Introduction to Analysis – MA 542 – Fall 2019 – R. Pollack
Galois theory

1 Field theory preliminaries

The following proposition will be key in the future to actually build automorphisms.

Proposition 1.1. *Let K/F be an algebraic field extension and let α and β in K be conjugate (i.e. α and β have the same minimum polynomial). Then there exists a unique isomorphism $F(\alpha) \cong F(\beta)$ which fixes F and maps α to β.*

Proof. If such an isomorphism exists, it must be unique as any map on $F(\alpha)$ is determined by what it does to F and what it does to α.

To see that the map exists, we use the fact that we have isomorphisms

$$F(\alpha) \xrightarrow{\varphi} F[x]/\langle \mathrm{irr}(\alpha, F)\rangle$$

and

$$F(\beta) \xrightarrow{\psi} F[x]/\langle \mathrm{irr}(\beta, F)\rangle$$

such that F is fixed and both α and β are sent to the equivalence class of x. But since $\mathrm{irr}(\alpha, F) = \mathrm{irr}(\beta, F)$, the map $\psi^{-1} \circ \varphi$ gives an isomorphism from $F(\alpha)$ to $F(\beta)$ fixing F and sending α to β. □

The following is also a key technical results that lets one extends maps built from the previous proposition to larger fields.

Theorem 1.1 (Extension theorem)**.** *Let K/F be an algebraic extension and let E be an algebraic closed field. Let $\sigma : F \to E$ be an embedding. Then there exists an embedding $\tau : K \to E$ lifting σ. That is, $\tau(x) = \sigma(x)$ for all $x \in F$.*

Proof. I won't recall the proof here, but just remind you that this is the proposition that required the use of Zorn's lemma. □

Theorem 1.2 (Equivalent notions of normal)**.** *Let K/F be an algebraic extension. Then the following are equivalent (TFAE)*

1. *K is a splitting field over F;*
2. *whenever $\tau : K \to \overline{F}$ is an embedding then $\tau(K) \subseteq K$;*
3. *if $p(x) \in F[x]$ is an irreducible polynomial with a zero in K, then $p(x)$ splits into linear factors in $K[x]$.*

Proof. (1) $\implies$ (2): Let K be the splitting field of $\{f_j\}$ with each $f_j \in F[x]$. Set R equal to the collection of all zeroes of all of the f_j in $\overline{F}$. Then $K = F(\{\alpha\}_{\alpha \in R})$. To show that $\tau(K) \subseteq K$ we thus only need to check that $\tau(\alpha) \in K$ for each $\alpha \in R$ as τ fixes F. To this end, take α in R and write f_j for the polynomial in our collection for which α is a root. Then $\tau(\alpha)$ is again a zero of f_j as $f_j \in F[x]$ and τ fixes F. Hence $\tau(\alpha) \in R$ which implies $\tau(\alpha) \in K$. Thus $\tau(K) \subseteq K$.

(2) $\implies$ (3): Let $p(x)$ be an irreducible polynomial in $F[x]$ with a zero α in K. Let β be another zero of $p(x)$ in $\overline{F}$. Then consider the map

$$\sigma : F(\alpha) \cong F(\beta) \hookrightarrow \overline{F}.$$

Here the first map is given by Proposition 1.1 and the second is just the identity map. By Theorem 1.1, σ can be extended to a map $\tau : K \to \overline{F}$. But then by (2) we know that $\tau(K) \subseteq K$. Since $\tau(\alpha) = \beta$ we deduce $\beta \in K$ as desired.

(3) $\implies$ (1): For every $\alpha \in K$, let $p_\alpha(x) = \mathrm{irr}(\alpha, F)$. By (3) each $p_\alpha(x)$ splits into linear factors in K as $p_\alpha(x)$ has $\alpha \in K$ as a root. But this implies that K is the splitting field of the family of polynomials $\{p_\alpha(x)\}_{\alpha \in K}$. □

Recall that an algebraic extension K/F is called *normal* if any of the parts of Theorem 1.2 hold.

The following lemma shows that in part (3) above we actually have $\tau(K) = K$ if K/F is finite.

Lemma 1.1. *If K/F is finite and τ is an embedding from K to K over F, then τ is an automorphism.*

Proof. We just need to check that τ is surjective. To this end, note that τ is an F-linear map. Indeed for $c \in F$ and $x \in K$, we have $\tau(cx) = \tau(c)\tau(x) = c\tau(x)$ as τ fixes F. Thus, $\tau(K)$ is isomorphic to K as an F-vector space. In particular, $\dim_F(K) = \dim_F(\tau(K))$. Since $\tau(K) \subseteq K$, we deduce $\tau(K) = K$ and τ is surjective. □

An algebraic extension K/F is called *separable* if for all $\alpha \in K$, we have $\mathrm{irr}(\alpha, K)$ has no repeated roots.

