Active sums of profinite groups

P. Ribenboim

Dedicated to Professor Philip Hall,
on his eightieth birthday.

Introduction.

In this paper, we extend the construction of active sums of active quivers of groups to the similar construction in categories of pro-$\mathscr{C}$-groups. Originally, the construction was considered by Tomás [6] in the particular case of active normal families of groups. We extended it in [4] for active quivers fo groups. Díaz-Barriga & López indicated in [1] how to make the construction for active partially ordered families of profinite groups.

We apply this construction to Galois groups of number fields, showing that the natural homomorphism from the profinite group active sum of the decomposition groups, to the Galois group, is always surjective.

1. **Active Sums of Pro-$\mathscr{C}$-Groups.**

Let $\mathscr{C}$ be a class of *finite* groups such that:

1) if $G \in \mathscr{C}$ and $H \leq G$ then $H \in \mathscr{C}$
2) if $G \in \mathscr{C}$ and $H \trianglelefteq G$ then $G/H \in \mathscr{C}$
3) if $1 \to H \to G \to K \to 1$ is an exact sequence of groups and $H, K \in \mathscr{C}$ then $G \in \mathscr{C}$.

For example, $\mathscr{C}$ may be any one of the following classes: all finite groups; all finite solvable groups; all finite nilpotent groups, all finite abelian groups; all finite cyclic groups; for each prime p, all finite p-groups.

A pro-$\mathscr{C}$-group is, by definition, any group G which is the inverse (= projective) limit of an inverse system of groups in the class $\mathscr{C}$. Equivalently, a pro-$\mathscr{C}$-group is a profinite group G, such that for every open normal subgroup U the group G/U is in the class $\mathscr{C}$.

We consider the category of pro-$\mathscr{C}$-groups, whose objects are the pro-$\mathscr{C}$-groups and whose morphisms are the continuous group-homomorphisms.

Recebido em 15/09/83.

We shall extend the constructions in the paper *Active Sums of Groups* [4] to the category of pro-$\mathcal{C}$-groups.

Let **G** be a category of groups, for example, the category of all groups, the category of all pro-$\mathcal{C}$-groups (where $\mathcal{C}$ is a class of groups, as indicated). Following [4], we recall the concept of an active quiver of groups of **G**.

Let $\mathcal{I}$ be a *directed graph.* It consists of a non-empty set I of *vertices* and for every $i, j \in I$ a set $A(i,j)$ (which may be empty) of *arrows.* If $\alpha \in A(i,j)$ then $i = \mathrm{o}(\alpha)$ is the *origin* of α and $j = t(\alpha)$ is the *terminal* of α. We denote by A the set of all arrows: $A = \coprod_{i,j \in I} A(i,j)$. Sometimes we write $\mathcal{I} = (I, A, \mathrm{o}, t)$.

Any non-empty set I may be viewed as a directed graph, with $A = \emptyset$. Any partially ordered set $(I, \leq)$ gives rise to a directed graph, with set of vertices I and

$$A(i,j) = \begin{cases} \text{set with only one element } \alpha_{ij}, \text{ when } i < j \\ \emptyset, \text{ otherwise} \end{cases}$$

and $\mathrm{o}(\alpha_{ij}) = i$, $t(\alpha_{ij}) = j$, when $i < j$.

A *morphism* from the directed graph $\mathcal{I}$ to the directed graph $\mathcal{I}'$ is a map $\sigma : I \coprod A \to I' \coprod A'$ such that $\sigma(I) \subseteq A'$, $\sigma \circ \mathrm{o} = \mathrm{o}' \circ \sigma$, $\sigma \circ t = t' \circ \sigma$. A morphism from $\mathcal{I}$ to $\mathcal{I}$ which is bijective is called an automorphism of $\mathcal{I}$. The set $\mathrm{Aut}(\mathcal{I})$ of automorphisms of $\mathcal{I}$ is a group under composition.

Let $\mathcal{I}$ be a directed graph. A *quiver of groups* in the category G, over $\mathcal{I}$, is a family $\mathcal{G} = (G_i)_{i \in I}$ of groups (indexed by the set I of vertices) and for every $i, j \in I$, a family $(c_\alpha)_{\alpha \in A(i,j)}$, where $c_\alpha \in \mathrm{Hom}_{\mathbf{G}}(G_i, G_j)$. We assume also (without loss of generality) that if α, β are distinct arrows then $c_\alpha \neq c_\beta$. Thus in the case when G is the category of pro-$\mathcal{C}$-groups, then each c_α is a continuous group-homomorphism.

