数理解析研究所講究録
第 1872 巻 2014 年 113-121

Fast decomposition of p-groups in the Roquette category, for $p>2$

Serge Bouc

Abstract : Let p be a prime number. In [9], I introduced the *Roquette category* $\mathcal{R}_p$ of finite p-groups, which is an additive tensor category containing all finite p-groups among its objects. In $\mathcal{R}_p$, every finite p-group P admits a canonical direct summand ∂P, called *the edge* of P. Moreover P splits uniquely as a direct sum of edges of *Roquette p-groups.*

In this note, I would like to describe a fast algorithm to obtain such a decomposition, when p is odd.

AMS Subject classification : 18B99, 19A22, 20C99, 20J15.

Keywords : p-group, Roquette, rational, biset, genetic.

1. Introduction

Let p be a prime number. The Roquette category $\mathcal{R}_p$ of finite p-groups, introduced in [9], is an additive tensor category with the following properties :

- Every finite p-group can be viewed as an object of $\mathcal{R}_p$. The tensor product of two finite p-groups P and Q in $\mathcal{R}_p$ is the direct product $P\times Q$.
- In $\mathcal{R}_p$, any finite p-group has a direct summand ∂P, called *the edge* of P, such that
$$P\cong \bigoplus_{N\trianglelefteq P}\partial(P/N)\ .$$
Moreover, if the center of P is not cyclic, then $\partial P=0$.
- In $\mathcal{R}_p$, every finite p-group P decomposes as a direct sum
$$P\cong\bigoplus_{R\in\mathcal{S}}\partial R\ ,$$
where $\mathcal{S}$ is a finite sequence of *Roquette groups*, i.e. of p-groups of normal p-rank 1, and such a decomposition is essentially unique. Given the group P, such a decomposition can be obtained explicitly from the knowledge of a *genetic basis* of P.
- The tensor product $\partial P\times\partial Q$ of the edges of two Roquette p-groups P and Q is isomorphic to a direct sum of a certain number $\nu_{P,Q}$ of copies of the edge $\partial(P\diamond Q)$ of another Roquette group (where both $\nu_{P,Q}$ and $P\diamond Q$ are known explicitly.

- The additive functors from $\mathcal{R}_p$ to the category of abelian groups are exactly the *rational p-biset functors* introduced in [4].

The latter is the main motivation for considering this category : any structural result on $\mathcal{R}_p$ will provide for free some information on such rational functors for p-groups, e.g. the representation functors R_K, where K is a field of characteristic 0 (see [2], [3], and L. Barker's article [1]), the functor of units of Burnside rings ([6]), or the torsion part of the Dade group ([5]).

The decomposition of a finite p-group P as a direct sum of edges of Roquette p-groups can be read from the knowledge of a genetic basis of P. The problem is that the computation of such a basis is rather slow, in general. For most purposes however, the full details encoded in a genetic basis are useless, and it would be enough to know the direct sum decomposition.

Hence it would be nice to have a fast algorithm taking any finite p-group P as input, and giving its decomposition as direct sum of edges of Roquette groups in the category $\mathcal{R}_p$. This note is devoted to the description of such an algorithm, when $p > 2$.

2. Rational p-biset functors

2.1. Recall that the characteristic property of the edge ∂P of a finite p-group in the Roquette category $\mathcal{R}_p$ is that for any rational p-biset functor F

$$\partial F(P) = \hat{F}(\partial P) \ ,$$

where $\partial F(P)$ is the faithful part of $F(P)$, and $\hat{F}$ denotes the extension of F to $\mathcal{R}_p$. Also recall the following criterion ([7], Theorem 3.1):

2.2. Theorem : *Let p be a prime number, and F be a p-biset functor. Then the following conditions are equivalent:*

1. *The functor F is a rational p-biset functor.*
2. *For any finite p-group P, the following conditions hold:*
   - *if the center of P is non cyclic, then* $\partial F(P) = \{0\}$.
   - *if* $E \trianglelefteq P$ *is a normal elementary abelian subgroup of rank 2, and if* $Z \leq E$ *is a central subgroup of order p of P, then the map*

$$\mathrm{Res}^P_{C_P(E)} \oplus \mathrm{Def}^P_{P/Z} : F(P) \to F\big(C_P(E)\big) \oplus F(P/Z)$$

   is injective.

