Galois continued

<u>Recall</u>: The Galois group of $K \subseteq F$ is

$$\mathrm{Aut}_K F = \{\varphi : F \to F \mid \varphi(k) = k \ \forall k \in K\}.$$

We ended with:

<u>Theorem</u>: Suppose $K \subseteq F$ are fields, and $f \in K[x]$. Then if u is a root of f and $\sigma \in \mathrm{Aut}_K F$, then $\sigma(u)$ is also a root of f.

As a consequence, suppose that u is a root of $f(x) \in K[x]$ and $F = K(u)$. Suppose that $\sigma \in \mathrm{Aut}_K F$ and $\sigma(u) = v$. <u>Then the lone equation $\sigma(u) = v$ completely determines $\sigma : F \to F$.</u> This is because $\sigma : F \to F$ is a map of vector spaces, and a basis for F is $\{1, u, u^2, \ldots, u^{n-1}\}$, and the action of σ on this basis is determined by $\sigma(u) = v$.

Since $\deg f = m$ implies f can have at most m distinct roots in F, this means

$$|\mathrm{Aut}_K K(u)| \leq m$$

in fact $|\mathrm{Aut}_K K(u)| \leq n$, where n is the number of distinct roots of f.

Example: If $F = K$, then $\mathrm{Aut}_K F = \{id\}$.
However $\mathrm{Aut}_K F = \{id\}$ does not imply $K = F$. For example, suppose u is the real cube root of 2. Then $\mathrm{Aut}_{\mathbb{Q}} \mathbb{Q}(u)$ contains automorphisms $\sigma : \mathbb{Q}(u) \to \mathbb{Q}(u)$ which permute the roots of $x^3 - 2$. But $\mathbb{Q}(u) \subseteq \mathbb{R}$, and the only roots of $x^3 - 2$ aside from u are complex. Thus ~~and~~ any $\sigma \in \mathrm{Aut}_{\mathbb{Q}} \mathbb{Q}(u)$ must satisfy $\sigma(u) = u$ and thus ~~be~~ the identity (since a basis for $\mathbb{Q}(u)$ over $\mathbb{Q}$ is $\{1, u, u^2\}$). So $\mathrm{Aut}_{\mathbb{Q}} \mathbb{Q}(u) = \{id\}$.

Example: Let i denote a root of x^2+1, so that its two roots are $\pm i$. Set $\mathbb{C} = \mathbb{R}(i)$. Then $\mathrm{Aut}_{\mathbb{R}} \mathbb{C}$ has order at most two, since x^2+1 has two distinct roots.
There is a non-identity element of $\mathrm{Aut}_{\mathbb{R}} \mathbb{C}$ given by

$$a+ib \longmapsto a-ib \quad \text{(complex conjugation)}$$

so $|\mathrm{Aut}_{\mathbb{R}} \mathbb{C}| = 2$ and $\mathrm{Aut}_{\mathbb{R}} \mathbb{C} \simeq \mathbb{Z}_2$.

Example: Set $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $K = \mathbb{Q}$. Then one can check that $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$, so any $\sigma \in \mathrm{Aut}_K F$ is determined by the two values $\sigma(\sqrt{2})$ and $\sigma(\sqrt{3})$.
But $\sigma(\sqrt{2}) = \pm\sqrt{2}$ (roots of x^2-2)
and $\sigma(\sqrt{3}) = \pm\sqrt{3}$ (roots of x^2-3).

Thus there are only 4 possibilities for σ. In fact, one can check that all possibilities are valid and that all give distinct automorphisms of order two. Thus $|\mathrm{Aut}_K F| = 4$, all elements of order 2

$$\Rightarrow \mathrm{Aut}_K F = \mathbb{Z}_2 \times \mathbb{Z}_2 .$$

Remarks: • Given any finite group G, there exists an extension $K \subseteq F$ with $\mathrm{Aut}_K F = G$.

• Open question: Fix a specific field K, say $K = \mathbb{Q}$. Which groups can arise from fixing the smaller field?