The *spread* of the quiver $\mathcal{G}$ is the set $\coprod_{i \in I} G_i$, which we denote by $\coprod \mathcal{G}$. On $\coprod \mathcal{G}$ we consider the following partial operation: if $f, g \in \coprod \mathcal{G}$ and there exists $i \in I$ such that $f, g \in G_i$ then fg is defined and it is equal to the product of the elements f, g in the group G_i; otherwise, fg is not defined. On $\coprod \mathcal{G}$ we consider also the sum of the topologies on the group $G_i (i \in I)$, so the above operation is continuous, whenever it is defined.

Let $\mathcal{G}$ be a quiver of groups over $\mathcal{I}$, let $\mathcal{G}'$ be a quiver of groups over $\mathcal{I}'$ (where the groups belong to the category **G**). A *morphism* from $\mathcal{G}$ to $\mathcal{G}'$ is a map $\sigma : \coprod \mathcal{G} \to \coprod \mathcal{G}'$ such that there is a morphism $\sigma : \mathcal{I} \to \mathcal{I}'$ and the following conditions are satisfied:

1.) for every $i \in I$, the restriction σ_i of σ to G_i belongs to $\mathrm{Hom}_{\mathbf{G}}(G_i, G'_{\sigma(i)})$.
2.) for every $i, j \in I$ and every $\alpha \in A(i,j)$, we have $\sigma_j \circ c_\alpha = c'_{\sigma(\alpha)} \circ \sigma_i$.

We say that σ lies over σ.

An *automorphism* of the quiver $\mathcal{G}$ over $\mathcal{I}$ is a morphism σ such that:
1.) for every $i \in I, \sigma_i$ is an isomorphism (in the category **G**) from G_i to $G'_{\sigma(i)}$.
2.) σ is an automorphism of $\mathcal{I}$.

The composition of morphisms of quivers of groups gives a morphism. The set $\mathrm{Aut}(\mathcal{G})$ of automorphisms of $\mathcal{G}$ is a group under composition.

Let $\mathcal{G}$ be quiver of groups (in the category **G**) over the directed graph $\mathcal{I}$. An *action* in $\mathcal{G}$ is a homomorphism $\pi : \coprod \mathcal{G} \to \mathrm{Aut}(\mathcal{G})$ such that the following conditions are satisfied:
$\tau 1)$ if $i \in I$ and $h \in G_i$ then τ^h, restricted to G_i, is the inner automorphism of G_i defined by $h : g \in G_i \to hgh^{-1} \in G_i$; in particular $\tau^h(i) = i$ when $h \in G_i$.
$\tau 2)$ if $i, j \in I$, $\alpha \in A(i,j)$ and $h \in G_i$ then $\tau^{c_\alpha(h)} = \tau^h$.

If there is no ambiguity, we write $h * k = \tau^h(k)$ for every $h, k \in \coprod \mathcal{G}$.

The action is said to be *trivial* when $h * k = k$ for all $h, k \in \coprod \mathcal{G}$. This implies that each group G_i is abelian.

The action τ is *normal* when τ^h is the identity automorphism of τ, for every $h \in \coprod \mathcal{G}$.

An *active quiver of groups* consists of a quiver of groups $\mathcal{G}$ (of the category **G**) over a directed graph $\mathcal{I}$, together with an action τ in $\mathcal{G}$. If the action is normal, we call it an *active normal quiver of groups.*

Let $\mathcal{I} = I$ be a partially ordered set. Let $\mathcal{G}$ be an active quiver of groups over $\mathcal{I}$, such that for every $i, j \in I$, with $i < j$, it is given a homomorphism $c_{ij} \in \mathrm{Hom}_{\mathbf{G}}(G_i, G_j)$ in such a way that if $i < j < k$ then $c_{ik} = c_{jk} \circ c_{ij}$. Then $\mathcal{G}$ is called an *active partially ordered family of groups.* If moreover the action is normal, then $\mathcal{G}$ is called an *active normal partially ordered family* of groups.

