Algebra Notes

Nov. 25: Solvable groups

Geoffrey Scott

Notation: One of you mentioned last class that your MAT301 professor used the notation $H \leq G$ to denote that H is a subgroup of G. I'll try to start using this notation too.

The fundamental theorem of Galois theory gives us the understanding about Galois groups that we need to start proving things about solvability of quintics. Recall that we were able to show that certain geometric constructions are impossible by translating facts about geometric constructions into facts about degrees of field extensions. Similarly, we can also translate facts about "having roots that can be expressed just in terms of rational numbers and symbols $\sqrt[n]{\ }$" into facts about Galois groups. To study this problem, we need to define rigorously the concept of "having roots that can be expressed in terms of rational numbers and $\sqrt[n]{\ }$."

Solvability

Definition: Let F be a field. A polynomial $f(x) \in F[x]$ is **solvable by radicals over** F if it splits in some extension field of the form $F(a_1, \ldots, a_n)$, where the elements a_i have the property that there are positive integers $k_1, \ldots, k_n$ such that

$$\begin{aligned} a_1^{k_1} &\in F \\ a_2^{k_2} &\in F(a_1) \\ a_3^{k_3} &\in F(a_1, a_2) \\ &\vdots \\ a_n^{k_n} &\in F(a_1, a_2, \ldots, a_{n-1}) \end{aligned}$$

Soon, we will prove that whenever a polynomial is solvable by radicals, the Galois group of its splitting field must be a *solvable* group.

Definition: A group G is **solvable** if there are subgroups $H_0, H_1, \ldots, H_n$ such that

$$\{\mathrm{id}\} = H_0 \leq H_1 \leq H_2 \leq \cdots \leq H_n = G$$

with the property that each H_i is normal in H_{i+1}, and H_{i+1}/H_i is abelian.

Examples: Every abelian group G is solvable (just take $H_0 = \{\mathrm{id}\}$ and $H_1 = G$). The fact that S_3 is solvable follows from the sequence of subgroups

$$\{\mathrm{id}\} \leq A_3 \leq S_3$$

The fact that D_4 is solvable follows from the sequence of subgroups

$$\{\mathrm{id}\} \leq H_1 \leq D_4$$

where H_1 is the subgroup of symmetries of a square that are orientation preserving (i.e. the rotations).

To prepare for the proof (on Monday) that when a polynomial is solvable by radicals, its splitting field has a solvable Galois group, we need to study certain properties of solvable groups.

Properties of Solvable Groups

Proposition: Let N be a normal subgroup of a group G. If G is solvable, then G/N is solvable.

Proof: Because G is solvable, there are subgroups

$$\{\mathrm{id}\} = H_0 \leq H_1 \leq \cdots \leq H_n = G$$

such that H_i is normal in H_{i+1} and H_{i+1}/H_i is abelian. Let $\varphi : G \to G/N$ be the quotient homomorphism. We will verify that the sequence of subgroups

$$\{\mathrm{id}\} = \varphi(H_0) \leq \varphi(H_1) \leq \cdots \leq \varphi(H_n) = G/N$$

satisfies the conditions needed to prove that G/N is solvable.

$\varphi(H_i)$ is normal in $\varphi(H_{i+1})$: Let $y \in \varphi(H_i)$ and $x \in \varphi(H_{i+1})$, so $y = \varphi(\tilde{y})$ and $x = \varphi(\tilde{x})$ for some $\tilde{y} \in H_i$ and $\tilde{x} \in H_{i+1}$. Then

$$xyx^{-1} = \varphi(\tilde{x})\varphi(\tilde{y})\varphi(\tilde{x})^{-1} = \varphi(\tilde{x}\tilde{y}\tilde{x}^{-1}).$$

Because H_i is normal in H_{i+1}, it follows that $\tilde{x}\tilde{y}\tilde{x}^{-1} \in H_i$. This means that $xyx^{-1} \in \varphi(H_i)$, so $\varphi(H_i)$ is normal in $\varphi(H_{i+1})$.