Idea of Galois theory: We will establish some sort of correspondence:

$$\left\{ \begin{matrix} \text{fields } E \text{ with} \\ K \subseteq E \subseteq F \end{matrix} \right\} \overset{?}{\Longleftrightarrow} \left\{ \begin{matrix} \text{subgroups of} \\ \mathrm{Aut}_K F \end{matrix} \right\},$$

eventually specializing to the case $[F : K] < \infty$. For now we keep it general, and have:

Theorem: Let F be an extension field of K, E an intermediate field and $H \leq \mathrm{Aut}_K F$. Then

(a) $H' = \{ h \in F \mid \sigma(h) = h \ \forall \sigma \in \mathrm{Aut}_K F \}$ is a subfield of F, and

(b) $E' = \{ \sigma \in \mathrm{Aut}_K F \mid \sigma(e) = e \ \forall e \in E \}$ is a subgroup of $\mathrm{Aut}_K F$. (it is $\mathrm{Aut}_E F$).

<u>Proof</u>: Easy exercise.

So we have a natural "first correspondence":

- Subgroups give fields by looking at the elements they fix
- Fields give subgroups by looking at the automorphisms that fix them.

<u>Definition</u>: The field H' in the Theorem above is the <u>fixed field</u> of $H \leq \mathrm{Aut}_K F$.

We shall also use the "prime notation" on fields, ie

$$\mathrm{Aut}_E F \subset \mathrm{Aut}_K F \quad \text{will be written } E' \subset \mathrm{Aut}_K F.$$

This notation then gives

$$\mathrm{Aut}_K F = K' \; \cancel{\{id\}} \quad \text{and} \quad F' = \{id\}.$$

On the other hand,

$$\{id\}' = \cancel{K} F \quad \text{with} \quad (\mathrm{Aut}_K F)' = ??$$

One might hope that $(\mathrm{Aut}_K F)' = K$, so that everything aside from K is moved by at least one automorphism. But this is not the case: We already saw

$$\mathrm{Aut}_{\mathbb{Q}} \mathbb{Q}(u) = \{id\} \quad \text{when } u \in \mathbb{R} \text{ is a root of } x^3 - 2,$$

so $(\mathrm{Aut}_{\mathbb{Q}} \mathbb{Q}(u))' = \mathbb{Q}(u)$ in that case.

So in general, $(\mathrm{Aut}_K F)'$ is some field E with $K \subseteq E \subseteq F$. $\mathrm{Aut}_K F = \{id\}$ is the special case $E = F$, the other special case $(E = K)$ gets a name:

<u>Definition</u>: Let $K \subseteq F$ be fields. If $(\mathrm{Aut}_K F)' = K$ then F is said to be a <u>Galois extension of K</u> or is called <u>Galois over K</u>.

<u>Example</u>: We can easily check that $\mathbb{C}$ is Galois over $\mathbb{R}$, since $\mathrm{Aut}_{\mathbb{R}} \mathbb{C} = \mathbb{Z}_2$ and $a+ib \longmapsto a+ib$ moves every element in $\mathbb{C} \setminus \mathbb{R}$. So $(\mathrm{Aut}_{\mathbb{R}} \mathbb{C})' = \mathbb{R}$.

We now have all of the information and terminology needed to state the fundamental theorem of Galois theory:

<u>Theorem</u>: Suppose $K \subseteq F$ are fields and $[F:K] < \infty$. If F is Galois over K then there is a correspondence

$$\left\{ \begin{array}{c} \text{fields } E \text{ with} \\ K \subseteq E \subseteq F \end{array} \right\} \Longleftrightarrow \left\{ \begin{array}{c} \text{subgroups of} \\ \mathrm{Aut}_K F \end{array} \right\}$$

given by $E \longmapsto E' = \mathrm{Aut}_E F$

such that

(i) For any two intermediate fields L, M with $K \subseteq L \subseteq M \subseteq F$ we have

$$[M:L] = |L' : M'|$$

field dimension

group index

in particular $L \subseteq M \Rightarrow M' \subseteq L'$ and

$$|\mathrm{Aut}_K F| = |\mathrm{Aut}_K F : \{id\}| = [F:K].$$

(ii) F is Galois over every intermediate field E, but E is Galois over K if and only if E' is normal in $\mathrm{Aut}_K F$. In this case

$$\mathrm{Aut}_K F / E' = \mathrm{Aut}_K F / \mathrm{Aut}_E F \cong \mathrm{Aut}_K E.$$

