# Polynomial ideals and classes of finite groups

Serge Bouc

The object of this note is to discuss properties of some polynomials (on a countable set of indeterminates) attached to any finite group, which generalize the Eulerian functions of a group defined by P. Hall ([8]). In particular, I will define some classes of finite groups associated to prime ideals of the polynomial ring, and I will show that each finite group has a unique largest quotient in such a class of groups.

This work is a generalization of the notion of $b$-group introduced in [2], by a systematic use of the polynomial formalism of section 7.2.5 of [2]. For the reader's convenience however, this paper is self-contained, and the proofs of the results already stated in [2] are included.

## 1. The polynomial ring

**(1.1) Notation:** *I will consider the (countable) set $\mathcal{S}$ of isomorphism classes of finite (non-trivial) simple groups, and the polynomial ring over $\mathcal{S}$*

$$\mathcal{R} = \mathbb{Z}[(X_S)_{S\in\mathcal{S}}]$$

In other words, the ring $\mathcal{R}$ is the algebra over $\mathbb{Z}$ of the Grothendieck *monoid* of the category of finite groups.

**(1.2) Notation:** *If $p$ is a prime number, and $S$ is the isomorphism class of the cyclic group $C_p$ of order $p$, I denote by $X_p$ the variable $X_S$ of $\mathcal{R}$.*

It is convenient to turn $\mathcal{R}$ into a $\mathbb{R}$-graded ring by setting

$$\deg(X_S) = \log|S|$$

If $G$ is a finite group, then I define the monomial $P(G) \in \mathcal{R}$ by

$$P(G) = \prod_{S\in\mathcal{S}} X_S^{\nu_S(G)}$$

where for each finite simple group $S$, the integer $\nu_S(G)$ is the multiplicity of $S$ as a composition factor of $G$. In particular $P(1) = 1$ and $P(S) = X_S$ if $S \in \mathcal{S}$. Note that with this definition, the degree of $P(G)$ is equal to $\log|G|$, for any finite group $G$.

I denote by $\tilde{P}(G)$ the polynomial obtained from $P(G)$ by Möbius inversion on the poset of subgroups of $G$, i.e.

$$\tilde{P}(G) = \sum_{H\leq G} \mu(H,G)P(H)$$

where the notation $H \leq G$ means that $H$ is a subgroup of $G$, and $\mu(H,G)$ is the Möbius function of the poset of subgroups of $G$. The monomial of highest degree in the expression of $\tilde{P}(G)$ corresponds to the subgroup $H = G$, and the coefficient $\mu(G, G)$ is equal to 1. Thus

$$\deg\big(\tilde{P}(G)\big) = \log|G| \tag{1.3}$$

Finally, if $N$ is a normal subgroup of $G$, I define

$$Q_{G,N} = \sum_{\substack{H \leq G \\ HN = G}} \mu(H, G) P(H \cap N)$$

This is a generalization of the previous formula, since $Q_{G,G} = \tilde{P}(G)$. On the other hand $Q_{G,1} = 1$ for any $G$. The terms of highest degree in $Q_{G,N}$ correspond to subgroups $H$ such that $H \cap N = N$ and $HN = G$. Hence the only possible subgroup is $H = G$, and again the coefficient of $P(H \cap N) = P(N)$ is equal to 1. Thus

$$\deg(Q_{G,N}) = \log|N| \tag{1.4}$$

The polynomials $P(G)$, $\tilde{P}(G)$, and $Q_{G,N}$ are invariant under group isomorphism: if $\varphi : G \to G'$ is an isomorphism, then obviously $P(G) = P(G')$, $\tilde{P}(G) = \tilde{P}(G')$, and $Q_{G,N} = Q_{G',\varphi(N)}$.

(**1.5**) **Remark:** The Eulerian function of the group $G$, defined by Hall ([8]), is the function $\phi(G, s)$ defined for a complex number $s$ by

$$\phi(G, s) = \sum_{H \leq G} \mu(H, G)|H|^s$$

Hence it is the evaluation of the polynomial $\tilde{P}(G)$ when $X_S$ is replaced by $|S|^s$, for all $S \in \mathcal{S}$. The name "Eulerian" comes from the fact that when $s$ is a positive integer, the value $\phi(G, s)$ is the number of sequences of $s$ elements of $G$ which generate $G$.

