Grothendieck's Galois Theory

Gabriele Rastello

November 29, 2020

Contents

1 Introduction

The Fundamental Theorem of Galois Theory is an old and profound result of field theory. In modern terms it establishes a one-to-one correspondence between the subextensions of a finite Galois extension of a field and the subgroups of the Galois group of that extension. A statement and a "classical" proof of this theorem can be found in [3].

Another similar result, this time in algebraic topology, is the Fundamental Theorem of Covering Theory. This theorems states the existence of a one-to-one correspondence between subgroups of the fundamental group and path-connected covering spaces of a path-connected topological space.

The two statements, at least on an intuitive level, have something in common. Intrigued by this curious fact and moved by a belief that this is no coincidence Grothendieck was able to prove a theorem (here Theorem 3.8) that has both of them as consequences; thus unifying the matter[1]. In this pages we will explore Grothendieck's approach following closely [1], but with some added details (mostly confined in the appendix).

The reader is assumed to have a basic knowledge of category theory (categories, functors, natural transformations, adjoint functors, some (co)limits) and of group actions (mostly about transitive actions).

[1] It is noteworthy to say that Grothendieck went even further than that and was able to prove an even more general theorem that, even for the classical case of fields, yields results that weren't previously known. However, we will stick to the base case here; the interested reader can check [1] section IV and V.

2 Group actions and adjoints

Definition 2.1. In a category $\mathscr{C}$ an arrow $f\colon X \to Y$ is a **strict epimorphism** if it is the joint coequalizer of all the pairs of arrows it coequalizes. This means that any arrow $g\colon X \to Z$ such that $g \circ x = g \circ y$ for all $x, y\colon C \to X$ such that $f \circ x = f \circ y$ there exists a unique arrow $h\colon Y \to Z$ such that $h \circ f = g$. Refer to Figure 2.1.

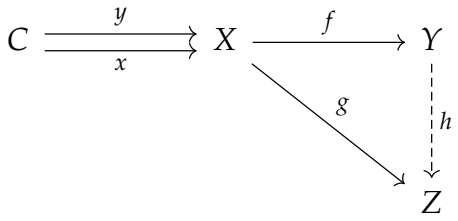


Figure 2.1

Remark 2.2. Strict epimorphisms are epimorphisms, as the name implies.

Remark 2.3. If an arrow is both a stric epimorphism and a monomorphism then it is an isomorphism.

Definition 2.4. Let H be a group, A an object of $\mathscr{C}$ and $G = \mathrm{Aut}(A)$ the group of automorphisms of A in $\mathscr{C}$ i.e. the group whose underlying set is the set of isomorphisms of type $A \to A$ of $\mathscr{C}$ and whose operation is composition in $\mathscr{C}$. An **action** of H on A is a group homomorphism $H \to G$.

Notation 2.5. Given an action of a group H on an object A of $\mathscr{C}$ we denote, with a slight abuse of notation, the automorphism of A associated to $h \in H$ by the same symbol h.

Definition 2.6. If H acts on A as defined in 2.4 we define the quotient of A by H in $\mathscr{C}$ to be an element A/H of $\mathscr{C}$ equipped with an arrow $q\colon A \to A/H$ such that:

(1) for all $h \in H$ we have $q \circ h = q$,

(2) for any $x\colon A \to X$ such that $x \circ h = x$ for all $h \in H$ there exists a unique arrow $\varphi\colon A/H \to X$ such that $x = \varphi \circ q$.

See also Figure 2.2.

Remark 2.7. Quotients are defined by a universal property, thus are unique up to unique isomorphism and we can speak of "the" quotient of A by H instead of "a" quotient of A by H.

Notation 2.8. Sometimes we use the sentence "the quotient of A by H" to refer to the object A/H, some others to the arrow $q\colon A \to A/H$; the context should be enough to differentiate between the two.

