

## PRINCIPAL HOMOGENEOUS SPACES AND GALOIS EXTENSIONS

ANDY R. MAGID

**Principal homogeneous spaces for finite groups in the category of sets with groupoid action are studied and classified. The results are applied to separable algebras, using the fundamental theorem of Galois theory of commutative rings, which embeds the category of separable algebras into the category of sets on which a certain profinite groupoid acts.**

The fundamental theorem of the Galois theory of commutative rings gives an anti-equivalence between the category of quasi-separable algebras [2, 2. 1, p. 113] over a commutative ring and the category of profinite spaces on which a certain groupoid (the fundamental groupoid of the ring) operates (see [4, THM IV. 31]). Since sets with groupoid action are more concrete objects than algebras, one hopes to be able to use the fundamental theorem to study algebras by studying the simpler category of groupoid sets. This paper employs that technique to study Galois extensions [1, THM 1. 3, p. 4] in terms of groupoid sets which are principal homogeneous spaces (PHS's).

The basic results are: Let  $A$  be a finite abelian group and  $G$  a groupoid. Then PHS's for  $A$  in the category of  $G$ -sets are classified by continuous homomorphisms from a profinite group  $P(G)$ , associated to  $G$ , to  $A$ . We define a cohomology theory for groupoids which gives the classification cohomologically. Finally, we characterize the quotients of PHS's (for a fixed finite group  $H$ ) by subgroups of  $H$ .

These have the following significance in the case that  $G$  is the fundamental groupoid of a commutative ring  $R$ : The group  $P(G)$  is the full abelian Galois group of  $R$  in the sense of [1, THM 4, p. 71], the cohomology is Amitsur cohomology, and the characterization of quotients is a theorem of Villamayor on embedding separable algebras in Galois algebras [7, p. 166].

The theory of groupoid sets, although straightforward is not readily available in the literature. Thus much of this paper is devoted to routine formalities. To keep the length of the proofs roughly in proportion to the significance of the results, many purely computational arguments are only outlined.

The translation from groupoids to commutative algebra requires some familiarity with the Boolean spectrum of a commutative ring  $R$  (denoted  $X(R)$ ) and the sheaf it carries (whose stalk at  $x$  in  $X(R)$

is denoted  $R_x$ ). See [5] and [8] for details. We also use some Galois theory; see [4] and the references contained therein.

If  $X, Y$  are topological spaces,  $\text{Cont}(X, Y)$  is the set of continuous function from  $X$  to  $Y$ . If  $G$  and  $H$  are topological groups,  $\text{Hom}_c(G, H)$  is the set of continuous homomorphisms from  $G$  to  $H$ .

We begin by recalling definitions and establishing notational conventions for categories of profinite sets with profinite groupoid action. We will normally identify a groupoid with its set of morphisms.

By a profinite space we mean a compact, zero-dimensional Hausdorff space (of course, every such space is an inverse limit of finite sets, whence the name).

A profinite groupoid is a groupoid whose sets of objects and morphisms are profinite, and such that composition and the functions assigning range and domain to morphisms, and identity morphisms to objects, are continuous.

Throughout this paper,  $G$  denotes a profinite groupoid with set of objects  $Y$  and  $r, d: G \rightarrow Y$  assign to a morphism its range and domain, respectively. By a profinite space  $(M, p)$  over  $Y$  we mean a profinite space  $M$  and a continuous surjection  $p: M \rightarrow Y$ . We recall:

DEFINITION [4, IV. 29]. A left  $G$ -action on a profinite space  $(M, p)$  over  $Y$  is a continuous function

$$a: G \times_{d,p} M \longrightarrow M$$

such that:

- (i) If  $g \in G$ ,  $m \in M$ , and  $d(g) = p(m)$  then  $r(g) = p(a(g, m))$ .
- (ii) If  $g, h \in G$ ,  $m \in M$ , and  $d(g) = r(h)$  and  $d(h) = p(m)$ , then  $a(gh, m) = a(g, a(h, m))$ .
- (iii) If  $g \in G$  is the identity map at  $y$  and  $p(m) = y$ , then  $a(g, m) = m$ .

If  $g \in G$ ,  $m \in M$ , and  $d(g) = p(m)$ , we write  $gm$  for  $a(g, m)$ .

A morphism  $f: (M, p) \rightarrow (N, q)$  of profinite spaces over  $Y$  with left  $G$ -action is a continuous function  $f: M \rightarrow N$  (written to the right of its argument) such that  $qf = p$  and if  $g \in G$ ,  $m \in M$  with  $d(g) = p(m)$ ,  $(gm)f = g(mf)$ . The profinite spaces over  $Y$  with left  $G$ -action thus form a category which we denote throughout this paper by  $\mathcal{M}$ .

DEFINITION 1. Let  $H$  be a finite group. An object  $(M, p)$  of  $\mathcal{M}$  is a *principal homogeneous space for  $H$*  (PHS for  $H$ ) if  $H$  is faithfully represented as automorphisms of  $M$  and the map

$$M \times H \longrightarrow M \times_{p,p} M$$

which sends  $(m, h)$  to  $(m, mh)$  is a homeomorphism. A morphism of PHS's for  $H$  is a morphism of  $\mathcal{M}$  preserving the  $H$ -action. A pointed

PHS for  $H$ , denoted  $(M, p, s)$ , is a PHS  $(M, p)$  for  $H$  plus a continuous section  $s$  of  $p$ . A morphism of pointed PHS's for  $H$  is a morphism of PHS's for  $H$  which preserves sections.