The polynomials $\tilde{P}(G)$ and $Q_{G,N}$ are also closely related to the *probabilistic zeta function* and its relative version, studied by K. Brown in [4]. The value $\zeta(G, s)$ of this zeta function at a complex number $s$ is given by

$$1/\zeta(G, s) = \frac{\phi(G, s)}{|G|^s} = \sum_{H \leq G} \frac{\mu(G, H)}{|G : H|^s}$$

(Brown's notation for $1/\zeta(G, s)$ is $P(G, s)$, but it is a bit confusing here, and I prefer to use another symbol).

Hence the value $\zeta(G, s)|G|^{-s}$ can also be recovered from $1/\tilde{P}(G)$ by replacing each variable $X_S$ by $|S|^s$.

(**1.6**) **Remark:** Let $\mathcal{D}$ denote the ring of Dirichlet polynomials over $\mathbb{Z}$, i.e. the ring of finite linear combinations with coefficients in $\mathbb{Z}$ of functions $s \mapsto n^{-s}$ from $\mathbb{C}$ to $\mathbb{C}$, for $n \in \mathbb{N} - \{0\}$. It is clear that the map sending $X_S \in \mathcal{R}$ for $S \in \mathcal{S}$ to the map $s \mapsto |S|^{-s}$ induces a surjective ring homomorphism from $\mathcal{R}$ to $\mathcal{D}$.

On the other hand, the decomposition of an integer $n \in \mathbb{N} - \{0\}$ as a product of prime factors yields an isomorphism from $\mathcal{D}$ to the algebra $\mathcal{R}'$ over $\mathbb{Z}$ of the multiplicative monoid $\mathbb{N} - \{0\}$, sending the function $s \mapsto n^{-s}$ to $\prod_{p \in \mathcal{P}} Y_p^{v_p(n)}$, where $\mathcal{P}$ is the set of prime numbers and $v_p(n)$ is the $p$-valuation of $n$, for $p \in \mathcal{P}$, and $Y_p$ is the image of the prime $p$ in $\mathcal{R}'$.

Hence the ring $\mathcal{D}$ is isomorphic to the quotient of $\mathcal{R}$ by the ideal generated by the elements $X_S - \prod_{p \in \mathcal{P}} X_p^{v_p(|S|)}$, for all non-abelian simple groups $S$.

The fundamental properties of the polynomial $P(G)$, $\tilde{P}(G)$, and $Q_{G,N}$ are given in the following lemma:

**(1.7) Lemma:** [[2] Lemme 19] *The $G$ be a finite group, let $N$ be a normal subgroup of $G$, and let $R$ be a subgroup of $G$ containing $N$. Then*

$$P(G) = P(G/N)P(N) \tag{1.8}$$

$$\sum_{\substack{H \leq G \\ HN=R}} \mu(H,G)P(H) = \mu(R,G)P(R/N)Q_{G,N} \tag{1.9}$$

$$\sum_{\substack{H \leq G \\ HN=R}} \mu(H,G)P(H \cap N) = \mu(R,G)Q_{G,N} \tag{1.10}$$

$$\tilde{P}(G) = \tilde{P}(G/N)Q_{G,N} \tag{1.11}$$

**Proof:** The first equality is a trivial consequence of the definition, since the multiplicity of the simple group $S$ as a composition factor of $G$ is the sum of its multiplicities as a composition factor of $N$ and $G/N$.

For the second one, by Crapo complementation formula (see [6] Theorem 3 and Theorem 5, or [5] pp. 420-421), for $H \leq G$

$$\mu(H,G) = \sum_{\substack{H \leq K \leq G \\ KN=G \\ K \cap HN=H}} \mu(H,K)\mu(K,G) = \sum_{\substack{H \leq K \leq G \\ KN=G \\ K \cap HN=H}} \mu(HN,G)\mu(K,G)$$

Now if $N \leq R \leq G$, the conditions $KN = G$, $K \cap HN = H$ and $HN = R$ are equivalent to $KN = G$ and $H = K \cap R$. This gives

$$\begin{aligned}
\sum_{\substack{H \leq G \\ HN=R}} \mu(H,G)P(H) &= \sum_{\substack{K \leq G \\ KN=G}} \mu(R,G)\mu(K,G)P(K \cap R) \\
&= \mu(R,G) \sum_{\substack{K \leq G \\ KN=G}} \mu(K,G)P(K \cap R)
\end{aligned}$$

Moreover $(K \cap R)N = R$, thus $R/N \simeq (K \cap R)/(K \cap N)$, and

$$P(K \cap R) = P(R/N)P(K \cap N)$$

It follows that for $N \leq R \leq G$

$$\sum_{\substack{H \leq G \\ HN=R}} \mu(H,G)P(H) = \mu(R,G)P(R/N) \sum_{\substack{K \leq G \\ KN=G}} \mu(K,G)P(K \cap N)$$

and equality 1.9 follows. Equality 1.10 is a consequence, since if $HN = R$, then $P(H) = P(R/N)P(H \cap N)$.