Remark 2.9. Consider a quotient $q\colon A \to A/H$; by condition (1) above $q \circ h = q = q \circ 1_A$ so q coequalizes all the pairs $(h, 1_A)$, for $h \in H$. If another arrow $x\colon A \to X$ coequalizes all the pairs that q does then this arrow is such that $x \circ h = x \circ 1_A = x$ for all $h \in H$ and thus, by condition (2), we have a unique factorization $x = \varphi \circ q$. This proves that all quotients are strict epimorphisms.

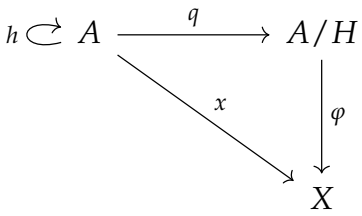


Figure 2.2

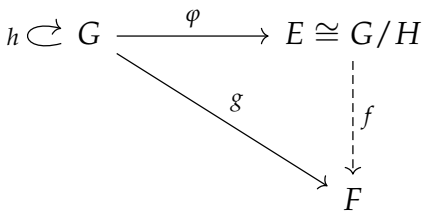


Figure 2.3

Notation 2.10. Let G be a group, then with **GSet** we denote the category of G-sets and G-invariant maps.

Remark 2.11. Consider **GSet**. The underlying set of G (that we also denote with G) is a G-set with the action given by left multiplication; we call this the **canonical action** of G on itself. Let $\varphi\colon G \to E$ be a G-invariant map; it is easy to see that such a φ, by virtue of being G-invariant, is determined uniquely by the value $\varphi(e)$, where e is the neutral element of G.

Let now E be a transitive G-set i.e. such that $E/G = \{*\}$ in **Set**[2]. Fix an $x \in E$ and let φ be the G-invariant map defined by $\varphi(e) = x$; we argue that $\varphi\colon G \to E$ makes E into a quotient of G by the subgroup

$$H = \mathrm{Fix}(x) = \{g \in G\colon g \cdot x = x\}.$$

Indeed by using the definition of H and the fact that φ is G-invariant we have

$$(\varphi \circ h)(e) = \varphi(h \cdot e) = h \cdot \varphi(e) = h \cdot x = x.$$

for all $h \in H$. Moreover let $g\colon G \to F$ satisfy (1) of Definition 2.6; as we discussed above g is entirely determined by the image of e so we obtain (2) defining an arrow $f\colon E \to F$ by $f(x) = g(e)$. The situation is depicted in Figure 2.3.

Finally: G is a transitive G-set and so is every G/H with $H \leq G$ and the action defined again by left multiplication (on cosets) so an object $E \in$ **GSet** is transitive if and only if it is isomorphic to some G/H.

For the rest of the section fix a category $\mathscr{C}$, an object $A \in \mathscr{C}$ and let $G = \mathrm{Aut}(A)$.

[2]This states that the set of orbits of E is a singleton that is of course the case if and only if E is transitive.

Remark 2.12. Consider a subgroup $H \leq G$ and an object $X \in \mathscr{C}$. H acts on the hom-set $[A, X]$ as follows[3]:

$$\begin{array}{rcl} H \times [A, X] & \longrightarrow & [A, X] \\ (h, x) & \longmapsto & h \cdot x = x \circ h. \end{array}$$

Remark 2.13. Assume that the action $G \times [A, X] \to [A, X]$ is transitive and let $\mathbf{GSet}^t$ be the category of transitive G-sets (a subcategory of G*set*). Then we have a functor

$$\begin{array}{rccc} [A, -]_G \colon & \mathscr{C} & \longrightarrow & \mathbf{GSet}^t \\ & X & & [A, X]_G \\ & \Big\downarrow f & \longmapsto & \Big\downarrow f_* \\ & Y & & [A, Y]_G \end{array}$$

where we indicate with $[A, X]_G$ the hom-set $[A, X]$ upon which G acts as described in Proposition 2.12 and f_* is post-composition with f. It is easy to check that f_* is indeed G-invariant.

