MAT 535 Notes on The Fundamental Theorem of Galois Theory

These are some notes accompanying the proof of the fundamental theorem of Galois theory presented in lecture. The textbook gives a slightly different proof which we also discuss.

1 Algebras of set functions.

Let F be a commutative ring with 1. For every set Σ, denote by F^Σ the set of all set functions $a : \Sigma \to F$. This is an F-algebra under pointwise addition, pointwise scaling, and pointwise multiplication; i.e., for a, b in F^Σ and for λ in F, for every σ in Σ we define

$$(a+b)(\sigma) := a(\sigma) + b(\sigma), \quad (\lambda \cdot b)(\sigma) := \lambda \cdot b(\sigma), \quad (a \cdot b)(\sigma) := a(\sigma) \cdot b(\sigma).$$

These structures make F^Σ into a commutative F-algebra whose additive identity is the constant function with value 0 and whose multiplicative identity is the constant function with value 1. For every element λ in F, we will denote by λ the constant function in F^Σ with value λ.

For every set function,

$$u : \Sigma \to T$$

there is an associated function

$$F^u : F^T \to F^\Sigma, \quad F^u(a) := a \circ u.$$

By the definition of addition, scaling and multiplication,

$$(a+b) \circ u = a \circ u + b \circ u, \quad (\lambda \cdot b) \circ u = \lambda \cdot (b \circ u), \quad (a \cdot b) \circ u = (a \circ u) \cdot (b \circ u).$$

Thus F^u is a homomorphism of F-algebras. For every pair of set functions,

$$u : \Sigma \to T, \quad v : T \to \Theta,$$

the composition

$$F^u \circ F^v : F^\Theta \to F^\Sigma$$

equals $F^{v \circ u}$. And for the identity map

$$\mathrm{Id}_\Sigma : \Sigma \to \Sigma,$$

also F^{Id_Σ} equals the identity map on F^Σ. Altogether we have the following.

Proposition 1.1. *The rule associating to every set Σ the associated F-algebra F^Σ and associating to every set function u the associated F-algebra homomorphism F^u is a contravariant functor from the category of sets to the category of F-algebras.*

As with all such general constructions, there is a universal property. For every set Σ and for every F-algebra B, define $\mathcal{F}_\Sigma(B)$ to be the set of all binary operations,

$$\beta : \Sigma \times B \to F$$

such that for every σ in Σ, the induced map

$$\beta_\sigma : B \to F, \quad b \mapsto \beta(\sigma, b)$$

is an F-algebra homomorphism. For every F-algebra homomorphism $f : A \to B$, there is an associated set map

$$\mathcal{F}_\Sigma(f) : \mathcal{F}_\Sigma(B) \to \mathcal{F}_\Sigma(A), \quad \beta \mapsto \beta \circ (\mathrm{Id}_\Sigma \times f).$$

It is straightforward to verify the following.

Proposition 1.2. *The rule $\mathcal{F}_\Sigma$ is a contravariant functor from the category of F-algebras to the category of sets.*

The point is that there is a natural object α_Σ in $\mathcal{F}_\Sigma(F^\Sigma)$,

$$\alpha_\Sigma : \Sigma \times F^\Sigma \to F, \quad (\sigma, a) \mapsto a(\sigma).$$

In fact, the F-algebra addition, scaling and multiplication are the unique operations that commute with the maps $\alpha_{\Sigma,\sigma}$ for every σ in Σ. Precisely, c equals $a+b$ if and only if for every σ in Σ, $\alpha_{\Sigma,\sigma}(c)$ equals $\alpha_{\Sigma,\sigma}(a) + \alpha_{\Sigma,\sigma}(b)$, and similarly for scaling and multiplication.

For every F-algebra B and for every element β in $\mathcal{F}_\Sigma(A)$, define the function

$$\widetilde{\beta} : B \to F^\Sigma, \quad b \mapsto (\sigma \mapsto \beta_\sigma(b)).$$

This set map has the property that $\alpha_{\Sigma,\sigma}(\widetilde{\beta}(b))$ equals $\beta_\sigma(b)$ for every σ in Σ. By hypothesis β_σ is an F-algebra homomorphism, i.e., it commutes with addition, scaling and multiplication. Thus $\alpha_{\Sigma,\sigma} \circ \widetilde{\beta}$ commutes with addition, scaling and multiplication for every σ in Σ. By the previous paragraph, this means that $\widetilde{\beta}$ commutes with addition, scaling and multiplication; i.e., $\widetilde{\beta}$ is an F-algebra homomorphism. Moreover, since an element a in F^Σ is uniquely determined by all of its value $\alpha_{\Sigma,\sigma}(a)$, $\widetilde{\beta}(b)$ is the unique element such that $\alpha_{\Sigma,\sigma}(\widetilde{\beta}(b))$ equals $\beta_\sigma(b)$ for every σ in Σ. In other words, $\widetilde{\beta}$ is the unique F-algebra homomorphism such that $\alpha_\Sigma \circ \widetilde{\beta}$ equals β. Altogether we have proved the following.

Proposition 1.3. *For every set Σ, the F-algebra F^Σ together with the object α_Σ in $\mathcal{F}_\Sigma(F^\Sigma)$ represent the functor $\mathcal{F}_\Sigma$.*

In fact the functor $\Sigma \mapsto F^\Sigma$ is the left adjoint functor in an adjoint pair of functors. The right adjoint functor in this pair is the Yoneda functor

$$h^F : F - \text{Algebras} \to \text{Sets}, \quad A \mapsto \text{Hom}_{F-\text{Alg}}(A, F).$$

Since we do not need this, we will not pursue it.

Proposition 1.4. *Assume that F is nonzero. Let $u : \Sigma \to T$ be a set map.*

(i) The F-algebra homomorphism F^u is injective if and only if u is surjective.

