1] *Solving Solvable Quintics*, Math. Comp., 57(195), 1991

Putting Algebra Into The Fundamental Theorem of Algebra, I

As one more fun application of Galois theory, I thought I'd show you how to prove the fundamental theorem of algebra using *algebra*, rather than complex analysis.

- An initial observation: $\mathbb{C}$ has no field extension of degree 2, because if $z = re^{i\theta}$ then $\sqrt{z} = r^{1/2}e^{i\theta/2} \in \mathbb{C}$.
- A second observation: any odd-degree polynomial with real coefficients has a real root. This is an immediate consequence of the intermediate value theorem.
- Thus, by the second observation, $\mathbb{R}$ has no nontrivial field extensions of odd degree: since any odd-degree irreducible polynomial must have a root, it must be linear.

Putting Algebra Into The Fundamental Theorem of Algebra, II

Now suppose that $p(x) \in \mathbb{C}[x]$ has positive degree: we claim that the Galois group of $p(x)$ over $\mathbb{C}$ is trivial, which will mean all its roots must lie in $\mathbb{C}$.

- Consider the polynomial $q(x) = p(x)\overline{p}(x)$. Complex conjugation fixes this polynomial since it interchanges p with $\overline{p}$, and so $q(x) \in \mathbb{R}[x]$.
- If K is the splitting field of $q(x)$, then $K/\mathbb{R}$ is Galois by definition: suppose the Galois group is G.
- By Sylow's theorems, G has a Sylow 2-subgroup H.
- Consider the fixed field E of H: by hypothesis, since the index of H in G is odd, by the fundamental theorem of Galois theory, the degree $[E : \mathbb{R}]$ is odd.
- But there are no nontrivial extensions of $\mathbb{R}$ of odd degree, so in fact $E = \mathbb{R}$, and thus $H = G$.

Putting Algebra Into The Fundamental Theorem of Algebra, III

This means the Galois group of $q(x) = p(x)\overline{p}(x)$ over $\mathbb{R}$ is a 2-group, so its splitting field $K/\mathbb{R}$ has degree equal to a power of 2.

- Then $K(i)/\mathbb{C}$ is also Galois by the sliding-up property, and its degree is also a power of 2.
- However, as we showed, any p-group G has a filtration of subgroups $\{e\} = G_0 \leq G_1 \leq G_2 \leq \cdots \leq G_k = G$ where each subgroup has index p in the next.
- Applying this observation to G shows that it has a chain of subgroups $\{e\} = G_0 \leq G_1 \leq G_2 \leq \cdots \leq G_k = G$ each of index 2 in the previous.
- But unless G is trivial, the Galois correspondence yields a chain of subfields $\mathbb{C} \leq E \leq \cdots \leq K(i)$, and in particular we have a field E with $[E : \mathbb{C}] = 2$.
- But there is no such field E. Therefore, G must be the trivial group, and so $p(x)$ splits completely over $\mathbb{C}$.

Some Heavier-Duty Group Theory, I

I thought it might also be useful to summarize some of the more heavy-duty group theory results related to simplicity and solvability.

Theorem (Burnside's $p^a q^b$ Theorem)

If p and q are primes, then any group of order $p^a q^b$ is solvable.

The "easiest" approach to Burnside's $p^a q^b$ theorem is to use representation theory, which (in its simplest description) concerns groups acting on vector spaces, or, equivalently, homomorphisms $\varphi : G \to GL(V)$.

Some Heavier-Duty Group Theory, II

Groups of odd order are also solvable:

Theorem (Feit-Thompson Theorem)

Every finite group of odd order is solvable.

The proof of this theorem is 255 pages, representing an entire issue of the Pacific Journal of Mathematics[2]. This result is one of the first lengthy arguments published in group theory; before this paper, most group theory papers were comparatively short.

[2] *Solvability of groups of odd order*, Pac. J. Math. 13:775–1029 (1962)

Some Heavier-Duty Group Theory, III

Even if a finite group G is not solvable, we can still think of building G up from simple groups.

- More specifically, G always possesses a composition series: a chain of subgroups $\{e\} = G_0 \leq G_1 \trianglelefteq G_2 \leq \cdots \leq G_n = G$ such that each G_i is normal in G_{i+1} and the successive quotients G_{i+1}/G_i are simple.
- The existence of a composition series is easy to establish by induction. The individual quotients in the chain are called the composition factors of G and are akin to irreducible factors in a factorization. More specifically:

Theorem (Jordan-Hölder Theorem)

Any two composition series for a group have the same length and composition factors, up to rearrangement and isomorphism.

So, What Now?

Here marks the official end of the material for this course.

- Of course, there is much more algebra out there to learn. The next course to take is Math 5112, which treats the fundamentals of commutative algebra: rings and modules and all of the various things you can do with them.
- If you like Galois theory, the natural next thing to learn is some algebraic number theory, which is more focused on studying finite-degree extensions of $\mathbb{Q}$, and which extends and pulls together many of the results we have developed here.
- If you like putting groups and linear algebra together (and why wouldn't you?), then you should consider learning some representation theory.
- There is also algebraic geometry, which is more closely tied to Math 5112, but it does tie into a lot of the material on function fields and transcendental extensions.

Summary

We discussed solvability of polynomials in radicals and the associated class of radical extensions.

We established some properties of solvable groups.

We proved that A_n is simple for $n \geq 5$.

We proved the Abel-Ruffini theorem on the insolvability of the quintic.

We proved the fundamental theorem of algebra, using algebra.

Next lecture: Math 5112.