The fundamental theorem of Galois theory is "order-reversing": If

$$K \subset L \subset M \subset F \quad \text{(fields) then}$$

$$\underset{\mathrm{Aut}_K F}{\overset{\shortparallel}{K'}} > L' > M' > \underset{\{id\}}{\overset{\shortparallel}{F'}}$$

and vice versa: Given

$$\{id\} < H < J < \mathrm{Aut}_K F, \text{ then}$$

$$\underset{F}{\overset{\shortparallel}{\{id\}'}} \supset H' \supset J' \supset \underset{K}{\overset{\shortparallel}{(\mathrm{Aut}_K F)'}}.$$

The "priming operations" outlined last class obey the following properties:

<u>Lemma</u>: Suppose $K \subseteq L \subseteq M \subseteq F$ are fields and $\{id\} \subset H, J \subset \mathrm{Aut}_K F = G$ are groups. Then:

(i) $F' = \{id\}$ and $K' = G$

(ii) $\{id\}' = F$

(iii) $L \subseteq M \Rightarrow M' < L'$, and $H < J \Rightarrow J' \subseteq H'$

(iv) $L \subset L''$ and $H < H''$

(v) $L' = L'''$ and $H' = H'''$

<u>Sketch</u>: (i)–(iii) are definitions (or follow in one line from definitions)

To prove (iv), it is only a matter of unpacking the meaning of a double prime. To prove (v), note that $L \subset L'' \Longrightarrow L''' \subset L'$, by applying (iii) and (iv) together. On the other hand, if we use the fact $H < H''$ with L' in place of H, then we get $L' \subset L'''$. Thus $L''' = L'$.

We argue similarly that $H' = H'''$.

<u>Remark</u>: • The containments $L \subset L''$ or $H < H''$ can easily be proper.

- Since F is Galois over K if $(\mathrm{Aut}_K F)' = K$ and $K' = \mathrm{Aut}_K F$, we get that F is Galois over K if and only if $\underset{\underset{(K')' = K''}{\parallel}}{(\mathrm{Aut}_K F)'} = K$, ie $K = K''$.
- By the same reasoning, if $K \subset E \subset F$ then F is Galois over E if and only if $E'' = E$.

<u>Definition</u>: If X is a field with $K \subset X \subset F$ or if X is a subgroup with $\{id\} \subset X \subset \mathrm{Aut}_K F$, then X will be called <u>closed</u> if $X = X''$.

Theorem: If $K \subseteq F$ are fields, then there is a correspondence

$$\left\{ \begin{array}{c} \text{closed fields } E \\ K \subset E \subset F \end{array} \right\} \Longleftrightarrow \left\{ \begin{array}{c} \text{closed subgroups } H \\ \{id\} < H < \mathrm{Aut}_K F \end{array} \right\}$$

Given by $E \longmapsto E'$

which is one-to-one and onto.

Proof: It essentially follows from part (v) of the previous lemma:

Since $E' = E'''$ and $H' = H'''$, all primed objects are closed. Thus we only need to check that $H \longmapsto H'$ provides an inverse to $E \longmapsto E'$, at which point we can be certain that the correspondence is 1-1 and onto.

Begin our technical lemmas.

We will eventually show that in an algebraic Galois extension, all intermediate fields are closed.

When $[F:K] < \infty$, all subgroups of $\mathrm{Aut}_K F$ are closed, too.

Lemma 2.8: Suppose $K \subset L \subseteq M \subset F$.

If $[M:L] < \infty$, then $|L' : M'| \leq [M:L]$. In particular, if $[F:K] < \infty$ then

$$|K' : F'| = |\mathrm{Aut}_K F : \{id\}| = |\mathrm{Aut}_K F| \leq [F:K].$$

<u>Proof</u>: First suppose $[M:L]=1$. Then $M=L$ and $L'=M'$ so $|L':M'| = [M:L]$, so we have a base case for an induction.