(ii) And F^u is surjective if and only if u is injective.

Proof. **(i)** First assume that u is injective, i.e., the associated surjective set map

$$u_{\text{surj}} : \Sigma \to u(\Sigma)$$

is a bijection. Denote by u_{surj}^{-1} the inverse bijection. For every set map $a : \Sigma \to F$, define $u_!(a) : T \to F$ to be the unique set map which equals $a \circ u_{\text{surj}}^{-1}$ on $u(\Sigma)$ and which equals 0 on the complement $T - u(\Sigma)$. Then $F^u(u_!(a))$ equals a, so that F^u is surjective. Note that the rule $a \mapsto u_!(a)$ is a right inverse to F^u which is an F-module homomorphism. But $u_!(1)$ equals 1 if and only if u is surjective. So in general $u_!$ is not a ring homomorphism (since it does not send 1 to 1).

Next assume that u is not injective. Then there exist distinct elements σ and σ' in Σ such that $u(\sigma)$ equals $u(\sigma')$. For every b in F^T, $F^u(b)$ equals $b \circ u$, and so has equal values on σ and σ'. Define $\mathbf{e}_\sigma : \Sigma \to F$ to be the set map which equals 1 on σ, and which equals 0 on $\Sigma - \{\sigma\}$. Since $\mathbf{e}_\sigma$ has different values on σ and σ' (since 1 does not equal 0 in F), $\mathbf{e}_\sigma$ is not in the image of F^u. Thus F^u is not surjective.

(ii) First assume that u is surjective. Let b and b' be elements in F^T such that $F^u(b)$ equals $F^u(b')$, i.e., $b \circ u$ equals $b \circ u'$. For every τ in T, there exists σ in Σ with $\tau = u(\sigma)$. Thus $b(\tau)$ equals $(b \circ u)(\sigma)$, which equals $(b' \circ u)(\sigma)$ by hypothesis, and this equals $b'(\tau)$. So b equals b'. Therefore F^u is injective.

Next assume that u is not surjective, i.e., there exists τ in T which is not in $u(\Sigma)$. Then $F^u(\mathbf{e}_\tau)$ equals 0, which equals $F^u(0)$. But $\mathbf{e}_\tau$ is not equal to 0. Thus F^u is not injective. $\square$

Because of the proposition, injective set maps with target Σ determine F-algebra quotients of F^Σ. Because quotient objects are a bit less canonical than subobjects, we will instead talk about the kernel of the quotient homomorphims, which is an ideal in F^Σ. Similarly, surjective set maps with source Σ determine F-subalgebras of F^Σ. If F is a field and if Σ is finite, every quotient F-algebra of F^Σ and every F-subalgebra of F^σ arises in this way.

Proposition 1.5. *Let F be a field and let Σ be a finite set. Every ideal in F^Σ is of the form Ker(F^u) for an injective set map $u : T \to \Sigma$. And if $u' : T' \to \Sigma$ is an injective set map with Ker($F^{u'}$) equal to Ker(F^u), then there exists a unique set map $v : T' \to T$ such that u' equals $u \circ v$ (and necessarily v is a bijection).*

Proof. Let I be an ideal in F^{Σ}. Define T_I to be the subset of Σ consisting of all elements τ such that $\alpha_{\Sigma,\tau}(I)$ equals $\{0\}$. Let $u_I : T_I \to \Sigma$ be the inclusion map. The claim is that I equals $\mathrm{Ker}(F^{u_I})$. By construction, I is contained in $\mathrm{Ker}(F^{u_I})$. It remains to prove the reverse inclusion.

For every element σ in Σ, denote by $\mathbf{e}_\sigma$ the set function which equals 1 on σ and which equals 0 on $\Sigma - \{\sigma\}$. Then $\mathrm{Ker}(F^{u_I})$ is precisely $\mathrm{span}(\mathbf{e}_\sigma | \sigma \in \Sigma - T_I)$. For every element σ in $\Sigma - T_I$, $\alpha_{\Sigma,\sigma}(I)$ is an F-submodule of F which is not equal to $\{0\}$, i.e., a nonzero ideal in F. Since F is a field, this ideal equals F, i.e., there exists an element a in I such that $a(\sigma)$ equals 1. Since I is an ideal, $\mathbf{e}_\sigma \cdot a$ is in I. But $\mathbf{e}_\sigma \cdot a$ equals $\mathbf{e}_\sigma$, so $\mathbf{e}_\sigma$ is in I. Thus I contains $\mathrm{span}(\mathbf{e}_\sigma | \sigma \in \Sigma - T_I)$, i.e., I contains $\mathrm{Ker}(F^{u_I})$.

Now let $u : T \to \Sigma$ be the inclusion of a subset of Σ. And let $u' : T' \to \Sigma$ be an injective set map such that $\mathrm{Ker}(F^{u'})$ equals $\mathrm{Ker}(F^{u})$. For every σ in $\Sigma - T$, since $\mathbf{e}_\sigma$ is in $\mathrm{Ker}(F^u)$, also $F^{u'}(\mathbf{e}_\sigma)$ equals 0. Thus σ is not in the image of u'. So $\mathrm{Image}(u')$ is contained in T. Define $v : T' \to T$ to be the unique map such that u' equals $u \circ v$.