We record some elementary properties of PHS's.

PROPOSITION 2. *Let  $H$  be a finite group.*

(a) *Let  $(M, p)$  be a PHS for  $H$ . Then  $H$  acts transitively and effectively on the fibres of  $p$ .*

(b) *Let  $f: (M, p) \rightarrow (N, q)$  be a morphism of PHS's for  $H$ . Then  $f$  is an isomorphism.*

*Proof.* (a) Both  $M \times H$  and  $M \times_{p,p} M$  sit over  $Y$  by projection on the first factor followed by  $p$ . The fibres over  $y$  in  $Y$  are  $p^{-1}(y) \times H$  and  $p^{-1}(y) \times p^{-1}(y)$ , respectively, and the homeomorphism restricts to a bijection between them giving (a). For (b), let  $y$  be in  $Y$  and consider the restriction of  $f$  to the fibres  $p^{-1}(y)$  and  $q^{-1}(y)$ . By Definition 1 and part (a) this is an  $H$ -map of sets on which  $H$  acts transitively and effectively and thus is a bijection. It follows that  $f$  is also bijective, hence an isomorphism.

As an example of a PHS, we have the trivial PHS: Let  $H$  be a finite group. We make  $Y \times H$  a  $G$ -set by defining  $g(d(g), h) = (r(g), h)$  for  $g \in G$  and  $h \in H$  and make  $H$  act on  $Y \times H$  by  $(y, k)h = (y, kh)$  for  $y \in Y, h, k \in H$ . These definitions (as we will show shortly) make  $Y \times H$  a PHS for  $H$  which we denote by  $t(H)$ . We will need to compute the endomorphisms as PHS for  $H$  of  $t(H)$ . This requires looking at the space of components of  $G$ .

LEMMA 3. *Define the relation  $R$  on  $Y$  by  $yRz$  if and only if there is  $g$  in  $G$  with  $d(g) = y$  and  $r(g) = z$ . Then  $R$  is an equivalence relation and the quotient space  $Z = Y/R$  is profinite.*

*Proof.*  $R$  is easily seen to be an equivalence relation. The graph of  $R$  is the image of the map  $G \rightarrow Y \times Y$  which sends  $g$  to  $(d(g), r(g))$  and hence is closed. It is now a standard topological exercise to verify that the quotient of a profinite space by an equivalence relation with closed graph is again profinite.

We call the space  $Z$  of Lemma 3 the space of components of  $G$ .

PROPOSITION 4. *The automorphisms of  $t(H)$  as a PHS for  $H$  are in one-to-one correspondence with  $\text{Cont}(Z, H)$ .*

*Proof.* Let  $f$  be an automorphism of  $t(H)$ . Consider the (continuous) function  $f_0: Y \rightarrow H$  which sends  $y$  to the second component of  $f(y, 1)$ . Since  $f$  is a map in  $M$ , if there is a  $g$  in  $G$  with  $d(g) = y$

and  $r(g) = z$ ,  $f(g(y, 1)) = gf(y, 1)$  so  $f_0(z) = f_0(y)$ . Thus  $f_0$  factors through  $R$  and induces a continuous map  $f_1: Z \rightarrow H$ . We claim that  $f_1$  determines  $f$ : for since  $f$  is an  $H$ -map  $f(y, h) = f(y, 1)h = (y, f_1(y)h)$ . Now let  $f_1: Z \rightarrow H$  be any continuous map. Then it is easy to check that  $f: t(H) \rightarrow t(H)$  defined by the above formula is an endomorphism (hence by Proposition 2b an automorphism) of  $t(H)$  as a PHS for  $H$ , and that the correspondence given here is one-to-one.

Next, we want to classify pointed PHS's. If  $(M, p, s)$  is a pointed PHS for  $H$ , let  $f_M: G \rightarrow H$  be the function defined by  $g(s(d(g))) = s(r(g))f_M(g)$  for  $g$  in  $G$ . We call  $f_M$  the associated functor of  $M$  (the terminology is justified below).

**THEOREM 5.** *There is a one-to-one correspondence between the set of isomorphism classes of pointed PHS's for  $H$  and the set of continuous functors  $G \rightarrow H$ . The correspondence is induced by sending  $(M, p, s)$  to  $f_M$ .*

*Proof.* The proof of the theorem requires a number of simple but lengthy verifications which we only sketch briefly. First,  $f_M$  is defined for all of  $G$  since, by Proposition 2a,  $H$  acts transitively and effectively on the fibres of  $p$ . One then checks that  $f_M$  is continuous by expressing it as a composite of continuous maps. To see that  $f_M$  is a functor, if  $g, h$  are in  $G$  with  $d(g) = r(h) = z$  and  $d(h) = y$ , then  $(gh)sy = g(sz)f_M(h) = sr(g)f_M(g)f_M(h)$  so  $f_M(gh) = f_M(g)f_M(h)$ , and one sees similarly that  $f_M$  carries identities to the identity. We now see that  $f_M$  only depends on  $(M, p, s)$  up to isomorphism: Let  $\alpha: (M, p, s) \rightarrow (N, q, t)$  be an isomorphism of pointed PHS's for  $H$ . Let  $g \in G$ . Then  $(g(sdg))\alpha = ((srg)f_M(g))\alpha = (srg)\alpha f_M(g) = t(tg)f_M(g)$ . But also  $(g(sdg))\alpha = g((sdg)\alpha) = g(tdq) = t(trg)f_N(g)$ , so  $f_M = f_N$ .