Now suppose the claim holds for $[M:L]<n$, and consider $=n$. Choose $u \in M \setminus L$. Since $[M:L]<\infty$, u is algebraic over L with some minimal polynomial $f(x) \in L[x]$ with $\deg f = k > 1$. Then $[L(u):L]=k$ and since $[M:L]=n$, $[M:L(u)] = n/k$. I.e, we have:

$$\underbrace{\underbrace{L \subset L(u)}_{k} \underbrace{\subset M}_{n/k}}_{n}$$

and $L' \geq L(u)' \geq M'$, though we cannot yet say what the index of these subgroups in the larger group may be. To determine this, we consider cases:

<u>Case 1</u>: If $k<n$, then $1<n/k<n$ and the induction hypothesis applies to both $[M:L(u)]$ and $[L(u):L]$ giving $[M:L(u)] \Rightarrow |L(u)':M'| \leq n/k$ and $|L':L(u)'| \leq k$ so

$$|L':M'| = |L':L(u)'|\,|L(u)':M'| \leq k\left(\tfrac{n}{k}\right) = n\text{; done.}$$

<u>Case 2</u>: If $k=n$, then $[M:L(u)]=1$ and $M=L(u)$.

This case requires <u>work</u>. Set

$S = \{\tau M' \mid \tau \in L'\}$, ie it's all left cosets of $M' \leq L'$.

and $T = \{\text{roots of } f(x) \text{ in } F\}$.

Construct an injective map $\psi : S \longrightarrow T$ as follows: (Completing this construction gives $|S| \leq |T|$, but $|S| = |L' : M'|$ by definition and $|T| \leq n$ gives $|L' : M'| \leq n = [M : L]$, finishing the proof).

Let $\tau M'$ be a left coset. Define ψ by

$$\psi(\tau M') = \tau(u).$$

First note that this map makes sense: Given $\tau \in L' = \mathrm{Aut}_L F$, we know τ permutes the roots of $f(x)$, so $\tau(u)$ is indeed a root of f. Next, suppose $\tau M' = \tau' M'$. Then $\tau = \tau' \sigma$ for some $\sigma \in M'$. Since $u \in M$, $\sigma(u) = u$ and therefore

$$\psi(\tau M') = \tau(u) = \tau' \sigma(u) = \tau'(u) = \psi(\tau' M'),$$

so ψ is well-defined.

Last, suppose $\psi(\tau M') = \psi(\tau' M')$. Then $\tau(u) = \tau'(u) \Rightarrow \tau^{-1}\tau'(u) = u$, so $\tau^{-1}\tau'$ fixes u. But then since we are in the situation $L(u) = M$, this means $\tau^{-1}\tau' : M \longrightarrow M$ is the identity since it fixes the basis $\{1, u, \ldots, u^{n-1}\}$. Thus $\tau^{-1}\tau' \in \mathrm{Aut}_M F = M'$, so $\tau M' = \tau' M'$ and ψ is injective.

We have an analagous lemma relating priming to subgroups of the Galois group.

<u>Lemma 2.9</u>: Let F be an extension field of K and let H, J be subgroups of the group $\mathrm{Aut}_K F$, with $H < J$. Then if $[J:H] < \infty$, we have $[H':J'] \leq |J:H|$.

<u>Proof</u>: Suppose that $|J:H| = n$ and $[H':J'] > n$. Then we can choose

- $u_1, u_2, \ldots, u_{n+1} \in H'$ that are linearly independent over J'
- $\tau_1, \tau_2, \ldots, \tau_n$ a set of coset representatives of H in J.