Theorem 1.3 (Primitive element theorem)**.** *If K/F is a finite separable extension then there is some γ such that $K = F(\gamma)$.*

Proof. I won't recall the proof here — the statement is much more important than the proof. □

One more lemma which will be important in the Galois correspondence.

Lemma 1.2. *Let $K/E/F$ be a tower fields. If K/F is normal, then K/E is normal. If K/F is separable, then K/E is separable.*

Proof. Let K/F be normal. By Theorem 1.2, K is a splitting field over F. But then the same collection of polynomials shows that K is a splitting field over E and is thus normal. Now let K/F be separable. Let $\alpha \in K$ and we need to check that $\mathrm{irr}(\alpha, E)$ has no multiple roots. But $\mathrm{irr}(\alpha, E)$ divides $\mathrm{irr}(\alpha, F)$ and we know this latter polynomial has no repeated roots as K/F is separable. □

2 Galois theory

Definition 2.1. A finite extension K/F is called *Galois* if the extension is both normal and separable. In this case, we write $\mathrm{Gal}(K/F)$ for $\mathrm{Aut}(K/F)$ so that

$$\mathrm{Gal}(K/F) = \{\sigma : K \to K \mid \sigma \text{ is an automorphism which fixes } F\}.$$

Theorem 2.2 (Galois extensions have the right number of automorphisms)**.** *If K/F is a Galois extension, then the size of* $\mathrm{Gal}(K/F)$ *equals* $[K : F]$.

Proof. By the Primitive Element theorem (Theorem 1.3), we can write $K = F(\gamma)$ for $\gamma \in K$. Then $[K : F]$ equals the degree of $\mathrm{irr}(\gamma, F)$. Since any automorphism of K which fixes F is determined by what it does to γ and γ must map to another root of $\mathrm{irr}(\gamma, F)$, we see that there can be at most $[K : F]$ automorphisms of K fixing F.

We now check that there are exactly $[K : F]$ automorphisms. First note that since K/F is separable, $\mathrm{irr}(\gamma, F)$ has exactly $[K : F]$ roots. Let β be one of these roots. We have a map

$$\sigma : K = F(\gamma) \cong F(\beta) \hookrightarrow \overline{F}.$$

Here the first map is given by Proposition 1.1 and the second is just the identity map. Since K/F is normal, we then have $\tau(K) \subseteq K$. But then Lemma 1.1 gives that τ is an automorphism. □

Let K/F be a Galois extension. The fundamental theorem of Galois theory relates the subfields of K/F to the subgroups of $\mathrm{Gal}(K/F)$. How can we make such a correspondence? Well, in one direction we need to take a subfield E of K/F and build a subgroup of $\mathrm{Gal}(K/F)$. To do this first note that K/E is Galois as it is both normal and separable by Lemma 1.2. Thus in makes sense to consider $\mathrm{Gal}(K/E)$ which is clearly a subgroup of $\mathrm{Gal}(K/F)$ as any automorphism that fixes E automatically fixes F since $E \supseteq F$.

For the other direction, we need to take a subgroup H of $\mathrm{Gal}(K/F)$ and build a subfield of K. To do this, define

$$K^H = \{\alpha \in K \mid \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}.$$

That is K^H is the fixed field of H, the set of all elements of K that are fixed by H. It is easy to see that this is a field and K^H certainly contains F as F is fixed by all of $\mathrm{Gal}(K/F)$.

We now state the main theorem.

Theorem 2.3. *Let K/F be a Galois extension. There is an inclusion reversing bijection between*

$$\{\textit{subfields of } K/F\} \quad \textit{and} \quad \{\textit{subgroups of } \mathrm{Gal}(K/F)\}.$$

The bijection is given by a subfield E maps to $\mathrm{Gal}(K/E)$ while a subgroup H maps to K^H.

The "inclusion reversing" part of the theorem is explained in the following lemma.

