GRADUATE ALGEBRA LECTURE NOTES

JOSH SWANSON

(These were adapted from Julia Pevtsova's lecture notes. They were given in Math 504 at the University of Washington on December 9th, 2015.)

Outline:

(1) Prove Fundamental Theorem of Galois Theory (FTGT)
(2) Application: $\mathbb{C} = \overline{\mathbb{R}}$
(3) Inverse Galois problem

Theorem 1. *Let K/k be a finite Galois extension. There is a bijection*

$$\{\textit{sub-extensions } K/F/k\} \overset{\sim}{\leftrightarrow} \{\textit{subgroups } 1 \leq H \leq G\}$$
$$F \overset{\Phi}{\mapsto} \mathrm{Gal}(K/F)$$
$$K^H \overset{\Psi}{\longmapsto} H$$

called the Galois correspondence.

Proof. Last time, showed

Lemma 2. $K^{\mathrm{Gal}(K/k)} = k$

Since K/F is Galois, lemma says $K^{\mathrm{Gal}(K/F)} = F$, i.e. $\Psi \circ \Phi = \mathrm{id}$.

Last time, stated

Theorem 3 (Artin)**.** *K a field, $G \leq \mathrm{Aut}(K)$ (ring aut's), $k := K^G$, $n := |G| < \infty$. Then*

(1) K/k is Galois of degree n
(2) $\mathrm{Gal}(K/k) = G$.

Proof. Last time, stated

Lemma 4. *Let K/k be algebraic, separable. Suppose for all $\alpha \in K$ there exists $f \in K[x]$ such that $\deg f \leq n$ and $f(\alpha) = 0$. Then $[K : k] \leq n$.*

Proof. Suppose not, so since K/k is algebraic, there exists some finite sub-extension $k \subset F \subset K$ such that $n < [F : k] < \infty$. Now F/k is separable, so $F = k(\alpha)$. But $[F : k] = \deg \mathrm{Irr}(\alpha, k) \leq n < [F : k]$, a contradiction. □

Returning to Artin's theorem, we have

Claim 5. *For any $\alpha \in K$, there is some $f \in k[x]$ such that*

(1) $f(\alpha) = 0$
(2) $\deg f \leq n$
(3) f splits in K

Date: December 9, 2015.

(4) f has distinct roots

Assuming the claim, by the (2) and the lemma, $[K : k] \leq n$. Also K/k is separable (4) and normal (3) so Galois. Now $G \leq \mathrm{Gal}(K/k)$, so

$$n = |G| \leq |\mathrm{Gal}(K/k)| = [K : k] \leq n,$$

hence $G = \mathrm{Gal}(K/k)$, which completes Artin's theorem. To wrap up the claim:

Proof (of claim). G acts on K, hence it also acts on the orbit $G \cdot \alpha = \{\sigma(\alpha) : \sigma \in G\} =: X$, so G acts on X by permutations. Now set $f(x) := \prod_{\beta \in X}(x - \beta)$. Since G permutes X, it permutes f, so it fixes f. Then $f(x) \in K^G[x] = k[x]$ and (1)-(4) are clear. □

□

Artin's theorem says $\mathrm{Gal}(K/K^G) = G$, so $\mathrm{Gal}(K/K^H) = H$, i.e. $\Phi \circ \Psi = \mathrm{id}$, completing the Galois correspondence proof. □

Remark 6. Constrast FTGT with the lattice isomorphism theorem, say for groups: $G \overset{\pi}{\twoheadrightarrow} G/K$ induces

$$\begin{aligned} \{H : K \leq H \leq G\} &\overset{\sim}{\leftrightarrow} \{S : S \leq G/K\} \\ H &\mapsto H/K \\ \pi^{-1}(S) &\hookleftarrow S \end{aligned}$$

This preserves lots more structure as well, e.g. $H \trianglelefteq G \Leftrightarrow H/K \trianglelefteq G/K$. The Galois correspondence does too:

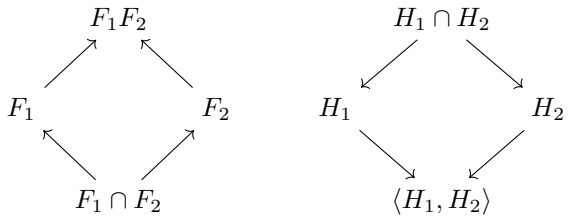
Theorem 7. *Suppose K/k is a Galois extension. Let F, F_1, F_2 be subfields corresponding to subgroups H, H_1, H_2 of $\mathrm{Gal}(K/k)$, respectively.*

(a) $F_1 \subset F_2 \Leftrightarrow H_1 \supset H_2$
(b) $F_1 F_2 \leftrightarrow H_1 \cap H_2$
(c) $F_1 \cap F_2 \leftrightarrow \langle H_1, H_2 \rangle$
(d) $[K : F] = |H|$, $[F : k] = [G : H]$.
(e) F/k *is normal if and only if* $H \trianglelefteq G$. *In that case* $\mathrm{Gal}(F/k) \cong G/H$.