The final claim is that v is a bijection. Since u' is an injection, also v is an injection. And for every τ in T, since $\mathbf{e}_\tau$ is not in $\mathrm{Ker}(F^u)$, also $\mathbf{e}_\tau$ is not in $\mathrm{Ker}(F^{u'})$. Thus τ is in the image of u. Therefore also v is surjective. Therefore v is a bijection. $\square$

Corollary 1.6. *Let F be a field and let Σ, T be finite sets. Every surjective F-algebra homomorphism $F^{\Sigma} \to F^{T}$ is of the form F^u for a unique set map $u : \Sigma' \to \Sigma$, and u is an injection. If F^u is an isomorphism, then u is a bijection.*

Proof. The corollary is trivial if T is empty. Thus assume that T is nonempty. Let $\phi : F^{\Sigma} \to F^{T}$ be a surjective F-algebra homomorphism. For every element τ of T, let $e_\tau : \{\tau\} \to T$ be the inclusion. The composition $F^{e_\tau} \circ \phi$ is a surjection from F^{Σ} to $F^{\{\tau\}}$ whose kernel is a maximal ideal. By Proposition 1.5, this is the kernel of the F-algebra homomorphism of a subset of F^{Σ}. And since this kernel is a maximal proper ideal, the subset is a minimal nonempty subset, i.e., a singleton set $\{\sigma\}$ for a unique element σ of Σ.

For every τ as above, define $u(\tau)$ to be this unique element σ. Then $u : T \to \Sigma$ is the unique set map such that $F^{e_\tau} \circ F^u$ equals $F^{e_\tau} \circ \phi$ for every element τ of T. But the product map

$$(F^{e_\tau})_{\tau \in T} : F^T \to \prod_{\tau \in T} F^{\{\tau\}}$$

is an isomorphism. Since the composition of this isomorphism with F^u equals the composition with ϕ, F^u equals ϕ. Thus u is the unique set map such that F^u equals ϕ.

Also, if $u(\tau)$ equals $u(\tau')$, then $F^{e_\tau} \circ F^u$ equals $F^{e_{\tau'}} \circ F^u$. Thus $F^{e_\tau} \circ \phi$ equals $F^{e_{\tau'}} \circ \phi$. Since ϕ is surjective, this means that F^{e_τ} equals $F^{e_{\tau'}}$. In particular they have equal kernels. But again by Proposition 1.5, this implies that τ equals τ'. Therefore u is injective.

Finally, if F^u is invertible, then the same argument proves that the inverse map is of the form F^v for a unique set map $v : \Sigma \to T$, which is an injective set map. But then $F^{u \circ v}$ and $F^{v \circ u}$ are the respective identity maps on F^{Σ} and F^{T}. Since F^{Id_Σ} and F^{Id_T} are also the identity maps, the uniqueness of the set maps above implies that $u \circ v$ equals Id_Σ and $v \circ u$ equals Id_T. Thus u is a bijection. $\square$

For the proof of the next proposition, it is useful to make two definitions. First of all, for every a in F^Σ, the *support* of a is the subset

$$\mathrm{Supp}(a) := a^{-1}(F - \{0\}) = \Sigma - a^{-1}(0).$$

Next, for every subset T of Σ, define $\mathbf{e}_T$ to be the set function $\Sigma \to F$ which equals 1 on T and which equals 0 on $\Sigma - T$. Sometimes this is called the *characteristic function* or the *indicator function* of T. Observe that $\mathrm{Supp}(\mathbf{e}_T)$ equals T.

Proposition 1.7. *Let F be a field and let Σ be a finite set. Every F-subalgebra in F^Σ is of the form Image(F^q) for a surjective set map $q : \Sigma \to \Theta$. And if $q' : \Sigma \to \Theta'$ is a surjective set map with Image($F^{q'}$) equal to Image(F^q), then there exists a unique set map $w : \Theta \to \Theta'$ such that q' equals $w \circ q$ (and necessarily w is a bijection).*

Proof. Let B be an F-subalgebra of F^Σ (in particular B contains 1). Let σ be any element of Σ. Consider the collection of all subsets of Σ of the form $\mathrm{Supp}(b)$ for an element b in B with $b(\sigma) \neq 0$, i.e., σ is in $\mathrm{Supp}(b)$. There is at least one such set, namely $\Sigma = \mathrm{Supp}(1)$. Let T be a minimal set among all such subsets, i.e., i.e., if b' is an element of B with $b'(1) \neq 0$, then $\mathrm{Supp}(b')$ is not properly contained in T. By definition, there exists b in B with $b(\sigma) \neq 0$ and with $\mathrm{Supp}(b)$ equals T. The claim is that b equals $b(\sigma) \cdot \mathbf{e}_T$. In particular, $\mathbf{e}_T$ equals $(1/b(\sigma)) \cdot b$, which is in the F-algebra B.

If T equals the singleton set $\{\sigma\}$, the claim is obvious. Thus assume there exists an element τ in T_σ different from σ. Consider the element $b' := b^2 - b(\tau)b$. Since B is an F-algebra which contains b, also B contains b'. Of course $\mathrm{Supp}(b')$ is contained in T. And $b'(\tau)$ equals 0, so that $\mathrm{Supp}(b')$ is properly contained in T. By the minimality of T, it follows that $b'(\sigma)$ equals 0. In other words, $b(\sigma)^2 = b(\sigma)b(\tau)$. Since $b(\sigma)$ is nonzero, we can divide each side by $b(\sigma)$ to conclude that $b(\tau)$ equals $b(\sigma)$. Since $b(\tau)$ equals $b(\sigma)$ for every element τ in T, and since $b(\tau)$ equals 0 for every element τ in $\Sigma - T$, b equals $b(\sigma)\mathbf{e}_T$.

