Math 562/662 **Spring 2024**
Sketch of Galois Theory **Drew Armstrong**

We did not have time in class to prove the Fundamental Theorem of Galois Theory. In this note I will sketch out the proof, assuming the Primitive Element Theorem, which you will prove on Homework 6. I will roughly follow the approach of Stillwell in his "Elements of Algebra". For simplicity we will only work with subfields of $\mathbb{C}$.

Primitive Element Theorem. Consider a field $\mathbb{F} \subseteq \mathbb{C}$. Then for any two elements $\alpha, \beta \in \mathbb{C}$ algebraic over $\mathbb{F}$ there exists a (non-unique) element $\gamma \in \mathbb{C}$ such that $\mathbb{F}(\alpha, \beta) = \mathbb{F}(\gamma)$.

It follows by induction that if $\mathbb{E} \supseteq \mathbb{F}$ is the splitting field for some polynomial $f(x) \in \mathbb{F}[x]$ then $\mathbb{E} = \mathbb{F}(\gamma)$ for some $\gamma \in \mathbb{E}$. The letter "γ" is for "Galois" since these elements used to be called "Galois resolvents". The exact nature of γ is not very interesting; just its existence.

Normal Field Extensions. Consider a field $\mathbb{F} \subseteq \mathbb{C}$ with $[\mathbb{F}/\mathbb{Q}] < \infty$. An *isomorphism of* $\mathbb{F}$ is any isomorphism $\sigma : \mathbb{F} \to \mathbb{F}'$ onto any other field $\mathbb{F}' \subseteq \mathbb{C}$. The number of isomorphisms of $\mathbb{F}$ equals $[\mathbb{F}/\mathbb{Q}]$. Proof: Write $\mathbb{F} = \mathbb{Q}(\gamma)$ and let $m(x) \in \mathbb{Q}[x]$ be the minimal polynomial of $\gamma/\mathbb{Q}$ so that $[\mathbb{F}/\mathbb{Q}] = \deg(m)$. Then for each root $\gamma' \in \mathbb{C}$ of $m(x)$ there exists a unique isomorphism

$$\mathbb{Q}(\gamma) \to \frac{\mathbb{Q}[x]}{m(x)} \to \mathbb{Q}(\gamma'),$$

and these are all of the isomorphisms of $\mathbb{F}$. QED. If $\gamma' \in \mathbb{F}$ then we have $\mathbb{Q}(\gamma) = \mathbb{Q}(\gamma')$ and the unique map sending $\gamma \to \gamma'$ is called an *automorphism of* $\mathbb{F}$. The field $\mathbb{F}$ is called *normal* when all of its isomorphisms are automorphisms. There is also a relative version. Given $\mathbb{C} \supseteq \mathbb{E} \supseteq \mathbb{F}$, the number of isomorphisms $\sigma : \mathbb{E} \to \mathbb{E}'$ that fix $\mathbb{F}$ is $[\mathbb{E}/\mathbb{F}]$ and we say that $\mathbb{E}$ *is normal over* $\mathbb{F}$ when every isomorphism of $\mathbb{E}$ over $\mathbb{F}$ is an automorphism. If $G = \text{Gal}(\mathbb{E}/\mathbb{F})$ then $\#G \leq [\mathbb{E}/\mathbb{F}]$, and $\#G = [\mathbb{E}/\mathbb{F}]$ if and only if $\mathbb{E} \supseteq \mathbb{F}$ is normal.

Splitting Fields. Given fields $\mathbb{C} \supseteq \mathbb{E} \supseteq \mathbb{F}$ with $[\mathbb{E}/\mathbb{F}] < \infty$ we have

$$\mathbb{E} \supseteq \mathbb{F} \text{ is normal} \quad \Longleftrightarrow \quad \mathbb{E} \text{ is a splitting field for some polynomial } f(x) \in \mathbb{F}[x].$$

Proof: Let $\mathbb{E} \supseteq \mathbb{F}$ be normal and write $\mathbb{E} = \mathbb{F}(\gamma)$. Let $m(x) \in \mathbb{F}[x]$ be the minimal polynomial of $\gamma/\mathbb{F}$. Then every root of $m(x)$ is in $\mathbb{E}$, hence $\mathbb{E}$ is the splitting field of $m(x)$. Conversely, let $\mathbb{E} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$ where $\alpha_1, \ldots, \alpha_n$ are the roots of some $f(x) \in \mathbb{F}[x]$. Then for any isomorphism $\sigma : \mathbb{E} \to \mathbb{E}'$ fixing $\mathbb{F}$ we see that $f(\sigma(\alpha_i)) = \sigma(f(\alpha_i)) = 0$, hence $\sigma(\alpha_i) = \alpha_j \in \mathbb{E}$. Hence σ sends $\mathbb{E}$ into itself. QED.