2.3. Let K be a commutative ring in which p is invertible. When P is a finite group, denote by $\mathsf{CF}_K(P)$ the K-module of central functions from P to K. The correspondence sending a finite p-group P to $\mathsf{CF}_K(P)$ is a rational p-biset functor:

2.4. Proposition : *If P and Q are finite p-groups, if U is a finite (Q,P)-biset, and if $f \in \mathsf{CF}_K(P)$, define a map $\mathsf{CF}_K(U) : \mathsf{CF}_K(P) \to \mathsf{CF}_K(Q)$ by*

$$\forall s \in Q,\ \ \mathsf{CF}_K(U)(f)(s) = \tfrac{1}{|P|} \sum_{\substack{u\in U,\, x\in P\\ su=ux}} f(x)\ .$$

With this definition, the correspondence $P \mapsto \mathsf{CF}_K(P)$ becomes a rational p-biset functor, denoted by CF_K.

Proof : A straightforward argument shows that $\mathsf{CF}_K(U)(f)$ is indeed a central function on Q, hence the map $\mathsf{CF}_K(U)$ is well defined. It is also clear that this map only depends on the isomorphism class of the biset U, and that for any two finite (H,G)-bisets U and U', we have

$$\mathsf{CF}_K(U \sqcup U') = \mathsf{CF}_K(U) + \mathsf{CF}_K(U')\ .$$

Moreover if U is the identity biset at P, i.e. if $U = P$ with biset structure given by left and right multiplication, then for $f \in \mathsf{CF}_K(P)$ and $s \in P$

$$\mathsf{CF}_K(U)(f)(s) = \tfrac{1}{|P|} \sum_{\substack{u\in U,\, x\in P\\ su=ux}} f(x) = \tfrac{1}{|P|} \sum_{u\in P} f(s^u) = f(s)\ ,$$

hence $\mathsf{CF}_K(U)$ is the identity map.

Now if R is a third finite p-group, and V is a finite (R,Q)-biset, then for any $t \in R$, setting $\lambda = \mathsf{CF}_K(V) \circ \mathsf{CF}_K(U)(f)(t)$, we have that

$$\begin{aligned}
\lambda &= \tfrac{1}{|Q|} \sum_{\substack{v\in V,\, s\in Q\\ tv=vs}} \tfrac{1}{|P|} \sum_{\substack{u\in U,\, x\in P\\ su=ux}} f(x)\\
&= \tfrac{1}{|Q||P|} \sum_{\substack{(v,u)\in V\times U\\ s\in Q,\, x\in P\\ tv=vs,\, su=ux}} f(x)\\
&= \tfrac{1}{|Q||P|} \sum_{\substack{(v,u)\in V\times U,\, x\in P\\ t(v,_Q u)=(v,_Q u)x}} |\{s \in Q \mid tv = vs,\ su = ux\}|\, f(x)
\end{aligned}$$

$$\begin{aligned}\lambda &= \frac{1}{|Q||P|}\sum_{\substack{(v,_Q u)\in V\times_Q U,\, x\in P\\ t(v,_Q u)=(v,_Q u)x}} |Q:Q_v\cap {}_uP||Q_v\cap {}_uP|\, f(x)\\ &= \frac{1}{|P|}\sum_{\substack{(v,_Q u)\in V\times_Q U,\, x\in P\\ t(v,_Q u)=(v,_Q u)x}} f(x) = \mathsf{CF}_K(V\times_Q U)(f)(t)\ .\end{aligned}$$

Hence $\mathsf{CF}_K(V)\circ\mathsf{CF}_K(U)=\mathsf{CF}_K(V\times_Q U)$, and CF_K is a p-biset functor.

To prove that this functor is rational, we use the criterion given by Theorem 2.2. Suppose first that the center $Z(P)$ of P is non-cyclic. Let E denote the subgroup of $Z(P)$ consisting of elements of order at most p. Then saying that $\partial\mathsf{CF}_K(P)=\{0\}$ amounts to saying that for any $f\in\mathsf{CF}_K(P)$, the sum

$$S=\sum_{Z\leq E}\mu(\mathbf{1},Z)\mathrm{Inf}_{P/Z}^P\mathrm{Def}_{P/Z}^P f$$

is equal to 0, where μ denotes the Möbius function of the poset of subgroups of P (or of E). Equivalently, for any $s\in P$

$$S(s)=\sum_{Z\leq E}\mu(\mathbf{1},Z)\frac{1}{|P|}\sum_{\substack{aZ\in P/Z,\, x\in P\\ saZ=aZx}} f(x)=0\ .$$