Now suppose that T' is any minimal element of the collection of all subsets of Σ of the form $\mathrm{Supp}(b)$ for an element b in B with $b(\sigma) \neq 0$. Then, by the same argument, also $\mathbf{e}_{T'}$ is in B. Since B is an algebra, the product $\mathbf{e}_T \cdot \mathbf{e}_{T'}$ is in B. But this product is $\mathbf{e}_{T \cap T'}$. Since $T \cap T'$ contains σ and is contained in T, by the minimality of T it follows that $T \cap T'$ equals T, i.e., T is contained in T'. By the same argument applied to T', also T' equals T. Thus T is the unique minimal element in this collection. Therefore, for every element σ in Σ, there exists a subset T_σ of Σ of the form $\mathrm{Supp}(b)$ for some b in B with $b(\sigma) \neq 0$, and such that for every element b' in B with $b'(\sigma) \neq 0$, T_σ is contained in $\mathrm{Supp}(b')$. Moreover $\mathbf{e}_{T_\sigma}$ is an element of B.

Let τ be any element of T_σ and consider T_τ. By the argument above, $\mathbf{e}_{T_\Sigma}$ and $\mathbf{e}_{T_\tau}$ are contained in B. Since B is an algebra, also the product $\mathbf{e}_{T_\sigma} \cdot \mathbf{e}_{T_\tau}$ is contained in B. And this equals $\mathbf{e}_{T_\Sigma \cap T_\tau}$. If $T_\sigma \cap T_\tau$ does not contain σ, i.e., if σ is contained in $T_\sigma - T_\tau$, then consider the difference $\mathbf{e}_{T_\sigma} - \mathbf{e}_{T_\sigma \cap T_\tau}$, which is also an element in the F-algebra B. This difference is simply $\mathbf{e}_{T_\Sigma - T_\tau}$. By hypothesis, $T_\sigma - T_\tau$ contains σ. And it does not contain τ, thus it is strictly contained in T_σ. This contradicts minimality of T_Σ. Thus σ is contained in $T_\sigma \cap T_\tau$. And then again by minimality of T_Σ, $T_\sigma \cap T_\tau$ equals T_Σ, i.e., T_σ is contained in T_τ. But then by minimality of T_τ, T_σ equals T_τ. So for every τ in T_σ, T_τ equals T_σ.

Next let σ' be any element of Σ. If $T_\sigma \cap T_{\sigma'}$ contains an element τ, then by the above paragraph T_τ equals T_σ. And by the same argument, also T_τ equals $T_{\sigma'}$. Thus T_σ equals $T_{\sigma'}$. Therefore, for every pair of elements σ, σ' in Σ, if T_σ and $T_{\sigma'}$ intersect, then they are equal. This precisely means that the collection Θ_B of subsets of Σ of the form T_σ for some σ is a *partition* of Σ. And there is a surjective function $q_B : \Sigma \to \Theta_B$ defined by $q_B(\sigma) := T_\sigma$. The algebra $\text{Image}(F^{q_B})$ is precisely the F-subalgebra of F^Σ consisting of functions b which are constant on each subset T of Θ_B. The claim is that B equals $\text{Imega}(F^{q_B})$.

For every element T in Θ_B, the inverse image $q_B^{-1}(\{T\})$ equals T as a subset of Σ. In particular, for the indicator function $\mathbf{e}_T$ in F^{Θ_B}, F^q maps this to the indicator function $\mathbf{e}_T$ in F^Σ. As proved, this is an element of B. And the elements $\mathbf{e}_T$ corresponding to elements T of Θ_B give an F-basis for F^{Θ_B} as an F-vector space. So $\text{Image}(F^{q_B})$ is contained in B. It remains to prove the reverse inclusion, i.e., to prove that every element b of B is constant on every subset T of Θ_B.

Let b be an element of B and let T be any element of Θ_B. The claim is that b is constant on T. If b is 0 on T, then b is constant on T. Thus suppose that b is not zero on T, i.e., there exists σ in $T \cap \text{Supp}(b)$. Since B is an algebra which contains both b and T, B contains the product $b_T := b \cdot \mathbf{e}_T$. The support of b_T equals $T \cap \text{Supp}(b)$, which contains σ and is contained in T. Thus by minimality of $T = T_\sigma$, the support of b_T equals T. As proved above, every element of B whose support equals T is of the form $b(\sigma)\mathbf{e}_T$. Thus b_T is constant on T. But for every τ in T, $b_T(\tau)$ equals $b(\tau)$. Thus b is constant on T. Since this holds for every τ in Θ_B, b is contained in $\text{Image}(F^{q_B})$. Therefore B equals $\text{Image}(F^{q_B})$.

Now let Θ be a partition of Σ and let $q : \Sigma \to \Theta$ be the corresponding surjective set map. Let $q' : \Sigma \to \Theta'$ be any surjective function such that $\text{Image}(F^{q'})$ equals $\text{Image}(F^q)$ as F-subalgebras of F^Σ. The collection Θ' of all fibers of q' is a partition of Σ. As above, $\text{Image}(F^{q'})$ is the collection of all set functions which are constant on every set T' in Θ'. In particular, for every T in Θ, since $\mathbf{e}_T$ is in $\text{Image}(F^q)$, which equals $\text{Image}(F^{q'})$, $mathbfe_T$ is constant on every fiber T' of q'. In particular the support T is a union of fibers T' of q'. By the same argument, every fiber T' of q' is a union of fibers T of q. Thus, every fiber T of q is a fiber T' of q'. Define $w(T)$ to be the unique point of Θ' whose fiber T' in Σ equals T. This is the unique set map $w : \Theta \to \Theta'$ such that q' equals $w \circ q$. Since q' is surjective, also w is surjective. But since the inverse image under q' of $w(T)$ equals T, also w is injective. Therefore w is a bijection. □

Corollary 1.8. *Let F be a field and let Σ, Σ' be finite sets. Every F-algebra homomorphism $\phi : F^{\Sigma'} \to F^\Sigma$ is of the form F^u for a unique set map $u : \Sigma \to \Sigma'$. And ϕ is surjective, resp. injective, if and only if u is injective, resp. surjective.*