Since moreover $\mu(R,G) = \mu(R/N, G/N)$, the summation of 1.9 for subgroups $R$ with $N \leq R \leq G$ gives

$$\tilde{P}(G) = \sum_{N \leq R \leq G} \mu(R,G)P(R/N)Q_{G,N} = \tilde{P}(G/N)Q_{G,N}$$

as was to be shown. □

(**1.12**) **Corollary:** *If $M$ and $N$ are normal subgroups of $G$ such that $G/M \simeq G/N$, then $Q_{G,M} = Q_{G,N}$.*

**Proof:** Indeed by 1.11 $Q_{G,N} = \tilde{P}(G)/\tilde{P}(G/N)$. □

## 2. The polynomials $\tilde{P}(G)$

In view of 1.11, it is natural to ask when the polynomial $\tilde{P}$ is irreducible:

(**2.1**) **Proposition:** *Let $G$ be a finite group. Then $\tilde{P}$ is irreducible if and only if $G$ is simple.*

**Proof:** Let $S$ be a simple group. Then

$$\tilde{P}(S) = X_S + R$$

where $R$ is a polynomial in the variables $X_T$, for simple groups $T$ not isomorphic to $S$. Hence $\tilde{P}(S)$ is irreducible.

Conversely, if $G$ is a finite group and $\tilde{P}(G)$ is irreducible, let $N$ be a normal subgroup of $G$. Then by 1.11 one of the polynomial $\tilde{P}(G/N)$ or $Q_{G,N}$ has degree 0. By 1.3 and 1.4, it follows that $N = G$ or $N = 1$. Hence $G$ is simple. □

(**2.2**) **Notation:** *If $N$ is a normal subgroup of $G$, I denote by $K_G(N)$ the set of complements of $N$ in $G$, i.e.*

$$K_G(N) = \{L \leq G \mid LN = G,\ L \cap N = 1\}$$

*If $M$ and $N$ are normal subgroups of $G$, I denote by $K_G(M,N)$ the set of subgroups of $G$ which are complements of $M$ and $N$, i.e.*

$$K_G(M,N) = K_G(M) \cap K_G(N)$$

**(2.3) Proposition:** *Let $G$ be a finite group, and $N$ be a minimal (non-trivial) abelian normal subgroup of $G$, isomorphic to $(C_p)^n$, for $p$ prime and $n > 0$. Then*

$$Q_{G,N} = X_p^n - |K_G(N)|$$

**Proof:** Let $H$ be a subgroup of $G$ such that $HN = G$. Then $H \cap N$ is normalized by $H$, and by $N$ since $N$ is abelian. Hence either $H \cap N = N$, and then $H = G$, or $H \cap N = 1$, and $H \in K_G(N)$. In this case $H$ is a maximal subgroup of $G$, and $\mu(H, G) = -1$. The proposition follows. □

**(2.4) Corollary:**

1. *Let $G$ be a solvable finite group, and*

$$1 = N_{-1} < N_0 < N_1 < \ldots < N_k = G$$

*be a chief series for $G$. Then for $0 \leq i \leq k$, there exist a prime number $p_i$ and a positive integer $n_i$ such that $N_i/N_{i-1} \simeq (C_{p_i})^{n_i}$. Denote by $m_i$ the number of complements of $N_i/N_{i-1}$ in the group $G/N_{i-1}$. Then*

$$\tilde{P}(G) = \prod_{i=0}^{k} (X_{p_i}^{n_i} - m_i) \qquad (2.5)$$

2. *Conversely, if $G$ is a finite group, and if there exists an integer $k$, if there exist prime numbers $p_i$ and integers $m_i$, for $0 \leq i \leq k$ such that 2.5 holds, then $G$ is solvable.*