Extension Lemma. Let $\mathbb{E} \supseteq \mathbb{F}$ be finite with $\mathbb{E} \supseteq \mathbb{K} \supseteq \mathbb{F}$. Then any isomorphism $\tau : \mathbb{K} \to \mathbb{K}'$ that fixes $\mathbb{F}$ extends to an isomorphism $\sigma : \mathbb{E} \to \mathbb{E}'$ that fixes $\mathbb{F}$. If $\mathbb{E} \supseteq \mathbb{F}$ is normal then this σ is an automorphism. Proof: Write $\mathbb{E} = \mathbb{K}(\gamma)$ and let $m(x) \in \mathbb{K}[x]$ be the minimal polynomial of $\gamma/\mathbb{K}$. Then the polynomial $m^\tau(x) \in \mathbb{K}'[x]$ is also irreducible and has some root $\gamma' \in \mathbb{C}$. Hence we obtain an isomorphism

$$\sigma : \mathbb{E} = \mathbb{K}(\gamma) \to \frac{\mathbb{K}[x]}{m(x)} \to \frac{\mathbb{K}'[x]}{m^\tau(x)} \to \mathbb{K}'(\gamma') \subseteq \mathbb{C},$$

which restricts to τ on $\mathbb{K}$, and hence fixes $\mathbb{F}$. QED.

The Fundamental Theorem I. For any field extension $\mathbb{E} \supseteq \mathbb{F}$ let $G(\mathbb{E}/\mathbb{F})$ be the group of automorphisms $\sigma : \mathbb{E} \to \mathbb{E}$ fixing $\mathbb{F}$. For any intermediate field $\mathbb{E} \supseteq \mathbb{K} \supseteq \mathbb{F}$ we obtain a subgroup $G(\mathbb{E}/\mathbb{K}) \subseteq G(\mathbb{E}/\mathbb{F})$ and for any subgroup $H \subseteq G(\mathbb{E}/\mathbb{F})$ we obtain a subfield

$\text{Fix}(H) = \{\alpha \in \mathbb{E} : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}$. For empty reasons,[1] this gives an order-reversing bijection between the set of intermediate fields $\mathbb{K}$ satisfying $\text{Fix}(G(\mathbb{E}/\mathbb{K})) = \mathbb{K}$ and the set of subgroups H satisfying $H = G(\mathbb{E}/\text{Fix}(H))$. Theorem: Let $\mathbb{C} \supseteq \mathbb{E} \supseteq \mathbb{K}$ with $\mathbb{E} \supseteq \mathbb{F}$ **finite and normal**. Then we have

- $\text{Fix}(G(\mathbb{E}/\mathbb{K})) = \mathbb{K}$ for all $\mathbb{E} \supseteq \mathbb{K} \supseteq \mathbb{F}$,
- $H = G(\mathbb{E}/\text{Fix}(H))$ for all $H \subseteq G(\mathbb{E}/\mathbb{F})$.

Hence we obtain an order-reversing bijection between the poset of all fields between $\mathbb{E}$ and $\mathbb{F}$ and the poset of all subgroups of $G(\mathbb{E}/\mathbb{F})$. Proof: Consider any $\mathbb{E} \supseteq \mathbb{K} \supseteq \mathbb{F}$. For empty reasons we have $\mathbb{K} \subseteq \text{Fix}(G(\mathbb{E}/\mathbb{K}))$. Suppose for contradiction that there exists $\alpha \in \text{Fix}(G(\mathbb{E}/\mathbb{F}))$ with $\alpha \notin \mathbb{K}$. Let $m(x) \in \mathbb{F}[x]$ be the minimal polynomial of $\alpha/\mathbb{K}$. Since $[\mathbb{K}(\alpha)/\mathbb{K}] \geq 2$ there exists $\tau : \mathbb{K}(\alpha) \to \mathbb{K}(\alpha')$ fixing $\mathbb{K}$ and sending α to another root $\alpha' \neq \alpha$ of $m(x)$. Note that $\alpha' \in \mathbb{E}$ because $\mathbb{E}/\mathbb{K}$ is normal. Hence by the Extension Lemma there exists $\sigma \in G(\mathbb{E}/\mathbb{K})$ restricting to τ. But then since $\alpha \in \text{Fix}(G(\mathbb{E}/\mathbb{K}))$ and $\sigma \in G(\mathbb{E}/\mathbb{K})$ we must have $\alpha' = \sigma(\alpha) = \alpha$. Contradiction. Next consider any subgroup $H \subseteq G(\mathbb{E}/\mathbb{F})$ and write $H = \{\sigma_1, \ldots, \sigma_r\}$. For empty reasons we have $H \subseteq G(\mathbb{E}/\text{Fix}(H))$. Write $\mathbb{E} = \mathbb{F}(\alpha)$ and let $f(x) = \prod(x - \sigma_i(\alpha))$. Since H permutes the roots it fixes the coefficients, so $f(x) \in \text{Fix}(H)[x]$. Any $\sigma \in G(\mathbb{E}/\text{Fix}(G))$ sends α to another root of $f(x)$, so $\sigma(\alpha) = \sigma_i(\alpha)$ and hence $\sigma = \sigma_i$ as functions on $\mathbb{E} = \mathbb{F}(\alpha)$. It follows that $G(\mathbb{E}/\text{Fix}(H)) \subseteq H$. QED.