Proof. Let $\phi : F^{\Sigma'} \to F^\Sigma$ be an F-algebra homomorphism. By Proposition 1.7, there exists a surjective set map $q : \Sigma \to \Theta$ such that $\text{Image}(\phi)$ equals $\text{Image}(F^q)$. Thus ϕ factors through a surjective F-algebra homorphism $\psi : F^{\Sigma'} \to F^{\Theta}$, i.e., $F^q \circ \psi$ equals ϕ, and ψ is unique. By Corollary 1.6, there exists a unique set map $v : \Theta \to \Sigma'$ such that F^v equals ψ, and v is injective. Thus $u = v \circ q$ is the unique set map such that F^u equals ϕ. And by Proposition 1.4, ϕ is surjective, resp. injective, if and only if u is injective, resp. surjective. □

Before continuing we note that both Proposition 1.5 and Proposition 1.7 fail if Σ is an infinite set. First, consider the ideal I in F^{Σ} consisting of all set functions $\Sigma \to F$ which have finite support. Let $q : T \to \Sigma$ be a set map such that $\text{Ker}(F^q)$ contains I. For every σ in Σ, $\mathbf{e}_\sigma$ is in I, thus $F^q(\mathbf{e}_\sigma)$ equals 0. This means that σ is not in the image of q, i.e., $\text{Image}(q)$ is the empty set. This forces T to be the empty set. But then $\text{Ker}(F^q)$ is all of F^{Σ}. Since Σ is infinite, 1 is not in I. Thus 1 is in $\text{Ker}(F^q)$, but not in I. Therefore I is not of the form $\text{Ker}(F^q)$.

Next, consider the F-subspace $B = F \cdot 1 + I$ of F^{Σ}. It is straightforward to check that this is an F-subalgebra of F^{Σ}. The supports of elements of B are precisely the finite subsets of Σ together with the cofinite subsets of Σ, i.e., sets whose complements are finite. The minimal sets among these sets are the singleton sets. So if B were of the form $\text{Image}(F^q)$ for a set map $q : \Sigma \to \Theta$, then the fibers of q would be singleton sets, i.e., q would be injective. But then by Proposition 1.4, F^q is surjective so that $\text{Image}(F^q)$ equals F^{Σ}. Every infinite set Σ contains an infinite subset T whose complement $\Sigma - T$ is also infinite. So $\mathbf{e}_T$ is an element in F^{Σ} which is not in B. Therefore B is not of the form $\text{Image}(F^q)$.

Next, let G be a group acting transitively on a set Σ, $\mu : G \times \Sigma \to \Sigma$. Let Θ be a partition of Σ which is *G-invariant*, i.e., for every T in Θ and for every g in G, $g \cdot T$ is also in Θ. Then there is an induced action of G on Θ. Moreover, for every T and T' in Θ, since G acts transitively on Σ there exists an element g in G mapping an element of T to an element of T', i.e., $g \cdot T$ intersects T'. Since Θ is partition, this implies that $g \cdot T$ equals T'. Thus G acts transitively on Θ.

Fix one element T in Θ, and denote by H the stabilizer subgroup, i.e., the set of all h in G such that $h \cdot T$ equals T. The claim is that T equals $H \cdot \tau$ for one, and hence every, element τ in T. Let τ be an element in T. Since $H \cdot T$ is contained in T (in fact equals T), $H \cdot \tau$ is contained in T. And for every element τ' in T, since G acts transitively on Σ, there exists g in G with $g \cdot \tau$ equal to τ'. But then $g \cdot T$ intersects T. Since Θ is a partition, $g \cdot T$ equals T. Thus g is contained in H. So τ' is contained in $H \cdot \tau$. Therefore T equals $H \cdot \tau$ for each element τ in T.

Since G acts transitively on Θ, every partition set is of the form $g \cdot T$. Therefore the partition sets of Θ are precisely the sets of the form $gH \cdot \tau$, as gH varies over the left cosets of H in G, i.e., the elements of G/H. In summary, we have proved the following.

Proposition 1.9. *Let G be a group, and let Σ be a set with a transitive left action of G. For every partition Θ of Σ which is G-invariant, for every element τ in Σ, denoting by H the stabilizer subgroup of the partition set containing τ, the partition Θ is precisely the collection of subsets $\{gH \cdot \tau | gH \in G/H\}$.*

There is one final observation, which did arise once last semester, but without much fanfare. So here it is again. Let H be a subgroup of G. Let $G \times (G/H) \to G/H$ be the standard left action of

G on G/H. Let $t : G/H \to G/H$ be a set map which is G-equivariant, i.e., $t(g \cdot kH) = g \cdot t(kH)$ for every coset kH in G/H. Define k_0H to be $t(H)$. Then for every coset kH in G/H, we have

$$t(kH) = t(k \cdot H) = k \cdot t(H) = (kk_0)H.$$

So t is uniquely determined by the coset k_0H. However, it is not necessarily well-defined. In order to be well-defined, we must have that $t(hH)$ equals $t(H)$ for every h in H, i.e., hk_0H must equal k_0H for every h in H. In other words Hk_0H must equal k_0H. But this is precisely the condition that k_0 is an element of the normalizer $N_G(H)$. In summary, we have the following.