This also can be written as

$$\begin{aligned}S(s) &= \sum_{Z\leq E}\mu(\mathbf{1},Z)\frac{1}{|P||Z|}\sum_{\substack{a\in P,\, x\in P\\ saZ=aZx}} f(x)\\ &= \frac{1}{|P|}\sum_{Z\leq E}\frac{\mu(\mathbf{1},Z)}{|Z|}\sum_{a\in P,\, z\in Z} f(s^a.z)\\ &= \frac{1}{|P|}\sum_{Z\leq E}\frac{\mu(\mathbf{1},Z)}{|Z|}\sum_{a\in P,\, z\in Z} f\big((sz)^a\big)\\ &= \sum_{Z\leq E}\frac{\mu(\mathbf{1},Z)}{|Z|}\sum_{z\in Z} f(sz)\\ &= \sum_{z\in E}\Big(\sum_{z\in Z\leq E}\frac{\mu(\mathbf{1},Z)}{|Z|}\Big)f(sz)\ .\end{aligned}$$

2.5. Lemma : *Let E be an elementary abelian p-group of rank at least 2. Then for any $z\in E$*

$$\sum_{z\in Z\leq E}\frac{\mu(\mathbf{1},Z)}{|Z|}=0\ .$$

Proof : For $z \in E$, set $\sigma(z) = \sum_{z \in Z \leq E} \frac{\mu(1,Z)}{|Z|}$. Assume first that $z \neq 1$, i.e. $|z| = p$. If $Z \ni z$ is elementary abelian of rank r, then $\mu(\mathbf{1}, Z) = (-1)^r p^{\binom{r}{2}}$, hence $\frac{\mu(1,Z)}{|Z|} = (-1)^r p^{\binom{r-1}{2}-1} = -\frac{1}{p}\mu(\mathbf{1}, Z/\langle z\rangle)$. Hence setting $\overline{Z} = Z/\langle z\rangle$ and $\overline{E} = E/\langle z\rangle$,

$$\sigma(z) = -\frac{1}{p} \sum_{\mathbf{1} \leq \overline{Z} \leq \overline{E}} \mu(\mathbf{1}, \overline{Z}) = 0 \ ,$$

since $|\overline{E}| > 1$. Now

$$\sum_{z \in E} \sigma(z) = \sigma(1) + \sum_{e \in E - \{1\}} \sigma(z) = \sum_{z \in Z} \sum_{z \in Z \leq E} \frac{\mu(1,Z)}{|Z|} = \sum_{\mathbf{1} \leq Z \leq E} \mu(\mathbf{1}, Z) = 0$$

hence $\sigma(1) = 0$, completing the proof of the lemma. □

It follows that $S(s) = 0$, hence $S = 0$, as was to be shown.

For the second condition of Theorem 2.2, suppose that E is a normal elementary abelian subgroup of P of rank 2, and that Z is a central subgroup of P of order p contained in E. Let $f \in \mathsf{CF}_K(P)$ which restricts to 0 to $C_P(E)$, and such that

$$\forall sZ \in P/Z, \ \ (\mathrm{Def}^P_{P/Z} f)(sZ) = \frac{1}{|P|} \sum_{z \in Z} f(sz) = 0 \ .$$

Thus $f(s) = 0$ if $s \in C_P(E)$. Assume that $s \notin C_P(E)$. Then for $e \in E$, the commutator $[s, e]$ lies in Z. Moreover the map $e \in E \mapsto [s, e] \in Z$ is surjective. it follows that for any $z \in Z$, there exists $e \in E$ such that $s^e = sz$. Thus $f(sz) = f(s^e) = f(s)$. Hence $\mathrm{Def}^P_{P/Z} f(s) = f(s) = 0$. Hence $f = 0$, as was to be shown. □

3. Action of p-adic units

Let $\mathbb{Z}_p$ denote the ring of p-adic integers, i.e. the inverse limit of the rings $\mathbb{Z}/p^n\mathbb{Z}$, for $n \in \mathbb{N} - \{0\}$. The group of units $\mathbb{Z}_p^\times$ is the inverse limits of the unit groups $(\mathbb{Z}/p^n\mathbb{Z})^\times$, and it acts on the functor CF_K in the following way: if $\zeta \in \mathbb{Z}_p^\times$ and P is a finite p-group, choose an integer r such that p^r is a multiple of the exponent of P, and let ζ_{p^r} denote the component of ζ in $(\mathbb{Z}/p^r\mathbb{Z})^\times$. For $f \in \mathsf{CF}_K(P)$, define $\widehat{\zeta_P}(f) \in \mathsf{CF}_K(P)$ by

$$\forall s \in P, \ \ \widehat{\zeta_P}(f)(s) = f(s^{\zeta_{p^r}}) \ .$$

Then clearly $\widehat{\zeta}_P(f)$ only depends on ζ, and this gives a well defined map

