Grothendieck's Galois Theory / Finite Étale Algebras

Goal: Introduce another generalization of the classical (finite) Galois correspondence. This will turn out to have a nice analoguous statement in the theory of covering spaces.

Consider a field k and choose algebraic and separable closures $k \subset k_s \subset \bar{k}$. We will develop the theory for the Galois extension $k_s | k$ without losing any generality, as this restricts to the arbitrary case.
Recall that for a finite extension $L|k$ of degree n, we have at most n distinct morphisms $\varphi: L \to \bar{k}$ over k. The extension is separable if and only if we have exactly n such homomorphisms.
In this case the image of φ is actually in k_s, hence we get that $\mathrm{Hom}_k(L, k_s) = \mathrm{Hom}_k(L, \bar{k})$ has n elements.
Composition gives a left action of $\mathrm{Gal}(k) := \mathrm{Gal}(k_s|k)$ on $\mathrm{Hom}_k(L, k_s)$.
We claim that this action is continuous.
Recall: If G is a topological group acting on a topological space X from the left we call the action continuous if the multiplication map $m: G \times X \to X$, $m(g,x) = gx$ is continuous.

Lemma: Let G be a topological group acting on a discrete space X. Then the action is continuous if and only if the stabilizer $G_x = \{g \in G \mid gx = x\}$ is open in G for each $x \in X$.
Pf: Suppose $m: G \times X \to X$ is continuous. For $x \in X$, composing m with the continuous map $\varphi: G \to G \times X$, $\varphi(g) = (g, x)$, yields that $G_x = (m \circ \varphi)^{-1}(x)$ is open.
Conversely, if G_x is open for each $x \in X$, consider $U = m^{-1}(x) = \{(g,y) \in G \times X \mid gy = x\}$.
This is the disjoint union of the sets $U_y := \{(g,y) \in G \times \{y\} \mid gy = x\}$.
If U_y is non-empty, choose $h \in G$ with $hy = x$. The map $\psi: G \to G \times X$ given by $\psi(g) = (gh, y)$ restricts to a homeomorphism $G \cong G \times \{y\}$. Further, $\psi(G_x) = U_y$, so U_y and hence also U is open in $G \times X$.

<u>Lemma 1.5.1</u> Let $L|k$ be a finite and separable extension. The action of $Gal(k)$ on $Hom_k(L, k_s)$ is continuous and transitive. Hence, as a $Gal(k)$-set, $Hom_k(L, k_s)$ is isomorphic to the coset space of some open subgroup of $Gal(k)$. If L is Galois over k, this is a quotient by an open normal subgroup.

Pf Let $\varphi \in Hom_k(L, k_s)$ and write $G = Gal(k)$. $G_\varphi = \{\sigma \in Gal(k) \mid \sigma\varphi = \varphi\}$ is isomorphic to $Gal(k_s|L)$ which is a closed subgroup of G with finite index, hence it is open. By the previous lemma, this implies that the action is continuous.

Since L is finite and separable over k we can choos a primitive element α that generates L and denote its minimal polynomial by f. We have a bijective correspondence between k-algebra homomorphisms $L \to k_s$ and roots of f in k_s. Since G acts transitively on the roots of f, this gives transitivity of the action.

For the second part, take $\varphi \in Hom_k(L, k_s)$ and consider the open subgroup G_φ as well as the map

$$\begin{aligned} Hom_k(L, k_s) &\longrightarrow G_\varphi \backslash G \\ g \circ \varphi &\longmapsto g G_\varphi \end{aligned}$$

This is well defined, as $g \circ \varphi = g' \circ \varphi$ implies $g^{-1} g' \varphi = \varphi$, hence $g' \in g G_\varphi$.

Surjectivity of this map is obvious from its definition, so we are left with checking injectivity.

If $g G_\varphi = g' G_\varphi$, one can find $h \in G_\varphi$ with $g' h = g$. ~~so g φ = g' h~~

We get $g\varphi = g' h \varphi = g' \varphi$, showing injectivity.

So $Hom_k(L, k_s)$ is indeed isomorphic to a coset space.

Finally, if L is Galois over k, we know by Krull's theorem that G_φ is normal, hence the above coset is the quotient G/G_φ $\square$

Note that a k-algebra homomorphism $\varphi: L \to M$ of finite separable extensions induces a map $\varphi^*: \mathrm{Hom}_k(M, k_s) \to \mathrm{Hom}_k(L, k_s)$ which is $\mathrm{Gal}(k)$-equivariant. Hence we get a contravariant functor

$$\mathrm{Hom}_k(-, k_s): \mathrm{FSep}_k \longrightarrow t\mathrm{G\text{-}Set}$$

<u>Thm 1.5.2</u> Let k be a field with a separable closure k_s. Then the functor $\mathrm{Hom}_k(-, k_s)$ gives an anti-equivalence between the category of finite and separable extensions over k, and the category of finite sets with continuous and transitive left $\mathrm{Gal}(k)$-action. Galois extensions give rise to $\mathrm{Gal}(k)$-sets isomorphic to a finite quotient of $\mathrm{Gal}(k)$.