Remark 2.14. Consider an object $E \in \mathbf{GSet}^t$, pick an element $x_0 \in E$ and let $H = \mathrm{Fix}(x_0) \leq G$ (the choice of x_0 is irrelevant as E is transitive). Moreover assume that $\mathscr{C}$ has quotients of A by any subgroup of G.

By what we observed in Remark 2.11 we have a bijection between elements of E and arrows of type $G \to E$. Consider then $f \in [A, X]_G$ and its corresponding arrow $\varphi \colon G \to [A, X]_G$; we claim that f factors through A/H if and only if φ factors through $E \cong G/H$ (see Figure 2.4). Indeed f factors if and only if $f \circ h = f$ for all $h \in H$, by using the fact that φ is G-invariant we obtain

$$\varphi(h \cdot e) = h \cdot \varphi(e) = h \cdot f = f \circ h = f$$

and, since φ is uniquely determined by $\varphi(e)$, $\varphi \circ h = \varphi$ for all $h \in H$; this happens if and only if φ factors through $E \cong G/H$.

This gives us, for each $X \in \mathscr{C}$ and $E \in \mathbf{GSet}^t$, a bijection

$$[A/H, X] \cong \mathbf{GSet}^t(E, [A, X]_G) \qquad (*)$$

natural in X in E (see Section 5).

Provided that $\mathscr{C}$ has quotients of A by subgroups of G we can define a functor $A \times_G -$ from $\mathbf{GSet}^t$ to $\mathscr{C}$ by setting $A \times_G E = A/H$ for $H = \mathrm{Fix}(x_0)$ and $x_0 \in E$ as above. The behaviour of $A \times_G -$ on arrows is defined as follows. Let $f \colon E \cong G/H \to F \cong G/H'$ be an arrow in $\mathbf{GSet}^t$ with $H = \mathrm{Fix}(x_0)$, $H' = \mathrm{Fix}(f(x_0))$ and $x_0 \in E$. Notice that for all $h \in H$ we have $f(h \cdot x_0) = f(x_0)$ by definition of H and $f(h \cdot x_0) = h \cdot f(x_0)$ by G-invariance of f; thus $H \leq H'$. This means that if $q \colon A \to A/H$ and $q' \colon A \to A/H'$ are the quotients in $\mathscr{C}$ there is a unique arrow $\tilde{f} \colon A/H \to A/H'$ such that $q' = \tilde{f} \circ q$; we set $A \times_G f = \tilde{f}$.

Finally the naturality of the bijection $(*)$ now indicates that we have an adjunction

$$A \times_G - \dashv [A, -]_G.$$

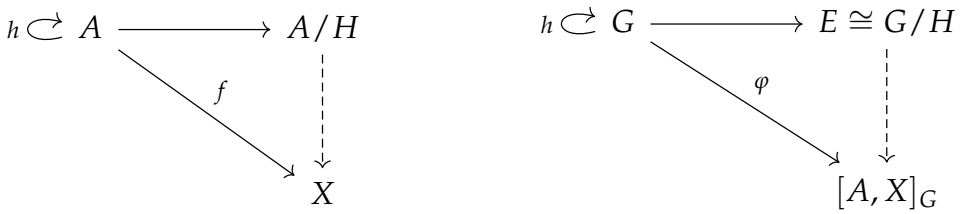


Figure 2.4

Our main problem will be that of finding conditions on $\mathscr{C}$ that make this adjunction into an equivalence of categories.

3 Categorial axiomatization of Galois Theory

Through this section fix a category $\mathscr{C}$ and an object $A \in \mathscr{C}$.

Definition 3.1. We define the following axioms.

(1) For every $X \in \mathscr{C}$ there is at least a map of type $A \to X$ and all maps $A \to X$ are strict epimorphisms.

(2) For any subgroup $H \leq \mathrm{Aut}(A)$ the quotient $q\colon A \to A/H$ exists and is preserved by $[A, -]\colon \mathscr{C} \to \mathbf{GSet}$.