Proposition 1.10. *For a subgroup H of G, every left G-equivariant map $t : G/H \to G/H$ is of the form $t(kH) = kk_0H$ for a unique coset k_0H in $N_G(H)/H$, and every such map is well-defined and G-equivariant.*

2 The Fundamental Theorem of Galois Theory

Let F be a field, and let $G \leq \mathrm{Aut}(F)$ be a finite subgroup of the group of field automorphisms of F. Denote by E the fixed set $\mathrm{Fix}^G(F)$, i.e.,

$$\mathrm{Fix}^G(F) := \{a \in F | \forall \sigma \in G, \sigma(a) = a\}.$$

Lemma 2.1. *The subset $\mathrm{Fix}^G(F)$ is a subfield of F, and the inclusion $\mathrm{Fix}^G(F) \to F$ is an algebraic field extension.*

Proof. Clearly $\mathrm{Fix}^G(F)$ is a subring of F which contains 1. In particular, $\mathrm{Fix}^G(F)$ is an integral domain. As proved in Theorem 26 (1) on p. 694 of the textbook (and also in lecture), if F is integral over $\mathrm{Fix}^G(F)$, then $\mathrm{Fix}^G(F)$ is a field. And then it follows that $\mathrm{Fix}^G(F) \to F$ is an algebraic field extension (since this is precisely the same thing as an integral ring extension if the source and target are fields). So it suffices to prove that every element b in F satisfies a monic polynomial $p(x)$ with coefficients in $\mathrm{Fix}^G(F)$. Consider the polynomial,

$$p(x) = \prod_{\sigma \in G} (x - \sigma(b)).$$

This is a monic polynomial with $p(b)$ equals 0 (since $x - \mathrm{Id}(b)$ is one of the factors of $p(x)$). And the coefficients of $p(x)$ are symmetric polynomials in the elements $\sigma(b)$, which clearly are G-invariant. Thus the coefficients are elements in $\mathrm{Fix}^G(F)$. $\square$

Now consider the set map

$$\beta : F \times F \to F^G, \quad \beta(c, b) : \sigma \mapsto c\sigma(b).$$

It is straightforward to verify that β is an E-bilinear map and thus determines an E-linear map

$$T : F \otimes_E F \to F^G.$$

In fact, if we consider $F \otimes_E F$ as a left F-vector space via the scaling rule $\lambda \cdot (c \otimes b) := (\lambda c) \otimes b$, then T is even F-linear. If we choose a basis $(b_i)_{i \in I}$ for F as an E-vector space, then $(1 \otimes b_i)_{i \in I}$ is an F-basis for $F \otimes_E F$ (with respect to this left F-vector space structure). And if we use the standard basis $\mathbf{e}_\sigma$ for F^G, then the matrix of the linear transformation T is $[\sigma(b_i)]_{(i,\sigma) \in I \times G}$, i.e.,

$$T(1 \otimes b_i) = \sum_{\sigma \in G} \sigma(b_i) \mathbf{e}_\sigma.$$

The key result is the following.

Theorem 2.2. *The F-linear map T is an isomorphism of F-vector spaces. Moreover it is a homomorphism of F-algebras, hence an isomorphism of F-algebras. In particular, $[F : E]$ is finite and equals $\#G$.*

Proof. As explained in lecture, the proof that F/E is a finite extension of degree $\#G$ in fact proves that the matrix $[\sigma(b_i)]_{(i,\sigma)}$ is a square, invertible matrix, i.e., T is an isomorphism of F-vector spaces. And for every pair of elements b, b' in F,

$$T(1 \otimes b) \cdot T(1 \otimes b') = \left(\sum_{\sigma in G} \sigma(b) \mathbf{e}_\sigma \right) \cdot \left(\sum_{\sigma \in G} \sigma(b') \mathbf{e}_\sigma \right) = \sum_{\sigma \in G} \sigma(b)\sigma(b') \mathbf{e}_\sigma.$$

On the other hand, $(1 \otimes b) \cdot (1 \otimes b')$ equals $1 \otimes (bb')$. Thus,

$$T((1 \otimes b) \cdot (1 \otimes b')) = T(1 \otimes (bb')) = \sum_{\sigma \in G} \sigma(bb') \mathbf{e}_\sigma.$$

Since each σ is a ring homomorphism, $\sigma(bb')$ equals $\sigma(b)\sigma(b')$. Thus T commutes with multiplication. Therefore the F-vector space isomorphism T is actually an F-algebra isomorphism. ☐

Since we know the F-subalgebras of F^G, this means that we know the F-subalgebras of $F \otimes_E F$.

Corollary 2.3. *For the left F-vector space structure on $F \otimes_E F$, every F-subalgebra of $F \otimes_E F$ is of the form $T^{-1}(Image(F^q))$ for a unique partition $q : G \to \Theta$.*

There is a left action of G on the ring $F \otimes_E F$ by E-algebra isomorphisms $\widehat{\sigma}$ defined as follows,

$$\widehat{\sigma} \cdot : F \otimes_E F \to F \otimes_E F, \quad \widehat{\sigma}(c \otimes b) := \sigma(c) \otimes b.$$

Notice that $\widehat{\sigma} \cdot$ is *not* F-linear for the left F-vector space structure on $F \otimes_E F$, (although it is F-linear for the *right* F-vector space structure). There is also a left action of G on F^G by E-algebra isomorphisms $\widetilde{\sigma} \cdot$ defined as follows,

$$\widetilde{\sigma} \cdot : F^G \to F^G, \quad \widetilde{\sigma} \cdot t : \tau \mapsto \sigma(t(\sigma^{-1}\tau)).$$

Proposition 2.4. *The E-algebra isomorphism T is left G-equivariant, i.e., $T((\widehat{\sigma}\cdot f)$ equals $\widetilde{\sigma}\cdot T(f)$ for every σ in G and every f in $F\otimes_E F$. Every left F-subalgebra of $F\otimes_E F$ which is mapped to itself by every $\widehat{\sigma}\cdot$ is of the form $T^{-1}(Image(F^q))$ for the quotient $q: G\to G/H$ associated to a unique subgroup H of G.*

Proof. It is straightforward to verify that $T(\widehat{\sigma}(c\otimes b))$, i.e., $T(\sigma(c)\otimes b)$, is the set map sending each element τ to $\sigma(c)\tau(b)$. But this is the same as $\sigma(t(\tau^{-1}\sigma))$ where t is the set map $\rho\mapsto c\otimes\rho(b)$, i.e., t equals $T(c\otimes b)$. Thus $T(\widehat{\sigma}(c\otimes b))$ equals $\widetilde{\sigma}T(c\otimes b)$.