$\varphi(H_{i+1})/\varphi(H_i)$ is abelian: Consider the homomorphism

$$H_{i+1} \to \varphi(H_{i+1})/\varphi(H_i)$$

obtained by following φ with the quotient homomorphism $\varphi(H_{i+1}) \to \varphi(H_{i+1})/\varphi(H_i)$. This is a surjective homomorphism whose kernel contains H_i, so it defines a homomorphism $H_{i+1}/H_i \to \varphi(H_{i+1})/\varphi(H_i)$. By the first isomorphism theory of group theory, $\varphi(H_{i+1})/\varphi(H_i)$ is the quotient of an abelian group, hence is itself abelian.

Proposition: Let N be a normal subgroup of a group G. If N and G/N are solvable, then G is solvable.

Proof: Let

$$\{\mathrm{id}\} = H_0 \leq H_1 \leq \cdots \leq H_n = N \text{ and}$$
$$\{\mathrm{id}\} = J_0 \leq J_1 \leq \cdots \leq J_k = G/N$$

be sequences of subgroups showing that N and G/N are solvable. To find such a sequence of subgroups of G, let $\varphi : G \to G/N$ be the quotient homomorphism and consider the sequence.

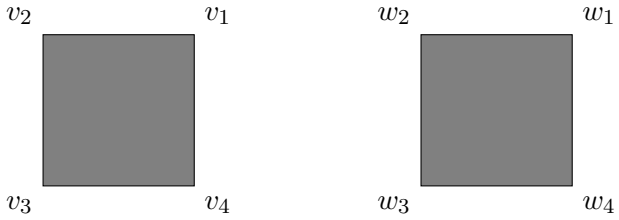
$$\{\mathrm{id}\} = H_0 \leq H_1 \leq \cdots \leq H_n = N = \varphi^{-1}(J_0) \leq \varphi^{-1}(J_1) \leq \cdots \leq \varphi^{-1}(J_k) = G$$

The fact that the solvability conditions are satisfied for the H_i subgroups follows from the fact that they arise from the sequence of subgroups that shows N is solvable.

To show that the solvability criteria are satisfied for the $\varphi^{-1}(J_i)$, consider the surjective homomorphism $\varphi^{-1}(J_{i+1}) \to J_{i+1}/J_i$ given by following φ by the quotient homomorphism. Its kernel is $\varphi^{-1}(J_i)$, so $\varphi^{-1}(J_i)$ must be normal, and the image is J_{i+1}/J_i, so by the first isomorphism theorem of Group theory, $\varphi^{-1}(J_{i+1})/\varphi^{-1}(J_i) \cong J_{i+1}/J_i$ which is abelian.

Example

We showed last time that the dihedral group D_4 is solvable. What about the subgroup of the symmetries of *two* squares?



To be precise, by "symmetry of two squares", I mean any permutation σ of the 8 verticies above such that drawing the lines

$$\sigma(v_1) - \sigma(v_2) - \sigma(v_3) - \sigma(v_4) - \sigma(v_1) \quad \text{and} \quad \sigma(w_1) - \sigma(w_2) - \sigma(w_3) - \sigma(w_4) - \sigma(w_1)$$

still makes the two squares in the figure above. Let G be this group of symmetries, H be the subgroup of G consisting of the symmetries that don't exchange the two squares, and let K be the subgroup of H that consists the symmetries that fix every one of the w verticies. Clearly, $K \cong D_4$, and $H \cong D_4 \oplus D_4$. We have the sequence of subgroups $K \leq H \leq G$. $K \cong D_4$ is solvable, and $H/K \cong D_4$ is also solvable, so $H \cong D_4 \oplus D_4$ is solvable. Similarly, since H is solvable and $G/H \cong \mathbb{Z}_2$ is solvable, then G is solvable.