**Proof:** Assertion 1) follows from an obvious induction argument. For assertion 2), suppose that $G$ is a finite group such that 2.5 holds. Then the monomial of highest degree in $\tilde{P}(G)$, which is equal to $P(G)$, is the product $\prod_{i=0}^{k} X_{p_i}^{n_i}$. This means that all the composition factors of $G$ are cyclic, i.e. that $G$ is solvable. □

**(2.6) Remark:** Corollary 2.4 can be viewed as a generalization of the Eulerian product formula obtained by Gaschütz ([7]) for the zeta function of a solvable group (see also [1]). It should also be compared with the following question, cited by Brown (Question 1 of [4]):

*Question:* If $G$ is a finite group such that $\zeta(G, s)$ has an Euler product expansion with factors of the form $\frac{1}{1-c_i q_i^{-s}}$, is $G$ solvable?

## 3. The two normal subgroups formula

**(3.1) Proposition:** [[2] Lemme 20] *Let $G$ be a finite group. If $N$ and $M$ are normal subgroups of $G$ then*

$$Q_{G,N} = \sum_{\substack{L \leq G \\ LM=LN=G}} \mu(L,G)P(L \cap M \cap N)Q_{G/M,(L\cap N)M/M}$$

**Proof:** By definition

$$Q_{G,N} = \sum_{\substack{H \leq G \\ HN=G}} \mu(H,G)P(H \cap N)$$

As noted above

$$\mu(H,G) = \sum_{\substack{H \leq L \leq G \\ LM=G \\ L\cap HM=H}} \mu(H,L)\mu(L,G)$$

This gives

$$Q_{G,N} = \sum_{\substack{H \leq G \\ HN=G}} \sum_{\substack{H \leq L \leq G \\ LM=G \\ L\cap HM=H}} \mu(H,L)\mu(L,G)P(H \cap N)$$

Now the conditions

$$HN = G \qquad H \leq L \qquad LM = G \qquad L \cap HM = H$$

are equivalent to the conditions

$$LM = LN = G \qquad H \leq L \qquad H(L \cap N) = L \qquad H \geq L \cap M$$

It follows that

$$Q_{G,N} = \sum_{\substack{L \leq G \\ LM=LN=G}} \mu(L,G) \sum_{\substack{H \leq L \\ H \geq L\cap M \\ H(L\cap N)=L}} \mu(H,L)P(H \cap N)$$

The inner summation is equivalent to a sum over subgroups $K = H/(L \cap M)$ of $\overline{L} = L/(L \cap M)$ such that $K.J = \overline{L}$, where $J$ denotes the normal subgroup $(L \cap N)(L \cap M)/(L \cap M)$ of $\overline{L}$.

Moreover since $HN = G$

$$\begin{aligned}
P(H \cap N) &= P(H)P(N)/P(G) = P(K)P(N)P(L \cap M)/P(G) \\
&= \frac{P(K \cap J)P(\overline{L})}{P(J)} P(N)P(L \cap M)/P(G) \\
&= \frac{P(K \cap J)P(L)P(N)}{P(J)P(G)} \\
&= \frac{P(K \cap J)P(L \cap N)}{P(L \cap N/L \cap N \cap M)} \\
&= P(K \cap J)P(L \cap M \cap N)
\end{aligned}$$

Thus

$$\begin{aligned} Q_{G,N} &= \sum_{\substack{L\leq G\\ LM=LN=G}} \mu(L,G)P(L\cap M\cap N) \sum_{\substack{K\leq \overline{L}\\ KJ=\overline{L}}} \mu(K,\overline{L})P(K\cap J) \\ &= \sum_{\substack{L\leq G\\ LM=LN=G}} \mu(L,G)P(L\cap M\cap N)Q_{\overline{L},J} \end{aligned}$$

The formula follows, since $\overline{L} \simeq G/M$, and since the image of $J$ under this isomorphism is $(L\cap N)M/M$. □

(**3.2**) **Corollary:** *If $M \leq N$, then*

$$Q_{G,N} = Q_{G,M}Q_{G/M,N/M}$$

**Proof:** This follows from the fact that if $LM = G$ and if $M \leq N$, then $(L\cap N)M = N$. This corollary has also an obvious direct proof, using 1.11. □

## 4. $\mathcal{I}$-groups

One of the methods used in [2] was to replace each variable $X_S$ by $|S|$, and to look whether the resulting number $Q_{G,N}$ is zero. This can be generalized by considering an ideal $\mathcal{I}$ of $\mathcal{R}$, and looking whether $Q_{G,N}$ is in $\mathcal{I}$ or not.