Next, let  $f: G \rightarrow H$  be any continuous functor. We produce a pointed PHS for  $H(M_f, q, t)$  whose associated functor is  $f$ . Let  $M_f = Y \times H$ ,  $q(y, h) = y$  and  $t(y) = (y, 1)$ . If  $g \in G$ , define  $g(d(g), h) = (r(g), f(g)h)$ . It is easy to verify, using that  $f$  is a functor, that this definition makes  $M_f$  into a space with left  $G$ -action. Let  $H$  act on  $M_f$  by  $(y, h)k = (y, hk)$  for  $h, k \in H$ ; this action makes  $M_f$  into a PHS for  $H$ . If  $g \in G$ , then  $g(tdq) = g(dg, 1) = (rg, f(g)) = (trg)f(g)$ , so the associated functor is  $f$  again.

To complete the proof, we need to show that if  $(M, p, s)$  is a pointed PHS for  $H$  with associated functor  $f$ , then  $(M_f, q, t)$  is isomorphic to  $(M, p, s)$ . Define  $b: M_f \rightarrow M$  by  $b(y, h) = (sy)h$ . This is a homeomorphism and  $qb = p$  and  $tb = s$ . If  $g \in G$  and  $h \in H$ , then  $b$  sends  $g(d(g), h) = (r(g), f(g)h)$  to  $(srg)t(g)h = g(sd(g))h$  so  $b$  is morphism of sets with  $G$ -action; it is also easy to see that  $b$  preserves the  $H$ -action, so  $b$  is an isomorphism of pointed PHS's for  $H$ .

According to Theorem 5, classifying pointed PHS's means classifying their associated functors. These functors map  $G$  continuously to groups. Our next step, then, is to construct a universal such functor: First we construct a universal continuous map of  $G$  to a group, and then introduce relations in the group to make the map a functor. We begin with a definition:

DEFINITION 6. Let  $X$  be a profinite space. A free profinite group on  $X$  is a pair  $(F, h)$  where  $F$  is a profinite group  $h: X \rightarrow F$  a continuous function such that if  $\mathcal{G}$  is a profinite group and  $g: X \rightarrow \mathcal{G}$  a continuous function then there is a unique continuous homomorphism  $f: F \rightarrow \mathcal{G}$  such that  $fh = g$ .

Clearly, if a free profinite group on  $X$  exists it is unique up to isomorphism; we denote it  $F(X)$ .

PROPOSITION 7. Let  $X$  be a profinite space. Then  $F(X)$  exists.

*Proof.* Let  $F_0$  be the free group on  $X$ . Let  $\mathcal{N}$  be the set of normal subgroups  $N$  of  $F_0$  of finite index such that every coset of  $N$  meets  $X$  in an open-closed subset.  $\mathcal{N}$  is partially ordered by inverse inclusion. Let  $F = \text{proj lim } (F_0/N; N \in \mathcal{N})$ . The compatible maps, for  $N$  in  $\mathcal{N}$ ;  $X \rightarrow F_0 \rightarrow F_0/N$  induce a continuous map  $h: X \rightarrow F$ . If  $\mathcal{G} = \text{proj lim } (\mathcal{G}_i)$  is any profinite group (with each  $\mathcal{G}_i$  finite) and  $X \rightarrow \mathcal{G}$  continuous, then for each  $i$  we have a continuous map  $p_i: X \rightarrow \mathcal{G} \rightarrow \mathcal{G}_i$  and hence a map  $q_i: X \rightarrow F_0 \rightarrow \mathcal{G}_i$  with  $p_i^{-1}(g) = q_i^{-1}(g)$  for all  $g$  in  $\mathcal{G}_i$ . So  $K = \text{Kernel}(F_0 \rightarrow \mathcal{G}_i)$  is of finite index and each coset of  $K$  meets  $X$  in an open-closed subset. So there is a unique  $F \rightarrow \mathcal{G}_i$  such that  $F_0 \rightarrow \mathcal{G} \rightarrow \mathcal{G}_i = F_0 \rightarrow F \rightarrow \mathcal{G}_i$ . This happens for each  $i$ , so there is a unique  $F \rightarrow \mathcal{G}$  with  $X \rightarrow F \rightarrow \mathcal{G} = X \rightarrow \mathcal{G}$ . Hence  $(F, h)$  is a free profinite group on  $X$ .

We remark that  $F(, )$  is a functor from profinite spaces to profinite groups adjoint to the forgetful functor. If  $D$  is a discrete space,  $\beta D$  its Stone-Ćech compactification, then  $F(\beta D)$  is the free profinite group on  $D$  in the sense of [6, 1.5, pI-5]. We denote the map  $X \rightarrow F(X)$  by  $x \mapsto [x]$ .