By Corollary 2.3, every left F-subalgebra of $F\otimes_E F$ comes from a unique partition $q: G\to\Theta$ of G. And Image(F^q) is spanned by the elements $\mathbf{e}_T$ for elements T of the partition. If this algebra is mapped to itself by $\widetilde{\sigma}$, then in particular $\widetilde{\sigma}(\mathbf{e}_T)$ is contained in the algebra. But this element is simply $\mathbf{e}_{\sigma\cdot T}$. So for every partition set T in Θ, $\sigma\cdot T$ is a union of partition sets in Θ. By considering the minimal partition sets, it follows that the partition is G-invariant. And then by Proposition 1.9, there exists a unique subgroup $H\leq G$ such that the partition Θ is simply G/H, the set of H-cosets in G. Conversely, it is straightforward to verify that for every subgroup H of G, the algebra corresponding to the partition G/H is G-invariant. Therefore the G-invariant F-subalgebras of F^G are precisely the subalgebras arising from the partitions G/H of subgroups H of G. ☐

There are also *right* actions of G on $F\otimes_E F$ and on F^G by E-algebra isomorphisms defined as follows,

$$\cdot\widehat{\sigma}: F\otimes_E F\to F\otimes_E F,\quad (c\otimes b)\cdot\widehat{\sigma} := c\otimes\sigma(b).$$

Notice that $\cdot\widehat{\sigma}$ is left F-linear, but it is not right F-linear. There is also a right action of G on F^G by F-algebra isomorphisms $\cdot\widetilde{\sigma}$ defined as follows,

$$\cdot\widetilde{\sigma}: F^G\to F^G,\quad t\cdot\widetilde{\sigma}:\tau\mapsto t(\tau\sigma).$$

Proposition 2.5. *The F-algebra isomorphism T is right G-equivariant, i.e., $T(f\cdot\widehat{\sigma})$ equals $T(f)\cdot\widetilde{\sigma}$ for every σ in G and every f in $F\otimes_E F$. For every left F-subalgebra B of $F\otimes_E F$ which is mapped to itself by every $\widehat{\sigma}\cdot$, there exists a unique subgroup H of G such that B equals $F\otimes_E Fix^H(F)$.*

Proof. Just as in the proof of Proposition 2.4, it is straightforward to check that T is right G-equivariant (in fact this is even easier than checking that T is left G-equivariant). In Proposition 2.5 we already characterized the subalgebras B as above as $T^{-1}(\text{Image}(F^q))$ coming from the quotient $q: G\to G/H$ for a unique subgroup H. The last step is to observe that F^q is the F-algebra of all set functions $t: G\to F$ which are constant on every fiber of q. But since these fibers are left cosets $\tau H = \{\tau\sigma|\sigma\in H\}$, this is precisely the same as saying that $(t\cdot\widetilde{\sigma})(\tau)$ equals $t(\tau)$ for every $\widetilde{\sigma}$ in H. And this is the same as saying that $t\cdot\widetilde{\sigma}$ equals t for every σ in H. Using that T is an F-algebra isomorphism which is G-equivariant, it follows that B is the set of elements,

$$B = \{f\in F\otimes_E F|\forall\sigma\in H, f\cdot\widehat{\sigma} = f\}.$$

Choose a basis $(c_i)_{i\in I}$ for F over E. Then every f in $F\otimes_E F$ is of the form

$$f = \sum_{i\in I} c_i\otimes b_i$$

for a unique I-tuple $(c_i)_{i\in I}$ of elements $c_i \in F$. And

$$f \cdot \widehat{\sigma} = \sum_{i\in I} c_i \otimes \sigma(b_i).$$

Thus $f \cdot \widehat{\sigma}$ equals f if and only if every $\sigma(b_i)$ equals b_i. Thus $f \cdot \widehat{\sigma}$ equals f for every σ in H if and only if every b_i is in the fixed field $\mathrm{Fix}^H(F)$. Therefore B is precisely $F \otimes_E \mathrm{Fix}^H(F)$ for a unique subgroup H of G, and for every subgroup H of B, $F \otimes_E \mathrm{Fix}^H(F)$ is a left G-invariant, left F-subalgebra of $F \otimes_E F$. ☐

Now we can prove the Fundamental Theorem of Galois Theory. But first we need to set up a little notation. With F, G and E as above, define a function,

$$\mathrm{Fix}^\bullet(F) : \{\mathrm{Subgroups} H \leq G\} \to \{\mathrm{Fields} L | E \subseteq L \subseteq F\}, \quad H \mapsto \mathrm{Fix}^H(F).$$

Similarly, define a function

$$\mathrm{Fix}^\bullet(G) : \{\mathrm{Fields} L | E \subseteq L \subseteq F\} \to \{\mathrm{Subgroups} H \leq G\}, \quad L \mapsto \mathrm{Fix}^L(G)$$

where we define

$$\mathrm{Fix}^L(G) := \{\sigma \in G | \forall b \in L, \sigma(b) = b\}.$$

Both sets are partially ordered under inclusion, and each is in fact a *lattice*. A lattice is a partially ordered set together with two operations known as *meet* and *join* satisfying all of the axioms familiar from the lattice of subsets of a fixed set, where meet is union and join is intersection. For subgroups of G, the meet of a collection of subgroups is the smallest subgroup of G containing all the given subgroups. And the join of a collection of subgroups is the intersection of the collection of subgroups. For subextensions of F/E, the meet of a collection of subextensions is the composite extension. And the joint of a collection of subextension is the intersection of the collection of fields.