In the special case when $\mathcal{I} = I$ is a discrete graph (i.e. $A = \emptyset$), then we call $\mathcal{G}$ an *active family of groups* and moreover, if the action is normal, an *active normal family of groups.*

In [4], we have shown:

Proposition 1. *Let $\mathcal{G}$ be an active quiver of groups over the directed graph $\mathcal{I}$. Then:*

1.) *there exists a group G and a homomorphism $\varphi : \coprod \mathcal{G} \to G$ such that*

$$\varphi \mid h * k) = \varphi(h)\,\varphi(k)\,\varphi(h)^{-1} \quad \text{for every } h, k \in \coprod \mathcal{G}$$

$$\varphi \circ c_\alpha = \varphi \quad \text{for every } \alpha \in A$$

2.) *if G' is a group, $\varphi' : \coprod \mathcal{G} \to G'$ is a homomorphism satisfying the above properties of G and φ, then there exists a unique homomorphism $\rho : G \to G'$ such that $\varphi' = \rho \circ \varphi$.*

From the universal property, G and φ are unique, up to a unique isomorphism.

The group G, together with the homomorphism φ, is called the *active sum* of the active quiver of groups $\mathscr{G}$. We use the notation $G = \boxplus\mathscr{G}$ when there is no ambiguity.

We prove the corresponding result for the case where G is not the category of all groups, but instead the category of all pro-$\mathscr{C}$-groups, for some class $\mathscr{C}$ of groups, as indicated. The special case of active families of pro-$\mathscr{C}$-groups was established by Díaz-Barriga and López in [1] modifying suitably our proof in [4].

Proposition 2. *Let $\mathscr{G}$ be an active quiver of pro-$\mathscr{C}$-group, over the directed graph $\mathscr{I}$. Then:*

1.) *there exists a pro-$\mathscr{C}$-group G and a continuous homomorphism $\varphi : \coprod\mathscr{G} \to G$ such that*

$$\varphi(h * k) = \varphi(h)\,\varphi(k)\,\varphi(h)^{-1} \text{ for every } h, k \in \coprod\mathscr{G}$$

$$\varphi \circ c_\alpha = \varphi \text{ for every } \alpha \in A.$$

2.) *if G' is a pro-$\mathscr{C}$-group, $\varphi' : \coprod\mathscr{G} \to G'$ is a continuous homomorphism satisfying the above properties of G and φ', then there exists a unique continuous homomorphism $\rho : G \to G'$ such that $\varphi' = \rho \circ \varphi$.*

Proof. Let $\widetilde{G}$ be the active sum of $\mathscr{G}$ in the category of all groups and let $\widetilde{\varphi} : \coprod\mathscr{G} \to \widetilde{G}$ be the canonical homomorphism ($\widetilde{G}$, $\widetilde{\varphi}$ exist by proposition 1).

Consider the inverse system of groups $\widetilde{G}/N$, where N is any normal subgroup of $\widetilde{G}$, of finite index, such that $\widetilde{G}/N \in \mathscr{C}$. Let $G = \lim \widetilde{G}/N$, so G is a pro-$\mathscr{C}$-group. Let $\psi : \widetilde{G} \to G$ be the canonical homomorphism and $\varphi = \psi \circ \widetilde{\varphi}$. It is routine to show that G, φ satisfy the conditions of the statement.

G, together with φ, is unique, up to a unique isomorphism. G is called the *active sum* of $\mathscr{G}$, in the category of pro-$\mathscr{C}$-groups. If there is no ambiguity, we write $G = \boxplus\mathscr{G}$ or even $G = \boxplus_{\mathscr{C}}\mathscr{G}$.

An alternative way of constructing the active sum in the category of pro-$\mathscr{C}$-groups (which was used by Díaz-Barriga and López, for active families) is the following: $G = F/R$ where F is the free pro-$\mathscr{C}$-product of the given pro-$\mathscr{C}$-groups (see Neukirch [3], Ribes [5]) and R is the closed normal subgroup generated by the obvious relations (see proof of the proposition 1 of [4]).

It is straight forward to derive for the active sum of pro-$\mathscr{C}$-groups properties similar to those indicated in [4]. Thus $\boxplus\mathscr{G}$ is the pro-$\mathscr{C}$-group generated by $\varphi(\coprod\mathscr{G})$.