DEFINITION 8.  $\pi(G)$  (the fundamental group of  $G$ ) is  $F(G)$  mod the closed normal subgroup generated by the identities and by all products  $[gh] [h]^{-1} [g]^{-1}$  where  $g, h$  in  $G$  are composable.

Then  $\pi( . )$  is a functor from profinite groupoids to profinite groups adjoint to the forgetful functor. We use Definition 8 to restate Theorem 5 as

THEOREM 5'. There is a one-to-one correspondence between the set

of isomorphism classes of pointed PHS's for  $H$  and  $\text{Hom}_c(\pi(G), H)$ .

Theorem 5 classified pointed PHS's. We would like to classify arbitrary PHS's. This will be done by introducing sections in arbitrary PHS's. To guarantee that this can be done, we introduce the hypothesis: (ED) The space  $Y$  of objects of  $G$  is extremally disconnected. (If  $G$  is the fundamental groupoid of a commutative ring,  $G$  satisfies (ED) [4, IV. 16].)

Isomorphism classes of pointed PHS's correspond to functors. We examine when two functors give rise to isomorphic (unpointed) PHS's.

LEMMA 9. *Let  $f, h$  be continuous functors from  $G$  to  $H$ . Then the PHS's associated to  $f$  and  $h$  are isomorphic if and only if there exists a continuous function  $b: X \rightarrow H$  with  $k(r(g))f(g) = h(g)k(d(g))$  for all  $g$  in  $G$ .*

*Proof.* Suppose the associated PHS's are isomorphic via a map  $a: Y \times H \rightarrow Y \times H$ . Since  $a$  commutes with projection on  $Y$ ,  $(y, 1)a = (y, b(y))$  for some continuous  $b: Y \rightarrow H$ . Since  $a$  is a  $G$ -set map,  $(g(d(g), 1))a = g((d(g), 1)a)$  so

$$\begin{aligned} (r(g), f(g))a &= ((r(g), 1)a)f(g) = (r(g), b(r(g))f(g)) \\ &= g(d(g), b(d(g))) = (r(g), h(g)b(d(g))), \end{aligned}$$

so  $b(r(g))f(g) = h(g)b(d(g))$  for all  $g$  in  $G$ . Conversely, any continuous  $b: Y \rightarrow H$  defines a map  $a: Y \times H \rightarrow Y \times H$  by  $(y, h)a = (y, b(y)h)$ . Calculations as above show  $a$  to be a morphism (hence isomorphism) of PHS's for  $H$ .

We will eventually make the set of isomorphism classes of PHS's for a fixed  $H$  into a group, with the trivial PHS  $t(H)$  representing the identity. Thus to tell whether PHS's are isomorphic, it will be enough to know when a PHS is isomorphic to  $t(H)$ , and the next lemma supplies this information.

LEMMA 10. *Let  $G$  satisfy (ED). A PHS  $(M, p)$  for  $H$  is isomorphic to  $t(H)$  if and only if there is a  $G$ -set morphism  $Y \rightarrow M$ .*

*Proof.*  $Y$  is a  $G$ -set via  $g(d(g)) = r(g)$ . Choose a section  $s$  of  $p$  and let  $f$  be the functor associated to the pointed PHS  $(M, p, s)$ .  $t(H)$  is the PHS associated to the trivial functor. By Lemma 9,  $t(H)$  and  $(M, p)$  are isomorphic if and only if there is a map  $b: Y \rightarrow H$  such that  $f(g) = b(r(g))b(d(g))^{-1}$ . Suppose such a  $b$  exists, and let  $a: Y \rightarrow M$  be  $(y)a = (sx)(bx)$ . It is easily verified that  $a$  is a  $G$ -set

morphism. Conversely, let  $\alpha: Y \rightarrow M$  be a  $G$ -set map. Then  $\alpha$  is a section of  $p$ , and calculation shows that the functor associated to  $(M, p, \alpha)$  sends all elements of  $G$  to 1.

We now introduce some notation.  $P(G, H)$  is the set of isomorphism classes of PHS's for  $H$  and  $P^*(G, H)$  is the set of isomorphism classes of pointed PHS's for  $H$ .

The function  $G \rightarrow F(Y)$  which sends  $g$  to  $r(g)^{-1}d(g)$  factors through  $\pi(G)$ . The resulting map from  $\pi(G)$  to  $F(Y)$  is called the augmentation.

PROPOSITION 11. *Let  $G$  satisfy (ED) and let  $A$  be a finite abelian group. Let  $C(A)$  denote the cokernel of the map*

$$\text{Hom}_c(F(Y), A) \longrightarrow \text{Hom}_c(\pi(G), A)$$

*induced by the augmentation. Then we have a commutative diagram*

$$\begin{array}{ccc} \text{Hom}_c(\pi(G), A) & \longrightarrow & C(A) \\ \downarrow & & \downarrow \\ P^*(G, A) & \longrightarrow & P(G, A) \end{array}$$

*where the vertical maps are bijections (the left being Theorem 5').*

*Proof.* Since we assume (ED), the bottom map is surjective. By Lemma 9, if  $f, k$  are in  $\text{Hom}_c(\pi(G), A)$  and their associated PHS's are isomorphic (unpointed) there is a function  $b: Y \rightarrow H$  with  $f(g) = k(g)b(r(g))^{-1}b(d(g))$  for all  $g$  in  $G$ . Then  $b$  gives rise to a homomorphism  $F(Y) \rightarrow H$  such that  $f$  is  $k$  times that homomorphism composed with the augmentation. Conversely,  $f$  times the image of any homomorphism  $F(Y) \rightarrow H$  corresponds to the same isomorphism class of PHS's, and the proposition results.