Say that $\mathbb{E} \supseteq \mathbb{F}$ is *Galois* when it satisfies the hypotheses of the Fundamental Theorem (i.e., with $[\mathbb{E}/\mathbb{F}] < \infty$ and $\mathbb{E} \supseteq \mathbb{F}$ normal).[2]

Conjugation. Let $\mathbb{E} \supseteq \mathbb{F}$ be Galois. Then for any $\mathbb{E} \supseteq \mathbb{K} \supseteq \mathbb{F}$ and $\sigma \in G(\mathbb{E}/\mathbb{F})$ we have

$$G(\mathbb{E}/\sigma(\mathbb{K})) = \sigma G(\mathbb{E}/\mathbb{K})\sigma^{-1}.$$

Proof: Easy. QED. If $\sigma G(\mathbb{E}/\mathbb{K})\sigma^{-1} = G(\mathbb{E}/\mathbb{K}')$ for some field $\mathbb{K}'$ it follows that $G(\mathbb{E}/\sigma(\mathbb{K})) = G(\mathbb{E}/\mathbb{K}')$ and hence $\sigma(\mathbb{K}) = \mathbb{K}'$ by applying Fix to both sides.

The Fundamental Theorem II. Let $\mathbb{E} \supseteq \mathbb{F}$ be Galois and let $\mathbb{E} \supseteq \mathbb{K} \supseteq \mathbb{F}$. Then $\mathbb{K} \supseteq \mathbb{F}$ is Galois if and only if $G(\mathbb{E}/\mathbb{K}) \subseteq G(\mathbb{E}/\mathbb{F})$ is a normal subgroup, in which case

$$\frac{G(\mathbb{E}/\mathbb{F})}{G(\mathbb{E}/\mathbb{K})} \cong G(\mathbb{K}/\mathbb{F}).$$

Proof: Write $G = G(\mathbb{E}/\mathbb{F})$ and $H = G(\mathbb{E}/\mathbb{K})$. If $H \subseteq G$ is normal then for all $\sigma \in G$ we have $\sigma H \sigma^{-1} = H$, which implies that $\sigma(\mathbb{K}) = \mathbb{K}$ by the previous result. On the other hand, let $\tau : \mathbb{K} \to \mathbb{K}'$ be any isomorphism fixing $\mathbb{F}$, which lifts to some isomorphism $\sigma : \mathbb{E} \to \mathbb{E}'$ fixing $\mathbb{F}$ by the Extension Lemma. Since $\mathbb{E} \supseteq \mathbb{F}$ is normal this implies that $\sigma \in G(\mathbb{E}/\mathbb{K})$ and hence $\tau(\mathbb{K}) = \sigma(\mathbb{K}) = \mathbb{K}$ so that τ is an automorphism. Hence $\mathbb{K} \supseteq \mathbb{F}$ is normal. Conversely, for any $\sigma : \mathbb{E} \to \mathbb{E}$ in G let $\sigma|_{\mathbb{K}} : \mathbb{K} \to \mathbb{E}$ be the restricted function. If $\mathbb{K} \supseteq \mathbb{F}$ is normal then $\sigma|_{\mathbb{K}} : \mathbb{K} \to \mathbb{K}$ and hence $\sigma|_{\mathbb{K}} \in G(\mathbb{K}/\mathbb{F})$. This shows that "restricting to $\mathbb{K}$" is a group homomorphism $G \to G(\mathbb{K}/\mathbb{F})$. And this homomorphism is surjective because any $\tau \in G(\mathbb{K}/\mathbb{F})$ extends to some $\sigma \in G$ by the Extension Lemma. Finally, since the kernel of the restriction map is clearly H, the First Isomorphism Theorem for Groups gives the result:

$$\frac{G}{H} = \frac{G}{\ker} \cong \text{im} = G(\mathbb{K}/\mathbb{F}).$$

[1] See the homework problem on "abstract Galois correspondences".

[2] In this note we restrict attention to subfields of $\mathbb{C}$. In general "Galois" is defined as "finite, normal and separable". Separability of $\mathbb{E} \supseteq \mathbb{F}$ means that for all $\alpha \in \mathbb{E}$ the minimal polynomial of $\alpha/\mathbb{F}$ has no repeated roots in any field extension. On the homework you showed that this holds for all fields of characteristic zero. Separability was needed in the proof of the Primitive Element Theorem.