Lemma 2.1. *Let K/F be a Galois extension.*

1. *If $E_1 \subseteq E_2$ are subfields of K/F, then $\mathrm{Gal}(K/E_1) \supseteq \mathrm{Gal}(K/E_2)$.*
2. *If $H_1 \subseteq H_2$ are subgroups of $\mathrm{Gal}(K/F)$, then $K^{H_1} \supseteq K^{H_2}$.*

Proof. Both parts are clear. Indeed, for the first part, for $\sigma \in \mathrm{Gal}(K/E_2)$, we have that σ fixes E_2 and thus σ fixes E_1 as $E_1 \subseteq E_2$. Thus $\sigma \in \mathrm{Gal}(K/E_1)$. For the second part, for $\alpha \in K^{H_2}$, by definition, α is fixed by everything in H_2. But since $H_1 \subseteq H_2$, we then have that α is fixed by everything in H_1 and hence $\alpha \in K^{H_1}$. □

To prove Theorem 2.3, we need to check that this correspondence is a bijection. And we do this by checking that the two maps are inverses of each other. That is, if we start with a field E and form the corresponding subgroup $\mathrm{Gal}(K/E)$ and then form the corresponding field $K^{\mathrm{Gal}(K/E)}$ we should get back E. Likewise, if we start with a subgroup H and form the corresponding field K^H and then the corresponding subgroup $\mathrm{Gal}(K/K^H)$ we should recover H. So we need the two facts

$$E = K^{\mathrm{Gal}(K/E)}$$

and

$$H = \mathrm{Gal}(K/K^H).$$

We first note that in each case the inclusion $\subseteq$ is clear if you think about. In the first case, to check $E \subseteq K^{\mathrm{Gal}(K/E)}$ we need to check that E is fixed by $\mathrm{Gal}(K/E)$. But of course it is because that's the definition of $\mathrm{Gal}(K/E)$! In the second case, to check $H \subseteq \mathrm{Gal}(K/K^H)$, we need to check that H fixes K^H. Again this is just the definition! But it is the other directions that require real work.

Theorem 2.4. *Let K/F be Galois and let E be a subfield. Then*

$$E = K^{\mathrm{Gal}(K/E)}.$$

Proof. As described above we know the inclusion $\subseteq$. To prove the converse, let $M = K^{\mathrm{Gal}(K/E)}$. We then have a tower of fields $K/M/E$. Note that by Lemma 1.2, we have that K/M and K/E are Galois extensions. We claim that $\mathrm{Gal}(K/M) = \mathrm{Gal}(K/E)$. To see this, note that the inclusion $\subseteq$ follows from Lemma 2.1 as $E \subseteq M$. For the reverse inclusion, for $\sigma \in \mathrm{Gal}(K/E)$ to see that σ is in $\mathrm{Gal}(K/M)$ we must check that σ fixes M. But that is the definition of M. Thus we have shown that $\mathrm{Gal}(K/M) = \mathrm{Gal}(K/E)$. Then by Theorem 2.2, we deduce that $[K : M] = [K : E]$ which implies $E = M$ as desired. □

Theorem 2.5. *Let K/F be Galois and let H be a subgroup of $\mathrm{Gal}(K/F)$. Then*

$$H = \mathrm{Gal}(K/K^H).$$

Proof. We have already seen that $H \subseteq \mathrm{Gal}(K/K^H)$. Thus $\#H \leq \#\,\mathrm{Gal}(K/K^H) = [K : K^H]$ where the last equality is Theorem 2.2. It suffices to see then that $[K : K^H] \leq \#H$.

To this end, write $K = K^H(\alpha)$ for $\alpha \in K$ by the Primitive Element theorem (Theorem 1.3). It then suffices to see that α satisfies a polynomial in $K^H[x]$ with degree less than or equal to $\#H$. Indeed, if α satisfied such a polynomial, then $\mathrm{irr}(\alpha, K^H)$ would have degree less than or equal to $\#H$ which implies $[K : K^H] = [K^H(\alpha) : K^H] \leq \#H$.

We now build such a polynomial. Set

$$h(x) = \prod_{\sigma \in H} x - \sigma\alpha.$$

Note that α is a root of $h(x)$ since when σ is the identity, we get a factor of $x - \alpha$ in $h(x)$. Next we claim $h(x) \in K^H[x]$. To see this take $\tau \in H$ and apply it to all of the coefficients of H. We get

$$(\tau h)(x) = \prod_{\sigma \in H} x - \tau\sigma\alpha = \prod_{\sigma \in H} x - \sigma\alpha = h(x).$$

Here the middle equality follows because multiplicity by τ on H simply permutes around the elements of H. Since $\tau h = h$, all of the coefficients of h are fixed by H and hence $h(x) \in K^H[x]$. This completes the proof since $[K : K^H] = \deg(\mathrm{irr}(\alpha, K^H)) \leq \deg(h) = \#H$. $\square$