COROLLARY 12. *Let  $G$  satisfy (ED). Then  $P(G, \_)$  is a functor from finite abelian groups to abelian groups.*

We want to represent the functor  $P(G, \_)$ . We will need to know that it is left exact, and this will require the following lemma.

LEMMA 13. *Let  $\mathcal{E} \rightarrow F(X)$  be a homomorphism of profinite groups and let  $C(\cdot)$  be the cokernel of the induced map of functors  $\text{Hom}_c(F(X), \cdot) \rightarrow \text{Hom}_c(\mathcal{E}, \cdot)$  on the category of finite abelian groups. If  $C(\cdot)$  preserves monomorphisms,  $C(\cdot)$  is left exact.*

The proof is a straightforward diagram chase which we omit. (One uses the fact that  $F(X)$  free implies that  $\text{Hom}_c(F(X), \cdot)$  preserves epimorphisms.)

PROPOSITION 14. *Let  $G$  have (ED). Then  $P(G, \_)$  is a left exact functor of finite abelian groups.*

*Proof.* By Lemma 13 and Proposition 11, we only need to check that  $P(G, \_)$  preserves monomorphisms. Let  $k: A \rightarrow B$  be a monomorphism of finite abelian groups, and suppose that  $(M, p)$  is a PHS for  $A$  whose class in  $P(G, A)$  goes to zero in  $P(G, B)$ . Choose a section  $s$  of  $p$  and let  $f$  be the functor associated to  $(M, p, s)$ . Then the PHS associated to  $kf$ , which we denote  $(M', p', s')$  is isomorphic to  $t(B)$ . Choose a function  $h: B \rightarrow A$  with  $ah(b) = g(f(a)b)$  for  $a$  in  $A$ ,  $b$  in  $B$ , map  $M'$  to  $M$  by sending  $(s'x)b$  to  $(sx)h(b)$ ; this is a  $G$ -set morphism. By Lemma 10 there is a  $G$ -set map  $X \rightarrow M'$  so we have a  $G$ -set map  $X \rightarrow M' \rightarrow M$ . By Lemma 10 again,  $(M, p)$  is isomorphic to  $t(A)$  so represents the zero class in  $P(G, A)$ .

The augmentation induces a map from the abelianization of  $\pi(G)$  to that of  $F(Y)$ . Let  $P(G)$  denote the kernel of this map; we can now conclude that  $P(G)$  represents  $P(G, \_)$ :

THEOREM 15. *Let  $G$  satisfy (ED). Then the functors  $\text{Hom}_c(P(G), \_)$  and  $P(G, \_)$  on the category of finite abelian groups are isomorphic.*

*Proof.* The functor  $K \rightarrow \text{Hom}_c(K, \_)$  is a contravariant equivalence between the category of profinite abelian groups and the category of left exact functors from finite abelian groups to abelian groups [1, p. 71]. It follows, therefore, by Proposition 14, that  $P(G, \_)$  is the cokernel in the category of left exact functors which is  $\text{Hom}_c(P(G), \_)$  by the above.

We next wish to interpret Theorem 15 in the case  $G$  is the fundamental groupoid of a commutative ring [4]. We begin by interpreting principal homogeneous spaces.

LEMMA 16. *Let  $R$  be a commutative ring,  $G$  the fundamental groupoid of  $R$  and  $H$  a finite group. Then the category of Galois extensions of  $R$  with group  $H$  [1, p. 6] and the category of PHS's for  $H$  are anti-equivalent.*

*Proof.* Let  $\mathcal{S}$  be the category of quasi-separable  $R$ -algebras and  $S$  a separable closure of  $R$  [4, IV. 19]. Then  $G = X(S \otimes_R S)$  and  $\mathcal{S}$  and  $\mathcal{M}$  (the category of spaces with  $G$ -action) are anti-equivalent via  $T \mapsto X(S \otimes_R T)$  [4, THM IV. 31]. Let  $T$  be a commutative  $R$ -algebra with  $H$  contained in  $\text{Aut}_R(T)$ . Then  $f: T \otimes_R T \rightarrow \text{Cont}(H, T)$  by  $(s \otimes t)(h) = sh(t)$  is an isomorphism exactly when  $T$  is a Galois extension with group  $H$ . Let  $M = X(S \otimes_R T)$ ,  $p: M \rightarrow X(S)$

being the induced structure map. Then  $X(S \otimes_R (T \otimes_R T))$  is canonically identified with  $MXp, pM$ .  $X(S \otimes_R \text{Cont}(H, T))$  can be identified with  $X(S) \times H$ . With these identifications  $f$  induces the map  $X(S) \times H \rightarrow MXp, pM$  which is an isomorphism if and only if  $M$  is a PHS for  $H$ .