And consider the following system of equations:

$$\begin{array}{ccccccc} \tau_1(u_1)x_1 & + & \tau_1(u_2)x_2 & + \cdots + & \tau_1(u_{n+1})x_{n+1} & = & 0 \\ \vdots & & \vdots & & \vdots & & \vdots \\ \tau_n(u_1)x_1 & + & \tau_n(u_2)x_2 & + \cdots + & \tau_n(u_{n+1})x_{n+1} & = & 0 \end{array}$$

Because this system has $n+1$ variables and n equations, there is a nontrivial solution, in fact there are potentially many solutions. Choose a solution

$$x_1 = a_1, \quad x_2 = a_2, \quad \ldots, \quad x_{n+1} = a_{n+1}$$

with a minimal number of nonzero a_i. We can, up to reindexing variables and scaling our solution (recall any scalar multiple of a solution is also a solution) assume that $a_1, \ldots, a_r$ are nonzero, $a_{r+1}, \ldots, a_{n+1}$ are zero, and $a_1 = 1$ (multiply by a_1^{-1} otherwise). Trick: we will find $\sigma \in J$ such that

$$\sigma a_1, \sigma a_2, \sigma a_3, \ldots, \sigma a_r, \sigma a_{r+1} = 0, \ldots, \sigma a_{n+1} = 0$$

is also a solution, with $\sigma a_2 \neq a_2$.

But then

$$a_1 - \sigma a_1, \; a_2 - \sigma a_2, \; \ldots, \; \text{etc}$$

is a solution to the system of equations as well, and since $a_1 - \sigma a_1 = 1 - 1 = 0$ and $a_2 - \sigma a_2 \neq 0$ we have a nontrivial solution with fewer nonzero entries, contradiction to our minimal choice.

So to finish the proof we need only find σ. Since $\tau_1, \ldots, \tau_n$ are coset reps of H in J, there's one τ_i that actually lies in H (a coset rep for $(id) \cdot H$)). Then this τ, because it's in H, must fix every element in H' by definition. So $\tau_i(u_j) = u_j \; \forall j = 1, \ldots, n+1$. Say $i = 1$ so it's τ_1 fixing all u_j. Then the first equation in the system is

$$u_1 x_1 + u_2 x_2 + \ldots + u_{n+1} x_{n+1} = 0.$$

Now since the a_i are a solution this means

$$\sum_{i=1}^{n+1} u_i a_i = 0$$

but the u_i are linearly independent over J', so at least one of the a_i must not be in J' — let's say $a_2 \notin J'$.

Since $a_2 \notin J'$, by definition there's $\sigma \in J$ with $\sigma(a_2) \neq a_2$. So now consider

$$\begin{aligned} &\sigma\tau_1(u_1)x_1 + \sigma\tau_1(u_2)x_2 + \dots + \sigma\tau_1(u_{n+1})x_{n+1} = 0 \\ &\vdots \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (*). \\ &\sigma\tau_n(u_1)x_1 + \dots + \sigma\tau_n(u_{n+1})x_{n+1} = 0, \end{aligned}$$

ie apply σ to the entire system we started with, and from this we also see that

$$\sigma a_1, \sigma a_2, \dots, \sigma a_{n+1}$$

is a solution to the new system above.

<u>Claim</u>: Although it looks different, aside from possibly re-ordering the equations, system $(*)$ is the same as the original. Thus, we'll find σ is the automorphism we need.

(i) First, note that since $\{\tau_1, \dots, \tau_n\}$ are coset representatives of H in J and $\sigma \in J$, then $\{\sigma\tau_1, \dots, \sigma\tau_n\}$ are a complete set of coset representatives, too.
(If not, say $\sigma\tau_i H = \sigma\tau_j H$, so $\sigma\tau_i = \sigma\tau_j\gamma$ for some $\gamma \in H$.
Then $\tau_i = \tau_j\gamma \Rightarrow \tau_i H = \tau_j H$, contradiction).

(ii) Also note that if $\gamma, \beta \in \tau_j H$ for some j, then $\gamma = \tau_j h$, $\beta = \tau_j h'$ for $h, h' \in H$ and so $\forall\, i = 1, \dots, n+1$

$$\gamma(u_i) = \tau_j h(u_i) = \tau_j(u_i) = \tau_j h'(u_i) = \beta(u_i)$$

Since $u_i \in H'$!