(3) Every endomorphism of A is an isomorphism i.e. $[A, A] = \mathrm{Aut}(A)$.

Remark 3.2. It is known that if $f \circ g$ is a strict epimorphism then so is f. Thus it follows from Axiom (1) that every arrow $X \to Y$ in $\mathscr{C}$ is a strict epimorphism.

Proposition 3.3. Axiom (1) implies that $[A, -]$ is faithful, reflects monomorphisms and isomorphisms.

Proof. Consider arrows $f, g\colon X \to Y \in \mathscr{C}$ such that $[A, f] = [A, g]$; that is $f_* = g_*$. By Axiom (1) let $h\colon A \to X$ be a third arrow of $\mathscr{C}$ then we have $f_*(h) = g_*(h)$ i.e. $f \circ h = g \circ h$. Again by Axiom (1) h is an epimorphism (really, a strong one) and thus we obtain $f = g$; that is: $[A, -]$ is faithful.

It is well known that every faithful functor reflects monomorphisms. Because of this if $f \in \mathbf{GSet}$ is an isomorphism and $g \in \mathscr{C}$ is such that $[A, g] = f$ then g is a monomorphism too; but, as an arrow of $\mathscr{C}$, g is also a strict epimorphism and thus an isomorphism. □

Remark 3.4. Consider $H \leq G$ and the quotient $q\colon A \to A/H$ in $\mathscr{C}$, then $q_*\colon [A, A] \to [A, A/H]$ in **GSet** is a quotient too because quotients are preserved by $[A, -]$ (Axiom (2)). Thus we have $[A, A]/H \cong [A, A/H]$, and the diagram in Figure 3.5 commutes (where ρ is a quotient arrow and η the isomorphism).

Isomorphisms in **GSet** are bijections so:

(i) for $f, g \in [A, A]$ if $q \circ f = q \circ g$ then there is some $h \in H$ such that $f = h \circ g$,

[3]Since an action as of Definition 2.4 is a map that sends elements of a group to arrows it is, in this case, equivalent to give the definition of an action by uncurrying.

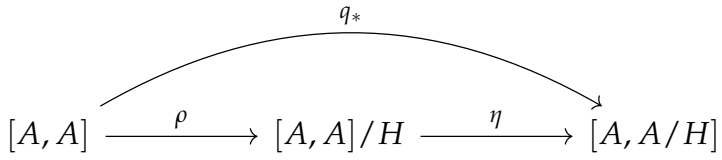


Figure 3.5

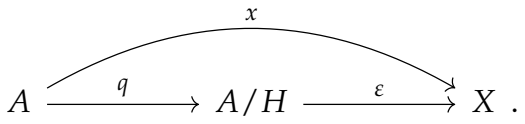


Figure 3.6

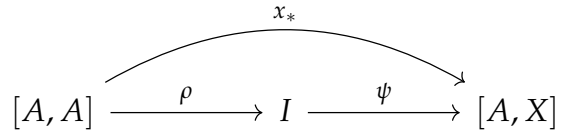
(ii) for all $x\colon A \to A/H$ there is an arrow $f \in [A,A]$ such that $q \circ f = x$.

Moreover, under Axiom (3), (i) implies the following:

(iii) $q \circ f = q$ implies $f \in H$.

Indeed by taking $g = 1_A$ in (i) we obtain that $f = h$ for some $h \in H$.

Remark 3.5. Consider an arrow $x\colon A \to X$ and the epi-mono factorization $x_* = \psi \circ \rho$[4]. With reference to the diagram below Axiom (3) implies that $I = [A,A]/H$ with $H = \mathrm{Fix}(x) \leq G$.



Indeed by Axiom (3) $[A,A] = G$ so an arrow from $[A,A]$ is determined by its behaviour on 1_A. Now

$$(\psi \circ \rho \circ h)(1_A) = x_*(1_A \circ h) = x \circ h = x = x_*(1_A) = (\psi \circ \rho)(1_A)$$

that is $\psi \circ \rho \circ h = \psi \circ \rho$ which, by monicness of ψ, implies $\rho \circ h = \rho$. This makes ρ into a quotient.