**COROLLARY 17.** *Let  $R$  be a commutative ring with fundamental groupoid  $G$ . Then  $P(G)$  is isomorphic to the full abelian Galois group of  $R$  in the sense of Harrison [1, p. 71].*

*Proof.* By Lemma 16 and Theorem 15, both Harrison's group and  $P(G)$  represent the same functor, so they are isomorphic.

In the theory of groups, principal homogeneous spaces are classified by a suitable one-dimensional cohomology group. We will now develop a cohomology theory of groupoids and use it to show that our Theorem 15 has a cohomological interpretation. In case the groupoid in question is the fundamental groupoid of a commutative ring, this cohomology theory is a special case of Amitsur cohomology, as we will show.

We begin with the definition of a semi-simplicial object associated to  $G$ . For  $n=0$ , let  $G^{(0)} = Y$ , and for  $n \geq 1$ , let  $G^{(n)} = \{(g_1, g_2, \dots, g_n) : g_i \in G \text{ and } r(g_i) = d(g_{i-1}) \ i = 2, 3, \dots, n\}$ . Note that each  $G^{(n)}$  is a profinite space (for  $n \geq 1$ , it is a closed subset of the  $n$ -fold product of  $G$ ). We define continuous maps  $d_i^n : G^{(n)} \rightarrow G^{(n-1)}$   $i = 0, 1, \dots, n$  by the following formulae:

$$\begin{aligned} n = 1: & \quad d_0^1(g) = d(g) \\ & \quad d_1^1(g) = r(g) \\ n \geq 1: & \quad d_0^n(g_1, \dots, g_n) = (g_2, \dots, g_n) \\ 1 \leq i \leq n - 1: & \quad d_i^n(g_1, \dots, g_n) = (g_1, \dots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \dots, g_n) . \end{aligned}$$

These maps satisfy the semi-simplicial identities

$$d_i^{n-1} d_j^n = d_{j-1}^{n-1} d_i^n \quad \text{for } i < j .$$

Now let  $A$  be a finite abelian group. We define a complex  $C^n(G, A)$  as follows: Let  $C^n(G, A) = \text{Cont}(G^{(n)}, A)$ .  $C^n(G, A)$  is an abelian group under pointwise addition of functions. Let  $e_i^n = \text{Cont}(d_i^{n+1}, A) : C^n(G, A) \rightarrow C^{n+1}(G, A)$   $i = 0, 1, 2, \dots, n$ . Finally, let  $\delta^n : C^n(G, A) \rightarrow C^{n+1}(G, A)$  be  $\delta^n = \sum_{i=0}^n (-1)^{i+1} e_i^n$ . Each  $e_i^n$  and hence each  $\delta^n$  is a homomorphism, and the semi-simplicial identities imply that  $\delta^{n+1} \delta^n = 0$ . Thus we have a complex of abelian groups. We define:

$$H^n(G, A) = H^n(C^*(G, A), \delta^*) .$$

We now calculate the low level cohomology.

PROPOSITION 18. *Let  $A$  be a finite abelian group. Then:*

(a)  $H^0(G, A)$  is the group of continuous functions from the space of components of  $G$  to  $A$ .

(b)  $H^1(G, A)$  is isomorphic to  $P(G, A)$ .

*Proof.* (a) See Lemma 3 for the definition of the space of components of  $G$ . An element of  $H^0(G, A)$  is continuous function  $f: Y \rightarrow A$  such that  $\delta^0 f = p$ , i.e., for all  $g$  in  $G$ ,  $f(d(g)) - f(r(g)) = 0$ , i.e.,  $f(d(g)) = t(d(g))$ . Such an  $f$  factors through the space of components of  $Y$ . The argument is clearly reversible.

(b) Let  $f$  in  $C^1(G, A)$  be such that  $\delta^1(f) = 0$ . Then if  $g_1, g_2 \in G$  and  $r(g_2) = d(g_1)$ , then  $\delta^1(f)(g_1, g_2) = -f(g_2) + f(g_1 g_2) - f(g_1) = 0$ , so  $f(g_1 g_2) = f(g_1) + f(g_2)$ , i.e.,  $f: G \rightarrow A$  is a continuous functor.  $f$  represents the zero class in  $H^1(G, A)$  if and only if  $f = \delta^0 h$  for some continuous  $h: Y \rightarrow A$ , i.e.,  $f(g) = h(d(g)) - h(r(g))$ . By Theorem 5 and Lemma 9, isomorphism classes of PHS's for  $A$  correspond to continuous functors modulo functors of the type  $\delta^0 h$ . Thus  $H^1(G, A)$  and  $P(G, A)$  are isomorphic.

Proposition 18 is true even if  $A$  is noncommutative, under suitable definitions for nonabelian  $H^0$  and  $H^1$ .