Diagramatically,

$$\begin{array}{ccc} K & & 1 \\ {\scriptstyle |H|}\uparrow & & \downarrow \\ F & & H \\ {\scriptstyle [G:H]}\uparrow & & \downarrow \\ k & & G \end{array}$$

and



Proof. For (a), $H_1 \leq H_2$ says $K^{H_1} \supset K^{H_2}$ since being fixed under H_2 is more restrictive than being fixed under H_1. For (b) and (c), everything can be described in terms of the partial orders. For instance, $F_1 \cap F_2$ is the unique largest subfield contained in both F_1 and F_2. (b) and (c) then follow formally from (a). (d) is obvious.

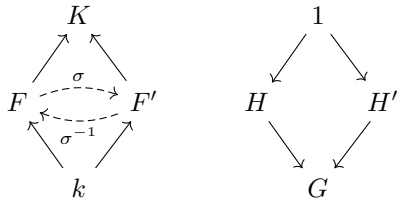
We turn to (e). For ($\Rightarrow$), if F/k is normal, we claim there is a short exact sequence

$$\begin{array}{ccccccccc} & & H & & G & & & & \\ & & \| & & \| & & & & \\ 1 & \longrightarrow & \mathrm{Gal}(K/F) & \hookrightarrow & \mathrm{Gal}(K/k) & \xrightarrow{\pi} & \mathrm{Gal}(F/k) & \longrightarrow & 1 \end{array}$$

which gives $H \trianglelefteq G$ and $\mathrm{Gal}(F/k) \cong G/H$. The inclusion is trivially an injection. Define $\pi(\sigma) := \sigma|_F$. Check:

- π well-defined: by normality, $\sigma|_F \colon F \to K$ is actually $\sigma|_F \colon F \to F$.
- Exactness at G: $\ker \pi = \{\sigma : \sigma|_F = \mathrm{id}\} = \mathrm{Gal}(K/F)$.
- Exactness at $\mathrm{Gal}(F/k)$: for $\tau \in \mathrm{Gal}(F/k)$, by the extension theorem again using normality there exists $\widetilde{\tau} \colon K \to K$ such that $\widetilde{\tau}|_F = \tau$, so π is surjective.

For ($\Leftarrow$), suppose F/k were not normal. Then there is some $\tau \colon F \to \overline{k}$ with $\tau(F) \neq F$. Extend this to $\sigma \colon K \to \overline{K} = \overline{k}$. Since K/k is normal, $\sigma \in \mathrm{Gal}(K/k)$ with $\sigma|_F = \tau$. Now $\sigma(F) = \tau(F) \neq F$, so set $F' := \sigma(F)$. Use the Galois correspondence to get



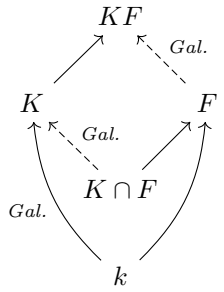
It is easy to see $\sigma H \sigma^{-1} = H'$—for instance, $\sigma H \sigma^{-1}$ fixes F'—but $F \neq F'$ says $H \neq H'$, so $H \not\trianglelefteq G$. □

We have an even stronger analogue of the second (diamond) isomorphism theorem:

Theorem 8. *Let K/k be Galois and let F/k be any field extension. Then $K/K \cap F$ and KF/F are Galois and*

$$\mathrm{Gal}(KF/F) \cong \mathrm{Gal}(K/K \cap F)$$
$$\sigma \overset{\phi}{\mapsto} \sigma|_K$$

Diagrammatically,



Proof. That $K/K \cap F$ is Galois is clear. To see that KF/F is Galois, note that K/k is the splitting field of some separable $f \in k[x]$. It's easy to check that KF/F is the splitting field of $f \in F[x]$ as well. For the isomorphism, check...