Pf We already showed the last part in the lemma, so we only need to check that $\mathrm{Hom}_k(-, k_s)$ is fully faithful and essentially surjective.

<u>Essential surjectivity:</u>

Let S be a finite set with continuous and transitive left G-action. Choose any $s \in S$ and consider the stabilizer G_s. Let $i: L \hookrightarrow k_s$ be the field fixed by G_s. Considering i as an element in $\mathrm{Hom}_k(L, k_s)$, one has $G_i = G_s =: H$. Repeating the argument from before gives $\mathrm{Hom}_k(L, k_s) \cong H \backslash G \cong S$.

Fully faithfullness:

Let L and M be finite and separable extensions of k. We claim that $\mathrm{Hom}_k(-,k_s)$ induces an isomorphism

$$\mathrm{Hom}_k(L,M) \xrightarrow{\sim} \mathrm{Hom}_G(\mathrm{Hom}_k(M,k_s),\mathrm{Hom}_k(L,k_s))$$

Choose and fix $\varphi \in \mathrm{Hom}_k(M,k_s)$. By transitivity, any G-equivariant map $f: \mathrm{Hom}_k(M,k_s) \to \mathrm{Hom}_k(L,k_s)$ is determined by $f(\varphi)$. Since elements of G_φ also fix $f(\varphi)$ one has $G_\varphi \subset G_{f(\varphi)}$. Taking the fixed subfields of k_s induced by these groups gives a map $i: f(\varphi)(L) \hookrightarrow \varphi(M)$. On its image, φ has an inverse $\psi: \varphi(M) \to M$, hence we can define $\Phi: \psi \circ i \circ f(\varphi): L \to M$. Composing with Φ maps φ to $f(\varphi)$, hence induces the map f. By construction it is the unique map in $\mathrm{Hom}_k(L,M)$ with this property. $\square$

Next we want to lift the transitivity restriction.

$\rightsquigarrow$ What corresponds to arbitrary finite sets with continuous $\mathrm{Gal}(k)$-action?

Def A finite dimensional k-algebra is étale over k if it is isomorphic to a finite direct product of separable extensions of k.

Thm 1.5.4 (Main theorem of Galois theory - Grothendieck's version)

The functor $\mathrm{Hom}_k(-,k_s): \mathrm{F\acute{E}t}_k \to G\text{-Set}$ gives an anti-equivalence between the category of finite étale algebras over k and the category of finite sets with continuous $\mathrm{Gal}(k)$-action.

Separable field extensions give rise to sets with transitive $\mathrm{Gal}(k)$-action and Galois extensions induce $\mathrm{Gal}(k)$-sets isomorphic to finite quotients of $\mathrm{Gal}(k)$.

Pf Observe that for $A = \prod L_i$, a product of field extensions over k any k-algebra homomorphism $A \xrightarrow{\varphi} k_s$ is given by $L_i \hookrightarrow k_s$ for exactly one L_i:

- If $\varphi(L_i) \neq 0$, then L_i injects into k_s
- If one had $1_i \in L_i$, $1_j \in L_j$ with $\varphi(1_i) \neq 0$ and $\varphi(1_j) \neq 0$, then $\varphi(1_i)\varphi(1_j) = \varphi(0) = 0$.
  But since k_s is a field it has no zero divisors.

Therefore $\mathrm{Hom}_k(A, k_s) = \coprod \mathrm{Hom}_k(L_i, k_s)$ and these sets are exactly the orbits of the action of G on $\mathrm{Hom}_k(A, k_s)$ if A is étale. This gives essential surjectivity.

For two finite étale k-algebras $A = \prod L_i$, $A' = \prod L_j'$ one has

$$\mathrm{Hom}_k(A, A') = \mathrm{Hom}_k\Big(\prod_i L_i, \prod_j L_j'\Big) \cong \prod_j \mathrm{Hom}_k\Big(\prod L_i, L_j'\Big) \cong \prod_j \coprod_i \mathrm{Hom}_k(L_i, L_j')$$

and on the other hand

$$\mathrm{Hom}_G(\mathrm{Hom}_k(A', k_s), \mathrm{Hom}_k(A, k_s)) \cong \mathrm{Hom}_G\Big(\coprod_j \mathrm{Hom}_k(L_j', k_s), \coprod_i \mathrm{Hom}_k(L_i, k_s)\Big)$$

$$\cong \prod_j \mathrm{Hom}_G\Big(\mathrm{Hom}_k(L_j', k_s), \coprod_i \mathrm{Hom}_k(L_i, k_s)\Big) \cong \prod_j \coprod_i \mathrm{Hom}_G(\mathrm{Hom}_k(L_j', k_s), \mathrm{Hom}_k(L_i, k_s))$$

where the last isomorphism holds since we decomposed the sets into transitive subsets.