Our next task is to relate groupoid and Amitsur cohomology. We need a sequence of definitions: Let  $R$  be a commutative ring with separable closure  $S$ . Let  $H$  be a finite group and let  $E_R(H)$  be the trivial Galois extension of  $R$  with group  $H$  [1, p. 68]. Let  $\#H$  be the functor from commutative  $R$ -algebras to groups defined by

$$\#H(T) = \text{Aut}_T(E_T(H)).$$

Let  $G = X(S \otimes_R S)$  be the fundamental groupoid of  $R$ .

PROPOSITION 19. *Let  $A$  be a finite abelian group. Then, in the above notation, we have natural isomorphisms*

$$H^*(S/R, \#A) \longrightarrow H^*(G, A)$$

where the left groups are the Amitsur cohomology groups and the right groups the groupoid cohomology defined above.

*Proof.* We will exhibit an isomorphism on the level of co-semisimplicial sets between  $C^*(S/R, \#A)$  and  $C^*(G, A)$ . Let  $S^{(n)}$  be the  $n + 1$ -fold tensor product of  $S$ ,  $n = 0, 1, \dots$ . Let  $a_i^n: S^{(n)} \rightarrow S^{(n+1)}$   $i = 0, 1, \dots, n + 1$   $a_i^n(s_0 \otimes \dots \otimes s_n) = s_0 \otimes \dots \otimes s_{i-1} \otimes 1 \otimes s_i \otimes \dots \otimes s_n$  be the Amitsur maps.  $C^*(S/R, \#A) = \text{Aut}_{S^{(n)}}(E_{S^{(n)}}(A)) = \text{Cont}(X(S^{(n)}), A)$ ,

the last equality following from Proposition 4, suitably interpreted. We identify  $X(S^{(n)})$  and  $G^{(n)}$  as follows: For  $n \geq 1$ , to  $(g_1, \dots, g_n) \in G^{(n)}$  we associate the set of idempotents in the kernel of the map  $S^{(n)} \rightarrow S_{d(g_1)}$  by  $s_0 \otimes \dots \otimes s_n \mapsto (s_0)_{r(g_1)} g_1((s_1)_{d(g_1)} g_2((s_2)_{d(g_2)} g_3 \dots g_n((s_n)_{d(g_n)})) \dots)$ . By techniques similar to [4, (8)], one sees that this induces a bijection between  $X(S^{(n)})$  and  $G^{(n)}$ . For  $n = 0$ ,  $X(S)$  is the set of objects  $Y$  of  $G$ . The maps  $a_i^n$  give rise to maps  $\#A(a_i^n): \#A(S^{(n)}) \rightarrow \#A(S^{(n+1)})$ . In fact, with the identification of these groups above, we have  $\#A(a_i^n) = \text{Cont}(X(a_i^n), A)$ . We now show that with the identification of  $X(S^{(n)})$  and  $G^{(n)}$  given above  $X(a_i^{n-1}) = d_i^n$   $i = 0, 1, \dots, n$ . Let  $z$  be a point of  $X(S^{(n)})$  corresponding to  $(g_1, \dots, g_n) \in g^{(n)}$ . Then  $X(a_i^{n-1})(z)$  is the set of idempotents in the kernel of the map  $S^{(n-1)} \rightarrow S_{d(g_1)}$  by  $s_0 \otimes \dots \otimes s_{n-1} \rightarrow s_0 \otimes 1 \otimes s_2 \otimes \dots \otimes s_n \rightarrow (s_0)_{r(g_1)} g_1(g_2((s_2)_{d(g_2)} \dots))$ , and this corresponds to the point  $(g_1 g_2, g_3, \dots, g_n)$  of  $G^{(n-1)}$ . The situation for  $X(a_i^{n-1})$ ,  $i \neq 1$  is similar. Thus, under the identifications above,

$$C^*(S/R, \#A) = C^*(G, A)$$

$$\#A(a_i) = d_i$$

and since both cohomologies are constructed in the same way from these isomorphic co-semi-simplicial complexes, we have  $H^*(S/R, \#A) = H^*(G, A)$ .

The remaining section of this paper is devoted to the study of quotients of principal homogeneous spaces for  $H$  by subgroups of  $H$ . We begin with an easy lemma:

LEMMA 20. *Let the  $G$ -set  $(M, p)$  be a principal homogeneous space for  $H$ . Let  $K$  be a subgroup of  $H$ . Then the quotient  $M/K$  is a covering space of  $Y$  with constant fibre dimension  $[H:K]$ .*

*Proof.* As a topological space,  $M = Y \times H$  and hence  $M/H = Y \times H/K$ . It turns out that the necessary condition of Lemma 20 is also sufficient.

PROPOSITION 21. *Let the  $G$ -set  $(M, p)$  be a covering space of  $Y$  with constant fibre dimension  $n$ . Then there is a PHS  $(N, q)$  for the symmetric group  $S_n$  on  $n$  letters such that  $M/S_{n-1}$  is  $G$ -isomorphic to  $(M, p)$  ( $S_{n-1}$  sits in  $S_n$  as the subgroup fixing the first letter).*

*Proof.* Because  $Y$  is zero-dimensional, a locally trivial space over  $Y$  is globally trivial. Thus we can find a homeomorphism  $M \rightarrow Y \times F$  where  $F$  is a finite set with  $n$  elements. Let  $N_0 = Mx_p \dots x_p M$  ( $n$ -times) and let  $S_n$  act on  $N_0$  in the obvious way (note that  $S_n$  acts as  $G$ -set morphisms). Let  $N = \{(m_1, \dots, m_n) \in M: m_i \neq m_j \text{ if } i \neq j\}$ .