Moreover, if the action satisfies the distributive condition

$$k * (h * \ell) = (k * h) * (k * \ell),$$

or equivalently

$$(k * h) * \ell = k * (h * (k^{-1} * \ell)),$$

then the construction of the active sum is associative (see [4], (e) and (g)).

We now indicate the extension of Puig's theorem to pro-$\mathscr{C}$-groups. For the convenience of the reader, we recall this result, as it was established in [4].

Let G be a group (in the given category **G**) let $\mathscr{G}$ be a family of subgroups of G, each in the category **G**, and such that the inclusion is a morphism in **G**. We say that $\mathscr{G}$ is *stable* if the following condition is satisfied:

$$\text{if } g \in \bigcup\{H \mid H \in \mathscr{G}\} \text{ and } K \in \mathscr{G} \text{ then } K^g = gKg^{-1} \in \mathscr{G}.$$

Let $\mathscr{G}$ be a stable set of subgroups of G (each in the category **G** and such that the inclusion is a morphism on **G**), let $I = \mathscr{G}$, partially ordered by inclusion. Consider the quiver of groups, indexed by I, such that to every $H \in I$ corresponds the group H itself, and such that if $H, K \in I$, $H \subseteq K$, there corresponds the inclusions map. We consider the following action τ in $\mathscr{G}$. If $H \in \mathscr{G}$, $h \in H$, let $\tau^h : \coprod\mathscr{G} \to \coprod\mathscr{G}$ be so defined: if $K \in \mathscr{G}$, $k \in K$ then $\tau^h(k) = hkh^{-1} \in hKh^{-1}$, $\tau^h(K) = hKh^{-1} \in I$. Then τ is a distributive action and $\mathscr{G}$ is an active partially ordered family of subgroups of **G**. For example, if G is a finite group, then the family $\mathscr{P}$ of its subgroups of prime-power order is an active family.

We assume now that **G** is either the category of all groups, or all pro-$\mathscr{C}$-groups, so that the active sum $A = \boxplus\mathscr{G}$ (in the category **G**) exists. Let $\varphi : \amalg\mathscr{G} \to A$ be the canonical homomorphism. Let $\iota : \coprod\mathscr{G} \to G$ be the homomorphism induced by the inclusion. By the definition of active sum, there exists a unique morphism (in the category **G**) $\rho : A \to G$ such that $\rho \circ \varphi = \iota$. It is easily shown that ρ is an epimorphism (in the category **G**) if and only if G is generated by $\bigcup\{H \mid H \in \mathscr{G}\}$ (in the category **G**).

Puig's theorem is the following (see [4], proposition 2):

Proposition 3. *If G is a finite group and $\mathscr{P}$ is the active family of its subgroups of prime-power order, then $\rho : \boxplus\mathscr{P} \to G$ is an isomorphism.*

Now, we assume that G is a prop-$\mathscr{C}$-group, let $\mathscr{P}$ be the active family of its closed subgroups of prime-power order (that is, each finite epimorphic image has prime-power order). This is a stable family of subgroups, which defines in the manner indicated above an active family of groups (in the category of pro-$\mathscr{C}$-groups).

We show:

Proposition 4. *If G is a pro-$\mathscr{C}$-group and $\mathscr{P}$ the active family of its closed subgroups of prime-power order, then the canonical homormorphism $\rho: \boxplus_{\mathscr{C}} \mathscr{P} \to G$ is an isomorphism.*

Proof. For every open normal subgroup N of G, let $\mathscr{P}(G/N)$ denote the family of subgroups of prime-power order of G/N. By proposition 3, the canonical homomorphism $\rho_N: \boxplus \mathscr{P}(G/N) \to G/N$ is an isomorphism. Since $\rho = \varprojlim \rho_N$ then ρ is also an isomorphism.

2. Applications to Galois number fields.

Let K_0 be any algebraic number field, $K \mid K_0$ a Galois extension (not necessarily of finite degree), G its Galois group, so G is a profinite group. Let V be the family of all (non-zero) prime ideals of the (ring of integers of the) field K. If $\mathscr{P} \in V$ then $g(\mathscr{P}) = \{g(x) \mid x \in \mathscr{P}\} \in V$.