- Well-defined: $\sigma|_K \colon K \to KF$ gives $\sigma|_K \colon K \to K$ since $\sigma|_K$ fixes k and K/k is normal.
- Injective: $\sigma|_K = \mathrm{id}$ says $\sigma|_F$ and $\sigma|_K$ are id, so $\sigma|_{KF} = \mathrm{id}$
- Surjective: $\mathrm{im}\,\phi = \mathrm{Gal}(K/K \cap F)$ iff $K^{\mathrm{im}\,\phi} = K \cap F$. Pick $\alpha \in K$. Now
$$\begin{aligned} \alpha \in K^{\mathrm{im}\,\phi} &\Leftrightarrow \sigma|_K(\alpha) = \alpha, \forall \sigma \in \mathrm{Gal}(KF/F) \\ &\Leftrightarrow \alpha \in (KF)^{\mathrm{Gal}(KF/F)} = F, \end{aligned}$$
so indeed $K^{\mathrm{im}\,\phi} = K \cap F$.

□

Example 9. We apply the FTGT to show that $\mathbb{C}$ is algebraically closed using a classic, mostly algebraic proof. We use two facts:

Lemma 10. *We have*

(1) All $a + bi \in \mathbb{R}(i) =: \mathbb{C}$ have a square root.
(2) If $f \in \mathbb{R}[x]$ has odd degree, then f has a root in $\mathbb{R}$

Proof. For (1), set
$$c^2 := \frac{a + \sqrt{a^2 + b^2}}{2} \qquad d^2 := \frac{-a + \sqrt{a^2 + b^2}}{2}.$$
Then
$$(c + di)^2 = (c^2 - d^2) + (2cd)i = \cdots = a + bi.$$
(2) is an immediate consequence of the intermediate value theorem. □

As a corollary, $\mathbb{C}$ has no degree 2 extensions. Now, suppose $L/\mathbb{C}$ is a finite extension. Possibly extending L further, we may assume $L/\mathbb{R}$ is Galois. Letting H be a Sylow 2-subgroup (possibly $H = 1$) of $\mathrm{Gal}(L/\mathbb{R})$ gives:

$$\begin{array}{cc} L & 1 \\ {\scriptstyle |H|}\uparrow & \downarrow \\ L^H & H \\ {\scriptstyle |G|/|H| \text{ odd}}\uparrow & \downarrow \\ \mathbb{R} & G \end{array}$$

Now we have some β with $\mathbb{R}(\beta) = L^H$. Then $\mathrm{Irr}(\beta, \mathbb{R})$ has odd degree and is irreducible, so from (2) it must be linear, so $G = H$ is a 2-group and $[L : \mathbb{C}]$ is a power of 2. If $[L : \mathbb{C}] > 1$, then $\mathrm{Gal}(L/\mathbb{C})$ has an index 2 subgroup, so $L/\mathbb{C}$ has a degree 2 extension, contrary to the corollary.

Remark 11. We end with a few brief remarks on the inverse Galois problem. First, some motivation:

Theorem 12. *For all finite G, there exists L/F Galois such that* $\mathrm{Gal}(L/F) = G$.

Proof. Start with the $G = S_n$ case. Let
$$\begin{aligned} K &:= F(x_1, \ldots, x_n) = \mathrm{Frac}(F[x_1, \ldots, x_n]) \\ L &:= K(e_1, \ldots, e_n) = \mathrm{Frac}(F[e_1, \ldots, e_n]) \end{aligned}$$
where e_i is the degree i elementary symmetric polynomial in $x_1, \ldots, x_n$. Let S_n act on K by permuting the x_i. By homework,
$$F[x_1, \ldots, x_n]^{S_n} = F[e_1, \ldots, e_n],$$

so

$$F(x_1, \ldots, x_n)^{S_n} = F(e_1, \ldots, e_n)$$

(formal verification/exercise) and $\mathrm{Gal}(K/L) = S_n$ by our Artin's theorem. By the Galois correspondence, subextensions of K/L give rise to all subgroups of S_n, which covers all finite G as n varies. □

Hence it's relatively easy to get an arbitrary Galois group, especially if we allow the bottom field to vary. However...

Conjecture 13. *For any finite group G, there exists $L/\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) \cong G$.*

Some known cases:

- True for cyclic groups and generally abelian groups (classical)
- True for S_n and A_n (Hilbert)
- True for solvable groups (Shaferevich)
- True for groups of odd order (these are solvable by Feit-Thompson)
- True for all sporadic simple groups except possibly M_{23} (according to Noam Elkies on MO as of two years ago)