$N$  is clearly  $G$ -stable and it is closed in  $N_0$  since  $N = Y \times K$  where  $K = \{(f_1, \dots, f_n) \in Fx, \dots, xF: f_i \neq f_j \text{ if } i \neq j\}$ . Thus  $N$  is a profinite set with left  $G$ -action. Also  $S_n$  acts on  $N$  and, using the homeomorphism  $N = Y \times K$ ,  $S_n$  acts transitively and effectively. Thus  $N$  is a PHS for  $S_n$ . Clearly the quotient of  $N$  under  $S_{n-1}$  is  $M$  again.

Proposition 21 has as a consequence a theorem of Villamayor [7, p. 166] when  $G$  is the fundamental groupoid of a commutative ring, as we now see.

**LEMMA 22.** *Let  $R$  be a commutative ring with separable closure  $S$  and fundamental groupoid  $G$ . Let  $T$  be a separable  $R$ -algebra which is a projective  $R$ -module of constant rank  $n$ . Then the  $G$ -set corresponding to  $T$  is a covering space of  $X(S)$  of constant fibre cardinality  $n$ .*

*Proof.* The set corresponding to  $T$  is  $X(S \otimes_R T)$ .  $S \otimes_R T$  is a separable projective  $S$ -algebra of constant rank  $n$ , and  $(S \otimes_R T)_x$  is a separable projective  $S_x$  algebra of rank  $n$  for each  $x$  in  $X(S)$ . Since  $S_x$  is separably closed [4], this means that  $(S \otimes_R T)_x$  is isomorphic to  $S_x \times \dots \times S_x$  ( $n$ -times). The separable projective algebras  $S \otimes_R T$  and  $S \times \dots \times S$  are isomorphic at each  $x$  in  $X(S)$ , so by [3, 1.7, p. 116] are isomorphic. Thus the space  $X(S \otimes_R T) = X(S \times \dots \times S) = X(S)v \dots vX(S)$  ( $n$ -fold disjoint union) is a covering space of  $X(S)$  of constant fibre cardinality  $n$ .

**COROLLARY 23.** *Let  $R$  be a commutative ring,  $T$  a separable  $R$ -algebra, projective of constant rank  $n$  as an  $R$ -module. Then there is an  $R$ -algebra  $T'$  which is Galois with group  $S_n$ , and an injection  $T \rightarrow T'$  such that  $T$  is isomorphic to the subring of  $S_{n-1}$  invariant elements of  $T'$  (see [7, p. 166]).*

*Proof.* By Lemma 22,  $X(S \otimes_R T)$  satisfies the hypotheses of Proposition 21. Let  $T'$  be the algebra corresponding to the PHS produced in Proposition 21 and  $T \rightarrow T'$  the resulting homomorphism. We can express the fact that  $X(S \otimes_R T)$  is the quotient of  $X(S \otimes_R T')$  by  $S_{n-1}$  by saying that

$$X(S \otimes_R T')X_{X(S)}t(S_{n-1}) \rightrightarrows X(S \otimes_R T') \longrightarrow X(S \otimes_R T)$$

(where the top left arrow is  $(n, (p(m), h)) \rightarrow m$  and the bottom is  $(m, (p(m), h)) \rightarrow mh$ ) is exact. Thus the diagram

$$T \longrightarrow T' \rightrightarrows T' \otimes_R E_R(S_{n-1}) = E_{T'}(S_{n-1})$$

is exact. Thinking of  $E_{T'}(S_{n-1})$  as functions from  $S_{n-1}$  to  $T'$ , the top right map sends  $t'$  to the constant function  $t'$  and the bottom sends

$t'$  to the function whose value at  $h$  is  $t'(h)$ . Thus the difference kernel is the invariant elements of  $T'$  and hence  $T$  is that ring of invariants.

## REFERENCES

1. S. Chase, D. Harrison, and A. Rosenberg, *Galois theory and cohomology of commutative rings*, Memoirs Amer. Math. Soc., **52**, 2nd printing with corrections, 1968.
2. A. Magid, *The separable closure of some commutative rings*, Trans. Amer. Math. Soc., **170** (1972), 109-124.
3. ———, *Pierce's representation and separable algebras*, Illinois J. Math., **15** (1971), 114-121.
4. ———, *The Separable Galois Theory of Commutative Rings*, Marcel Dekker, Inc., New York, 1974.
5. R. Pierce, *Modules over commutative regular rings*, Memoirs Amer. Math. Soc., no **70**, (1967).
6. J. P. Serre, *Cohomologie Galoisienne*, Lecture Notes in Math, 5, Springer-Verlag, New York, 1965.
7. O. Villamayor, *Separable algebras and Galois extensions*, Osaka J. Math., **4** (1967), 161-171.
8. O. Villamayor and D. Zelinsky, *Galois theory with infinitely many idempotents*, Nagoya Math. J., **35** (1969), 83-98.

Received March 12, 1973 and in revised form November 28, 1973.

UNIVERSITY OF OKLAHOMA