For every $\mathscr{P} \in V$ let $D_{\mathscr{P}}$ be its decomposition group, that is $D_{\mathscr{P}} = \{g(\mathscr{P}) = \mathscr{P}\}$. Hence $D_{g(\mathscr{P})} = gD_{\mathscr{P}}g^{-1}$. Therefore the family $\mathscr{D}$ of all decomposition groups is a stable set of closed subgroups of G, and we may consider the active sum $\boxplus \mathscr{D}$ (in the category of profinite groups).

The following result is essentially known:

Proposition 5. $\bigcap_{\mathscr{P} \in V} D_{\mathscr{P}} = \{1\}$.

Proof. Let g belong to this intersection. For any Galois extension of finite degree $L \mid K_0$, $L \subseteq K$, the restriction g_L of g to L belongs to the intersection I of the decomposition groups of all prime ideals $\mathscr{P}_L$ of L. Let H be the fixed field of I; it contains the decomposition field of every prime ideal of L. Thus, every prime ideal of H has exactly one extension to a prime ideal of L.

For any prime ideal $\mathscr{A}$ of H we have the relation

$$[L:H] = e_{\mathscr{A}} f_{\mathscr{A}}$$

where $e_{\mathscr{A}}$ denotes the ramification index and $f_{\mathscr{A}}$ the inertial degree of $\mathscr{A}$ in the extension $L \mid H$.

By Dedekind's theorem, there are only finitely many prime ideals $\mathscr{A}$ of H ramified in $L \mid H$. On the other hand, by Čebotarev's theorem there exists an infinite number of prime ideals $\mathscr{A}$ of H such that $f_{\mathscr{A}} = 1$. Hence there exists a prime ideal $\mathscr{A}$ such that $e_{\mathscr{A}} = f_{\mathscr{A}} = 1$ so $[L:H] = 1$, thus $g_L \in \cap D_{\mathscr{P}_L} = \{1\}$. Since this holds for every L as indicated then g itself is equal to 1.

The Galois group G acts by permutation on $\mathscr{D}$, as follows: $\pi: G \to \text{Perm}\ (\mathscr{D})$, with $\pi_g(D_{\mathscr{P}}) = D_{g(\mathscr{P})} = gD_{\mathscr{P}}g^{-1}$. The kernel of π is $\ker(\pi) = \bigcap_{\mathscr{P} \in V} N_G(D_{\mathscr{P}})$, where $N_G(D_{\mathscr{P}})$ denotes the normalizer of $D_{\mathscr{P}}$ in G.

If each $N_G(D_{\mathscr{P}}) = D_{\mathscr{P}}$ then by proposition 5, $\ker(\pi) = \{1\}$. If $N_G(D_{\mathscr{P}}) = G$ for every $\mathscr{P} \in V$ then $\ker(\pi) = G$, that is π_g is the identity permutation for every $g \in G$. This happens, for example, when G is abelian.

Let $K_0 \mid \mathbb{Q}$ be an extension of finite degree and let $K \mid K_0$ be a finite Galois extension. If $g \in G$ by Čebotarev's theorem (see [2], p. 169) there exist infinitely many prime ideals $\mathscr{P}$ of K such that $g = (\mathscr{P}, K \mid K_0)$ (the Artin symbol), and in particular $g \in D_{\mathscr{P}}$. Thus $G = \bigcup_{\mathscr{P} \in V} D_{\mathscr{P}}$.

More generally, if $K_0 \mid \mathbb{Q}$ has finite degree and $K \mid K_0$ is a Galois extension with group G, then $\bigcup_{\mathscr{P} \in V} D_{\mathscr{P}}$ is a dense subset of G. Therefore, its fixed subfield is the ground field K_0.