Proposition 3.6. Any arrow $x\colon A \to X$ of $\mathscr{C}$ is a quotient of A by $H = \mathrm{Fix}(x) \leq G$ (with respect to the action on $[A,X]$ described in Remark 2.12) i.e. $X = A/H$.

Proof. By choosing $H = \mathrm{Fix}(x)$ we get $x \circ h = x$ for all $h \in H$ and thus there is a unique arrow $\varepsilon\colon A/H \to X$ of $\mathscr{C}$ such that $x = \varepsilon \circ q$, where $q\colon A \to A/H$ is the quotient of A by H (see Figure 3.6).

By applying $[A,-]$ we obtain Figure 3.7 where ρ, ψ and η are as discussed before. We have

$$\varepsilon_* \circ \eta \circ \rho = \varepsilon_* \circ q_* = x_* = \psi \circ \rho$$

that by epicness of ρ implies $\varepsilon_* \circ \eta = \psi$. Now ε_* must be monic since ψ and η are; but this, by Proposition 3.3, implies that $\varepsilon \in \mathscr{C}$ is monic too. Being an arrow of $\mathscr{C}$, by Axiom (i), ε is also a strict epimorphism and thus an isomorphism. □

[4]We recall that **GSet** is a topos and, as such, has epi-mono factorization. The interested reader can find evidence of both facts in [4].

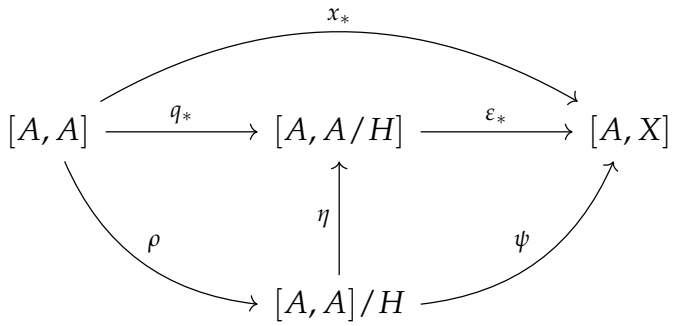


Figure 3.7

Proposition 3.7. The action of $\mathrm{Aut}(A)$ on $[A, X]$ is transitive for all $X \in \mathscr{C}$.

Proof. Consider again Figure 3.7. We proved that ε is an isomorphism and thus ε_* must be one too. Moreover from Remark 3.4 we know η is iso too and so we have $[A, X] \cong [A, A]/H$, but by Axiom (3) $[A, A] = \mathrm{Aut}(A)$ and so we have that $[A, X]$ is transitive. □

Theorem 3.8. Given a category $\mathscr{C}$ and an object $A \in \mathscr{C}$ such that Axioms (1), (2) and (3) hold there exists an adjunction

$$A \times_G - \dashv [A, -]_G$$

where $G = \mathrm{Aut}(A)$ such that the maps

$$\eta \colon E \cong [A, A]/H \to [A, A/H]$$

$$\varepsilon \colon A/H \to X$$

are isomorphisms. This enstablishes an equivalence of categories between $\mathscr{C}$ and $\mathbf{GSet}^t$.

Proof. The existence of the adjunction follows from the discussion in Section 2, the fact that η and ε are (the components of) the unit and counit of the andjunction is a calculation that has been moved to the appendix and the fact that they are isomorphisms follows respectively from Remark 3.4 and Proposition 3.6. □

4 Conclusion

Let k be a field and E a finite Galois extension of k. Let $\mathscr{C}$ be the opposite category of the category of subextensions of E (with arrows restricted to the field homomorphisms that fix the base field k) then it is possible to prove that $\mathscr{C}$ satisfies Axioms (1), (2) and (3) with $A = E$. Indeed:

- Axiom (3) is trivially satisfied and $G = \mathrm{Aut}(A, A)$ is the Galois group of E,
- Axiom (2) is satisfied as one can check that, for each $H \leq G$ the fixed field

  $$E^H = \{x \in E \colon \forall h \in H \; h(x) = x\}$$

  is the quotient of E by H in $\mathscr{C}$[5],

[5] If we prefer to work in the original category of subextensions (not in the dual) this means that E^H is the coquotient of E by H.