Theorem 2.6. *The two correspondences above are inverse bijections. Each one is inclusion reversing, and interchanges meets with joins. For every subgroup H of G, and for every subgroup K of H, $[Fix^K(F) : Fix^H(F)]$ equals $[H : K]$. For every subextension $L = Fix^H(F)$, the group of automorphisms of L which fix E is canonically isomorphic to $N_G(H)/H$. In particular, L/E is Galois if and only if H is normal in G.*

Proof. Let H be a subgroup of G, and let L be $\mathrm{Fix}^H(F)$. Let H' be $\mathrm{Fix}^L(G)$. By definition, H is contained in H'. Also by definition, L is contained in $L := \mathrm{Fix}^{H'}(F)$. So $\#H'$ is $\geq \#H$ and $[F : L']$ is $\leq [F : L]$. And by Theorem 2.2, we have

$$\#H = [F : L], \#H' = [F : L'].$$

Thus $\#H$ equals $\#H'$, i.e., H' equals H. So $\mathrm{Fix}^\bullet(F)$ is injective, and $\mathrm{Fix}^\bullet(G)$ is a left inverse of this injective map.

For every subextension L of F/E, consider the F-subalgebra $B_L := F \otimes_E L$ of $F \otimes_E F$. The field L is the set of elements b in F such that $1 \otimes b$ is in B_L, so the number of subextensions L is no greater than the number of F-subalgebras B_L. But B_L is a left G-invariant, left F-subalgebra of $F \otimes_E F$. By Proposition 2.4, the number of such F-subalgebras equals the number of subgroups H of G. And since $\text{Fix}^\bullet(F)$ is injective, the number of extensions of the form $L = \text{Fix}^H(F)$ also equals the number of subgroups of G. Therefore every subextension L of F/E is of the form $\text{Fix}^H(F)$ for some subgroup H of G. So $\text{Fix}^\bullet(F)$ is surjective. Thus $\text{Fix}^\bullet(F)$ is a bijection. And since $\text{Fix}^\bullet(G)$ is a left inverse, it is the inverse bijection.

It is straightforward to check that both bijections are order reversing. Since they are inverses, it follows that both are strictly order reversing, i.e., one element is greater than a second element if and only if the image of the first is less than the image of the second. Thus they strictly reverse upper bounds and lower bounds, i.e., meets and joins.

Let L be $\text{Fix}^H(F)$. Since $[F:E]$ equals $[F:L][L:E]$, and since $[F:E] = \#G$ and $[F:L] = \#H$, it follows that $[L:E]$ equals $[G:H]$. Iterating gives $[\text{Fix}^K(F) : \text{Fix}^H(F)]$ equals $[H:K]$.

Finally, let L be $\text{Fix}^H(F)$. For every σ in $N_G(H)$ and for every τ in H, $\tau' := \sigma\tau\sigma^{-1}$ is also in H, and every τ' in H arises in this way. Thus for every b in L,

$$\tau'\sigma(b) = \sigma\tau(b) = \sigma(b),$$

so that $\sigma(b)$ is fixed by every τ' in H, i.e., $\sigma(b)$ is again in L. Therefore the action of $N_G(H)$ on F maps L back into itself. So there is a homomorphism from $N_G(H)$ to $\text{Aut}(L/E)$. By the definition of L, the kernel of this homomorphism is H. Thus there is an injective homomorphism $N_G(H)/H \to \text{Aut}(L/E)$. The claim is that every E-automorphism $\theta : L \to L$ is in the image of this homomorphism, i.e., this homomorphism is an isomorphism.

Every E-automorphism $\theta : L \to L$ determines an F-algebra automorphism,

$$\text{Id}_F \otimes \theta : F \otimes_E L \to F \otimes_E L, \quad c \otimes b \mapsto c \otimes \theta(b).$$

And this F-algebra automorphism commutes with the left G-action by $\widehat{\sigma}\cdot$. Of course we can recover θ for $\text{Id}_F \otimes \theta$ by applying this to elements of the form $1 \otimes b$. So the number of E-automorphisms of L is no greater than the number of F-algebra automorphisms of $F \otimes_E L$ which commute with the left G-action. Using T, every such automorphism is equivalent to an F-algebra automorphism of the F-subalgebra $F^{G/H}$ of F^G which commutes with the left G-action by $\widetilde{\sigma}\cdot$. By Corollary 1.8, every automorphism of $F^{G/H}$ is of the form F^t for a unique bijection $t : G/H \to G/H$. Finally, since θ commutes with the left G-action on $F \otimes_E L$, t commutes with the left G-action on G/H. Thus, by Proposition 1.10, there exists a unique coset k_0H in $N_G(H)/H$ such that $t(kH) = kk_0H$ for every kH in G/H. Therefore the number of such automorphisms is bounded by $[N_G(H) : H]$. But we already produced an injective homomorphism from $N_G(H)/H$ into the group of such automorphisms. Therefore this injective homomorphism is an isomorphism, i.e., $\text{Aut}(L/E)$ equals $N_G(H)/H$.

In particular, since $[L:E]$ equals $[G:H]$, the size of $\text{Aut}(L/E)$ equal $[L:E]$ if and only if $N_G(H)$ equals all of G, i.e., if and only if H is normal in G. Therefore, using Theorem 2.2 once more,

E equals $\mathrm{Fix}^{\mathrm{Aut}(L/E)}(L)$ if and only if H is normal in G, i.e., L/E is Galois if and only if H is a normal subgroup of G. And in this case $\mathrm{Aut}(L/E)$ equals $N_G(H)/H$. $\square$