For the special case when $K_0 = \mathbb{Q}$, we may prove this assertion, without appealing to Čebotarev's theorem:

The fixed field H of $\bigcup_{\mathscr{P} \in V} D_{\mathscr{P}}$ is the intersection of the decomposition fields $Z_{\mathscr{P}}$ for all prime ideals $\mathscr{P}$ of K. If $\mathscr{A}$ is any prime ideal of H, if $\mathscr{P}$ is a prime ideal of K dividing $\mathscr{A}$, the restriction $\overline{\mathscr{P}}$ of $\mathscr{P}$ to $Z_{\mathscr{P}}$ is unramified over $\mathbb{Q}$ and extends $\mathscr{A}$. So $\mathscr{A}$ is also unramified over $\mathbb{Q}$. Thus every prime ideal of H is unramified over $\mathbb{Q}$. By Minkowski's theorem, every subfield of H of finite degree over $\mathbb{Q}$ must be equal to $\mathbb{Q}$, hence $H = \mathbb{Q}$.

Let $\boxplus \mathscr{D}$ denote the active sum of the active family $\mathscr{D}$ (in the category of profinite groups). With the notation already introduced, we have:

Proposition 6. *The canonical homomorphism $\rho: \boxplus \mathscr{D} \to G$ is surjective.*

Proof. The image of ρ is the subgroup of G generated by $\rho(\varphi(\coprod \mathscr{D}))$, that is, the subgroup generated by $\bigcup_{\mathscr{P} \in V} D_{\mathscr{P}}$, so by the above remark it is a dense subgroup of G. On the other hand, ρ is a continuous homorphism, $\boxplus \mathscr{D}$ is a profinite group, hence it is compact and therefore its image is a compact subgroup of G, so it is closed. Therefore the image of ρ is equal to G.

It should be of interest to study the kernel of the homomorphism ρ, for example when $K_0 = \mathbb{Q}$.

The above proposition is analogue to theorem 2 of Tomás [7]. For every prime ideal $\mathscr{P}$ of K let $W_{\mathscr{P}}$ be the smallest normal subgroup of G containing the decomposition group $D_{\mathscr{P}}$. If $\mathscr{P}$, $\mathscr{P}'$ are prime ideals of K dividing the same prime ideal $\mathscr{P}_0$ of K_0 then $D_{\mathscr{P}}$, $D_{\mathscr{P}'}$, are conjugate subgroups of G and $W_{\mathscr{P}} = W_{\mathscr{P}'}$; we denote this group by $W_{\mathscr{P}_0}$. Let $\mathscr{W}$ be the family of all such normal subgroups $W_{\mathscr{P}_0}$ of G. With action given by conjugation, $\mathscr{W}$ is an active normal family of groups. Tomás considered their active sum $\overline{W}$, in the category of *all* groups and he showed the existence of a canonical homomorphism $\overline{\psi} : \overline{W} \to G$, such that the image is the subgroup of G generated by the union of all subgroups $W_{\mathscr{P}_0}$ (actually, since G is the union of the subgroups $D_{\mathscr{P}}$, hence also of the subgroups $W_{\mathscr{P}_0}$, then $\overline{\psi}(\overline{W}) = G$). In this paper, using the general construction of active sums of active families of profinite groups (which in case of Tomás, must be an active normal family), we do not have to consider the normal subgroups $W_{\mathscr{P}_0}$ and may work with the decomposition groups.

Bibliography

[1] Diáz-Barriga, A.J. & López, L.Y.; *Sumas activas de grupos pro-$\mathscr{C}$*, Anales del Instituto de Matemáticas, Univ. México, 19, 1979, 21-40.

[2] Lang, S.; *Algebraic Number Theory*, Addison-Wesley, 1970, Reading, Massachussets.

[3] Neukirch, J.; *Freie Produkte pro-endlicher Gruppen und ihre Kohomologie*, Archiv der Math., 22, 1971, 337-357.

[4] Ribenboim, P.; *Active sums of groups*, Journal f.d. reine u.angew. Math., 325, 1981, 153-182.

[5] Ribes, L.; *Introduction to Profinite Groups and Galois Cohomology*, Queen's Papers in Pure and Applied Math., 24, 1970, Queen's University, Kingston, Ontario, Canada.

[6] Tomás, F.; *Un análogo de suma directa para sistemas de subgrupos normales*, Anales del Instituto de Matemáticas, Univ. Mexico, 13, 1973, 161-186.

[7] Tomás, F.; *Sobre los normalizados de los grupos de descomposicion*, Anales del Instituto de Matemáticas Univ. Mexico, 13, 1973, 187-208.

P. Ribenboim
Queen's University
Kingston
Ontario
Canada