- Axiom (1) is satisfied because in the category of subextensions of E every object has an arrow to E and every such arrow is a strict monomorphism.

We can then apply Theorem 3.8 to obtain that $\mathscr{C}$ and $\mathbf{GSet}^t$ are equivalent. The correspondance of Galois can then be retrieved by associating to each $F \in \mathscr{C}$ the subgroup $H \leq G$ such that the transitive G-set G/H is precisely the G-set associated to F by the equivalence above.

Theorem 3.8 can also be used to give alternative proofs of other well-known results (such as the corespondence between subgroups of the fundamental group and path-connected covering spaces of a path-connected topological space) that intuitively share some similarities with the case of Galois Theory. Indeed the most beautiful part about this theorem is that, through its very abstract nature, is able to clearly identify, capture and unify these "intuitive similarities" that different pieces of mathematics posses[6].

5 Appendix

5.1 Naturality of $[A/H, X] \cong \mathbf{GSet}^t(E, [A, X]_G)$

Fix a category $\mathscr{C}$, an element $A \in \mathscr{C}$ and let $G = \mathrm{Aut}(A)$. Let's indicate with ψ_{EX} the bijection between $[A/H, X]$ and $\mathbf{GSet}^t(E, [A, X]_G)$ described in Remark 2.14; we shall prove that it is natural in both $X \in \mathscr{C}$ and $E \in \mathbf{GSet}^t$.

Naturality in X. Given an arrow $f\colon X \to Y$ of $\mathscr{C}$ we want to prove that the ψ_{EX} are the components of a natural transformation $[A/H, -] \Rightarrow \mathbf{GSet}^t(E, [A, -]_G)$ i.e that the following diagram commutes.

$$\begin{array}{ccc} [A/H, X] & \xrightarrow{\psi_{EX}} & \mathbf{GSet}^t(E, [A, X]_G) \\ \downarrow{\scriptstyle f_*} & & \downarrow{\scriptstyle (f_*)_*} \\ [A/H, Y] & \xrightarrow{\psi_{EY}} & \mathbf{GSet}^t(E, [A, Y]_G) \end{array}$$

Recall that here $H = \mathrm{Fix}(x_0)$ for $x_0 \in E$. Pick any $x \in [A/H, X]$ and let $q\colon A \to A/H$ be the quotient arrow (the quotient exists because $\mathscr{C}$ is assumed to have all quotients by subgroups of G); then chasing x through the diagram down the two possible ways yields two arrows in $\mathbf{GSet}^t$ of type $E \to [A, Y]_G$. Since E is transitive arrows out of E are determined uniquely by the image of x_0; keeping this in mind the following computations show that the square commutes.

$$((f_*)_* \circ \psi_{EX})(x)(x_0) = (f_* \circ \psi_{EX}(x))(x_0) = f_*(\psi_{EX}(x)(x_0)) = f_*(x \circ q) = f \circ x \circ q$$

$$(\psi_{EY} \circ f_*)(x)(x_0) = \psi_{EX}(f \circ x)(x_0) = f \circ x \circ q$$

□

[6] Arguably this is the goal of category theory as a whole, making this particular theorem into a quintessential example.