Solvable Galois Groups

Proposition: Let F be any subfield of $\mathbb{C}$, and n be a positive integer, and E be the splitting field for $x^n - 1$ over F. Then $\mathrm{Gal}(E/F)$ is abelian.

Proof: Let $\varphi, \psi \in \mathrm{Gal}(E/F)$. We will prove the claim by verifying that $\varphi\psi = \psi\varphi$.

Let $\xi = e^{\frac{2\pi i}{n}}$. The roots of $x^n - 1$ are $\{1, \xi, \xi^2, \ldots, \xi^{n-1}\}$, and $E = F(\xi)$. Any F-automorphism is determined by its image of ξ, and each F-automorphism sends ξ to a power of ξ. Suppose $\varphi(\xi) = \xi^a$ and $\psi(\xi) = \xi^b$. Then

$$\psi\varphi(\xi) = \psi(\xi^a) = \psi(\xi)^a = \xi^{ab} \text{ and}$$
$$\varphi\psi(\xi) = \varphi(\xi^b) = \varphi(\xi)^b = \xi^{ab}$$

so $\psi\varphi(\xi) = \varphi\psi(\xi)$. Since any F-automorphism is determined by where it sends ξ, this proves that $\psi\varphi = \varphi\psi$, so $\mathrm{Gal}(E/F)$ is abelian.

Proposition: Let F be any subfield of $\mathbb{C}$, n be a positive integer, $c \in \mathbb{R}$, and let E be the splitting field for $x^n - c$ over F. The Galois group $\mathrm{Gal}(E/F)$ is solvable.

Proof: Let $\xi = e^{\frac{2\pi i}{n}}$, so the splitting field E for $x^n - c$ over F is given by $E = F(\xi, \sqrt[n]{c})$. By the fundamental theorem of Galois theory, the field extensions $F \subseteq F(\xi) \subseteq E = F(\xi, \sqrt[n]{c})$ correspond to the subgroups

$$\{\mathrm{id}\} \leq \mathrm{Gal}(E/F(\xi)) \leq \mathrm{Gal}(E/F)$$

Because $F(\xi)$ is the splitting field for $x^n - 1$ over F, it follows that $\mathrm{Gal}(E/F(\xi))$ is a normal subgroup of $\mathrm{Gal}(E/F)$ and that $\mathrm{Gal}(E/F)/\mathrm{Gal}(E/F(\xi)) \cong \mathrm{Gal}(F(\xi)/F)$, which is abelian by the previous proposition.

It remains only to show that $\mathrm{Gal}(E/F(\xi))$ is abelian. To show this, note that the zeros of $x^n - c$ are $\{\sqrt[n]{c}, \sqrt[n]{c}\xi, \ldots, \sqrt[n]{c}\xi^{n-1}\}$, so $E = F(\xi)(\sqrt[n]{c})$, and every $F(\xi)$-automorphism of E is determined by which zero of $x^n - c$ it sends $\sqrt[n]{c}$.

Let $\varphi, \psi \in \mathrm{Gal}(E/F(\xi))$. Then, $\varphi(\sqrt[n]{c}) = \sqrt[n]{c}\xi^a$ and $\psi(\sqrt[n]{c}) = \sqrt[n]{c}\xi^b$ for some a and b. Then,

$$\psi\varphi(\sqrt[n]{c}) = \psi(\sqrt[n]{c}\xi^a) = \psi(\sqrt[n]{c})\xi^a = \sqrt[n]{c}\xi^{a+b} \text{ and}$$
$$\varphi\psi(\sqrt[n]{c}) = \varphi(\sqrt[n]{c}\xi^b) = \varphi(\sqrt[n]{c})\xi^b = \sqrt[n]{c}\xi^{a+b}.$$

Because $\psi\varphi$ and $\varphi\psi$ send $\sqrt[n]{c}$ to the same element, $\psi\varphi = \varphi\psi$. This shows that $\mathrm{Gal}(E/F(\xi))$ is abelian.