By the previous theorem we now get fully faithfulness $\square$

Note that for an arbitrary Galois extension $K|k$, one can restrict the above to get an anti-equivalence between the finite étale k-algebras consisting of subfields of K and finite sets with continuous left $\mathrm{Gal}(K|k)$-action.

We conclude with a characterization of finite étale algebras:

Prop 1.5.6 Let A be a finite dimensional commutative algebra over a field k. Then the following are equivalent:

1. A is étale
2. $A \otimes_k \bar{k}$ is isomorphic to $\bar{k}^n$ for some $n \in \mathbb{N}$
3. $A \otimes_k \bar{k}$ is reduced, i.e has no nilpotent elements.

To this aim we need one more result:

Lemma 1.5.7 A finite dimensional commutative algebra A over a field F is isomorphic to a product of finite field extensions of F if and only if it is reduced.

Pf „$\Rightarrow$" is obvious.

„$\Leftarrow$": If A is the (finite) product of k-algebras we can check the statement on each factor, therefore we may assume that A cannot be written as a (non-trivial) product of k-algebras. This implies that A has no other idempotents than 0 and 1. Indeed, if $e \neq 0,1$ has $e^2 = e$, then $A \cong Ae \times A(1-e)$ would be a nontrivial product.

We are done if we can show that A is a field, so we want an inverse for any nonzero $x \in A$. Since A is finite dimensional, the chain of ideals $(x) \supset (x^2) \supset (x^3) \supset \dots$ terminates, i.e. we can find $n \in \mathbb{N}$ and $y \in A$ with $x^n = x^{n+1} y = x x^n y = x^{n+2} y^2 = \dots = x^{2n} y^n$. Multiplying with y^n gives $x^n y^n = (x^n y^n)^2$, hence $x^n y^n$ is either 0 or 1. If $x^n y^n = 0$, then also $x^n = x^n (x^n y^n) = 0$, which contradict the assumption that A is reduced. So $x^n y^n = 1$, in particular x has an inverse. $\square$

Pf of 1.5.6 2 => 3: is obvious

3 => 2: Since $A \otimes_k \bar{k}$ is a reduced commutative algebra over $\bar{k}$, the lemma implies that it can be written as a finite product of finite field extensions. But the only finite field extension of $\bar{k}$ is $\bar{k}$ itself.

1 => 2: Tensoring commutes with finite products, therefore we may assume $A = L$ to be a finite separable extension of k. So we can find $f \in k[x]$ such that $L = k[x]/(f)$ and with coefficients in $\bar{k}$ one has $f(x) = \prod_{i=1}^{n} (x - \alpha_i)$ for some $\alpha_i \in \bar{k}$. Then

$$L \otimes_k \bar{k} \cong \bar{k}[x]/(f) = \bar{k}[x]/\prod(x-\alpha_i) \cong \prod_{i=1}^{n} \bar{k}[x]/(x-\alpha_i) \cong \prod_{i=1}^{n} \bar{k}$$

Where we made use of the chinese remainder theorem.

$2 \Rightarrow 1$: Let $I \subset A$ be the ideal generated by the nilpotent elements of A and set $A' := A/I$. By the lemma we can write A' as the finite product of finite field extensions L_i of k. Again, any map $A' \to \bar{k}$ is given by a mophism $L_i \to \bar{k}$ from one of the factors.

Any map $A \to \bar{k}$ factors through A' as $\bar{k}$ is reduced, by the remark just given it even factors through some $L_i \to \bar{k}$.

We know $|\mathrm{Hom}_k(L_i, \bar{k})| \leq [L_i : k]$ with equality exactly when the extension is separable. With the previous observation in mind, we have that $|\mathrm{Hom}_k(A, \bar{k})| \leq \dim_k(A)$ and equality holds if and only if $A = A'$ and A is étale.

So we finish by showing $|\mathrm{Hom}_k(A, \bar{k})| = \dim_k(A)$. For this note that we have a bijection

$$\begin{aligned} \mathrm{Hom}_k(A, \bar{k}) &\longrightarrow \mathrm{Hom}_{\bar{k}}(A \otimes_k \bar{k}, \bar{k}) \\ \varphi &\longmapsto [a \otimes b \mapsto \varphi(a) b] \\ [A \cong A \otimes_k k \to A \otimes_k \bar{k} \xrightarrow{\psi} \bar{k}] &\longleftarrow\!\shortmid \ \psi \end{aligned}$$

One concludes

$$|\mathrm{Hom}_k(A, \bar{k})| = |\mathrm{Hom}_{\bar{k}}(A \otimes_k \bar{k}, \bar{k})| = \dim_{\bar{k}}(A \otimes_k \bar{k}) = \dim_k(A) \quad \square$$