Naturality in E. We want to prove that the ψ_{EX} are the components of a natural transformation $[A/-, X] \Rightarrow \mathbf{GSet}^t(-, [A, X]_G)$. Given $f\colon E \cong G/H \to F \cong G/H'$ with $H = \mathrm{Fix}(x_0), H' = \mathrm{Fix}(f(x_0)), x_0 \in E$, using the notation $\tilde{f} = A \times_G f$ (see Remark 2.14), we show the naturality of the following square.

$$\begin{array}{ccc} [A/H, X] & \xrightarrow{\psi_{EX}} & \mathbf{GSet}^t(E, [A, X]_G) \\ \uparrow{\scriptstyle \widetilde{f}^*} & & \uparrow{\scriptstyle f^*} \\ [A/H', X] & \xrightarrow{\psi_{FX}} & \mathbf{GSet}(F, [A, X]_G) \end{array}$$

As before we chase an $x \in [A/H', X]$ down the two possible paths to get two arrows of type $E \to [A, X]_G$ and prove that they are the same by evaluating them on $x_0 \in E$:

$$(\psi_{EX} \circ \widetilde{f}^*)(x)(x_0) = \psi_{EX}(x \circ \widetilde{f})(x_0) = x \circ \widetilde{f} \circ q = x \circ q',$$

$$(f^* \circ \psi_{FX})(x)(x_0) = (\psi_{FX}(x) \circ f)(x_0) = \psi_{FX}(x)(f(x_0)) = x \circ q'.$$

□

5.2 η and ε are the unit and counit of $A \times_G - \dashv [A, -]_G$

η is the unit. Our adjunction is given by the bijection

$$\psi\colon \mathscr{C}(A \times_G E, X) \cong \mathbf{GSet}^t(E, [A, X]_G)$$

natural in $X \in \mathscr{C}$ and $E \in \mathbf{GSet}^t$. To obtain the unit we set $X = A \times_G E$:

$$\mathscr{C}(A \times_G E, A \times_G E) \cong \mathbf{GSet}^t(E, [A, A \times_G E]_G)$$

and so

$$\mathscr{C}(A/H, A/H) \cong \mathbf{GSet}^t(E, [A, A/H]_G)$$

where $H = \mathrm{Fix}(x) \leq G$ ($x \in E$) by definition of $A \times_G E$. Now (the component at E of) the unit is given by the image of $1_{A/H}$ under this bijection. By the discussion in Section 2 if $q\colon A \to A/H$ is the quotient arrow in $\mathscr{C}$ then $\psi(1_{A/H})$ is the map $E \cong [A, A]_G/H \to [A, A/H]_G$ of $\mathbf{GSet}^t$ that factors the map $G \to E$ that sends e to q. But this last map is q^* as in Figure 3.5. □

ε is the counit. Keeping the proof above in mind we set $E = [A, X]$ and obtain

$$\psi\colon \mathscr{C}(A \times_G [A, X], X) \cong \mathbf{GSet}^t([A, X]_G, [A, X]_G)$$

that becomes

$$\mathscr{C}(A/H, X) \cong \mathbf{GSet}^t([A, X]_G, [A, X]_G)$$

with $H = \mathrm{Fix}(x)$ for some $x \in [A, X]$. Notice that since $[A, X] \cong G/H$ by Proposition 3.7 we can consider $1_{[A,X]}$ as a map of type $G/H \to [A, X]$ such that $1_{[A,X]}(e) = x$ (this can be obtained by chasing 1_A around Figure 3.7) there is iso). Now we have that $\psi^{-1}(1_{[A,X]})$ is the arrow $A/H \to X$ of $\mathscr{C}$ that factorizes x i.e. $\psi^{-1}(1_{[A,X]}) = \varepsilon$ as in Figure 3.6. □

References

[1] E.J. Dubuc, C. Sanchez de la Vega, *On the Galois Theory of Grothendieck*, arXiv:math/0009145, 2007.

[2] Saunders Mac Lane, *Categories for the Working Mathematician*, Springer, second edition, 1997.

[3] Serge Lang, *Algebra*, Springer - Graduate Texts in Mathematics, revised third edition, 2005.

[4] Robert Goldblatt, *Topoi - the categorical analysis of logic*, Dover, revised edition, 2006.