$$\widehat{\zeta}_P : \mathsf{CF}_K(P) \to \mathsf{CF}_K(P) \ .$$

One can check easily (see [8] Proposition 7.2.4 for details) that if Q is a finite p-group, and U is a finite (Q,P)-biset, then the square

$$\begin{array}{ccc} \mathsf{CF}_K(P) & \xrightarrow{\widehat{\zeta}_P} & \mathsf{CF}_K(P) \\ {\scriptstyle \mathsf{CF}_K(U)}\downarrow & & \downarrow{\scriptstyle \mathsf{CF}_K(U)} \\ \mathsf{CF}_K(Q) & \xrightarrow{\widehat{\zeta}_Q} & \mathsf{CF}_K(Q) \end{array}$$

is commutative. In other words, we have an endomorphism $\widehat{\zeta}$ of the functor CF_K. It is straightforward to check that for $\zeta,\zeta' \in \mathbb{Z}_p^\times$, we have $\widehat{\zeta\zeta'} = \widehat{\zeta}\circ\widehat{\zeta'}$, and that $\widehat{1}$ is the identity endomorphism of CF_K. So this yields an action of the group $\mathbb{Z}_p^\times$ on CF_K.

It follows in particular that when $n \in \mathbb{N}-\{0\}$, and P is a finite p-group, if we set

$$F_n(P) = \{f \in \mathsf{CF}_K(P) \mid \forall s \in P,\ f(s^{1+p^n}) = f(s)\} \ ,$$

then the correspondence $P \mapsto F_n(P)$ is a subfunctor of CF_K: indeed F_n is the subfunctor of invariants by the element $1+p^n$ of $\mathbb{Z}_p^\times$.

It follows that F_n is a rational p-biset functor, for any $n \in \mathbb{N}-\{0\}$, hence it factors through the Roquette category $\mathcal{R}_p$. In particular, for any finite p-group P, if P splits as a direct sum

$$P \cong \mathop{\oplus}_{R\in\mathcal{S}} \partial R$$

of edges of Roquette groups in $\mathcal{R}_p$, then there is an isomorphism

$$F_n(P) \cong \mathop{\oplus}_{R\in\mathcal{S}} \partial F_n(R) \ .$$

3.1. Notation : *For a finite p-group P, and an integer $n \in \mathbb{N}-\{0\}$, let $l_n(P)$ denote the number of conjugacy classes of elements s of P such that s^{1+p^n} is conjugate to s in P. Also set $l_0(P) = 1$.*

With this notation, for any finite p-group P, and any $n \in \mathbb{N}-\{0\}$, the K-module $F_n(P)$ is a free K-module of rank $l_n(P)$. In particular, if $P = C_{p^m}$ is cyclic of order p^m, then $F_n(P)$ has rank $l_n(P) = p^{\min(m,n)}$. Thus if $m > 0$, then $\partial F_n(C_{p^m})$ has rank $p^{\min(m,n)} - p^{\min(m-1,n)}$, since $C_{p^m} \cong \partial C_{p^m} \oplus C_{p^{m-1}}$ in $\mathcal{R}_p$.

3.2. Theorem : *Assume that a p-group P splits as a direct sum*

$$P \cong \mathbf{1} \oplus \bigoplus_{m=1}^{\infty} a_m \partial C_{p^m}$$

of edges of cyclic groups in the Roquette category $\mathcal{R}_p$, where $a_m \in \mathbb{N}$. Then

$$\forall m \geq 1, \quad a_m = \frac{l_m(P) - l_{m-1}(P)}{p^{m-1}(p-1)} \quad .$$

Proof : For any $n \in \mathbb{N} - \{0\}$, we have

$$l_n(P) = 1 + \sum_{m=1}^{\infty} a_m(p^{\min(m,n)} - p^{\min(m-1,n)}) = 1 + \sum_{m=1}^{n} a_m(p^m - p^{m-1}) \quad .$$

For $n \in \mathbb{N} - \{0\}$, this gives $l_n(P) - l_{n-1}(P) = a_n(p^n - p^{n-1})$. □

3.3. Corollary : *Suppose $p > 2$. If P is a finite p-group, then*

$$P \cong \mathbf{1} \oplus \bigoplus_{m=1}^{\infty} \frac{l_m(P)-l_{m-1}(P)}{p^{m-1}(p-1)} \partial C_{p^m}$$

in the Roquette category $\mathcal{R}_p$.

Proof : Indeed for p odd, all the Roquette p-groups are cyclic, hence the assumption of Theorem 3.2 holds for any P. □

Appendix

3.1. A GAP function : The following function for the GAP software ([10]) computes the decomposition of p-groups for $p > 2$, using Corollary 3.3:

```
#
# Roquette decomposition of an odd order p-group g
# output is a list of pairs of the form [p^n,a_n]
# where a_n is the number of summands of g
# isomorphic to the edge of the cyclic group of order p^n
#
```

```
roquette_decomposition:=function(g)
local prem,cg,s,i,x,y,z,pn,u;
    if IsTrivial(g) then return [[1,1]];fi;
    prem:=PrimeDivisors(Size(g));
    if Length(prem)>1 then
        Print("Error : the group must be a p-group\n");
        return fail;
    fi;
    prem:=prem[1];
    if prem=2 then
        Print("Error : the order must be odd\n");
        return fail;
    fi;
    cg:=ConjugacyClasses(g);
    s:=[];
    for i in [2..Length(cg)] do
        x:=cg[i];
        y:=Representative(x);
        pn:=1;
        u:=y;
        repeat
            pn:=pn*prem;
            u:=u^prem;
            z:=y*u;
        until z in x;
        Add(s,pn);
    od;
    s:=Collected(s);
    s:=List(s,x->[x[1],x[2]*prem/(prem-1)/x[1]]);
    s:=Concatenation([[1,1]],s);
    return s;
end;
```

3.2. Example :

```
gap> l:=AllGroups(81);;
gap> for g in l do
> Print(roquette_decomposition(g),"\n");
> od;
[ [ 1, 1 ], [ 3, 1 ], [ 9, 1 ], [ 27, 1 ], [ 81, 1 ] ]
[ [ 1, 1 ], [ 3, 4 ], [ 9, 12 ] ]
[ [ 1, 1 ], [ 3, 7 ], [ 9, 3 ] ]
[ [ 1, 1 ], [ 3, 7 ], [ 9, 3 ] ]
[ [ 1, 1 ], [ 3, 4 ], [ 9, 3 ], [ 27, 3 ] ]
[ [ 1, 1 ], [ 3, 4 ], [ 9, 4 ] ]
[ [ 1, 1 ], [ 3, 8 ] ]
[ [ 1, 1 ], [ 3, 5 ], [ 9, 1 ] ]
[ [ 1, 1 ], [ 3, 5 ], [ 9, 1 ] ]
[ [ 1, 1 ], [ 3, 5 ], [ 9, 1 ] ]
```

```
[ [ 1, 1 ], [ 3, 13 ], [ 9, 9 ] ]
[ [ 1, 1 ], [ 3, 16 ] ]
[ [ 1, 1 ], [ 3, 16 ] ]
[ [ 1, 1 ], [ 3, 13 ], [ 9, 1 ] ]
[ [ 1, 1 ], [ 3, 40 ] ]
```

For example, the group on line 6 of the previous list, isomorphic to the semidirect product $C_{27} \rtimes C_3$, is isomorphic to $\mathbf{1} \oplus 4\partial C_3 \oplus 4\partial C_9$ in $\mathcal{R}_3$.

References

[1] L. Barker. Rhetorical biset functors, rational p-biset functors, and their semisimplicity in characteristic zero. *J. of Algebra*, 319(9):3810–3853, 2008.

[2] S. Bouc. Foncteurs d'ensembles munis d'une double action. *J. of Algebra*, 183(0238):664–736, 1996.

[3] S. Bouc. The functor of rational representations for p-groups. *Advances in Mathematics*, 186:267–306, 2004.

[4] S. Bouc. Biset functors and genetic sections for p-groups. *J. of Algebra*, 284(1):179–202, 2005.

[5] S. Bouc. The Dade group of a p-group. *Inv. Math.*, 164:189–231, 2006.

[6] S. Bouc. The functor of units of Burnside rings for p-groups. *Comm. Math. Helv.*, 82:583–615, 2007.

[7] S. Bouc. Rational p-biset functors. *J. of Algebra*, 319:1776–1800, 2008.

[8] S. Bouc. *Biset functors for finite groups*, volume 1990 of *Lecture Notes in Mathematics*. Springer, 2010.

[9] S. Bouc. The Roquette category of finite p-groups. preprint, `http://fr.arxiv.org/abs/1111.3469`, 2011.

[10] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.6.3*, 2013. (`http://www.gap-system.org`).

Serge Bouc - CNRS-LAMFA, Université de Picardie, 33 rue St Leu, 80039, Amiens Cedex 01 - France.
`email : serge.bouc@u-picardie.fr`
`web : http://www.lamfa.u-picardie.fr/bouc/`