(**4.1**) **Convention:** *In the sequel, the expression "the group $H$ is a quotient of the group $G$" means that $H$ is isomorphic to a factor group of $G$.*

(**4.2**) **Definition:** *Let $\mathcal{I}$ be an ideal of $\mathcal{R}$. A finite group $G$ is called an $\mathcal{I}$-group if for any non-trivial normal subgroup $N$ of $G$, the polynomial $Q_{G,N}$ belongs to $\mathcal{I}$.*

(**4.3**) **Proposition:** *Let $G$ be a finite group, and $\mathcal{I}$ be an ideal of $\mathcal{R}$. If $M$ and $N$ are normal subgroups of $G$, and if $G/M$ is an $\mathcal{I}$-group, then*

$$Q_{G,N} \equiv \sum_{\substack{L\leq G\\ LM=LN=G\\ L\cap N\leq L\cap M}} \mu(L,G)P(L\cap N) \quad (mod.\ \mathcal{I})$$

*In particular, if $Q_{G,N} \notin \mathcal{I}$, then $G/M$ is a quotient of $G/N$.*

**Proof:** The first assertion follows from proposition 3.1, and from the definition of an $\mathcal{I}$-group. Now if $Q_{G,N} \notin \mathcal{I}$, then there exists a subgroup $L$ of $G$ such that $LM = LN = G$ and $L\cap N \leq L\cap M$. Now $G/M \simeq L/(L\cap M)$ is a quotient of $G/N \simeq L/(L\cap N)$. □

**(4.4) Proposition:** *Let $G$ be a finite group, and $\mathcal{I}$ be a prime ideal of $\mathcal{R}$. There exists a factor group $\beta_{\mathcal{I}}(G)$ of $G$, characterized uniquely up to isomorphism by the following properties:*

1. *The group $\beta_{\mathcal{I}}(G)$ is an $\mathcal{I}$-group.*
2. *If $K$ is a quotient of $G$, and if $K$ is an $\mathcal{I}$-group, then $K$ is a quotient of $\beta_{\mathcal{I}}(G)$.*

*Moreover if $N$ is a normal subgroup of $G$, then the following conditions are equivalent:*

a) *The group $\beta_{\mathcal{I}}(G)$ is a quotient of $G/N$.*

b) *$\beta_{\mathcal{I}}(G/N) \simeq \beta_{\mathcal{I}}(G)$.*

c) *$Q_{G,N} \notin \mathcal{I}$.*

**Proof:** Properties 1) and 2) clearly show that the group $\beta_{\mathcal{I}}(G)$ is unique up to isomorphism, if it exists.

Let $M$ be a normal subgroup of $G$, maximal subject to $Q_{G,M} \notin \mathcal{I}$. Then by Corollary 3.2, if $N$ is a normal subgroup of $G$ strictly containing $M$

$$Q_{G,N} = Q_{G,M} Q_{G/M,N/M} \in \mathcal{I}$$

Since $Q_{G,M} \notin \mathcal{I}$ and since $\mathcal{I}$ is prime, it follows that $Q_{G/M,N/M} \in \mathcal{I}$. This holds for any non-trivial normal subgroup $N/M$ of $G/M$, hence $G/M$ is an $\mathcal{I}$-group.

By Proposition 4.3, since $Q_{G,M} \notin \mathcal{I}$, it follows that any $\mathcal{I}$-group which is a quotient of $G$ is a quotient of $G/M$. Thus $\beta_{\mathcal{I}}(G) = G/M$ has properties 1) and 2).

Note that by construction, and by 1.12, if $M$ is a normal subgroup of $G$ such that $G/M \simeq \beta_{\mathcal{I}}(G)$, then $Q_{G,M} \notin \mathcal{I}$.

Now if $N$ is a normal subgroup of $G$, then the group $\beta_{\mathcal{I}}(G/N)$ is an $\mathcal{I}$-group, which is quotient of $G/N$, hence of $G$. Thus $\beta_{\mathcal{I}}(G/N)$ is always a quotient of $\beta_{\mathcal{I}}(G)$.

If a) holds, then $\beta_{\mathcal{I}}(G)$ is an $\mathcal{I}$-group, which is a quotient of $G/N$. Hence $\beta_{\mathcal{I}}(G)$ is a quotient of $\beta_{\mathcal{I}}(G/N)$, and b) holds.

If b) holds, and if $M/N$ is a normal subgroup of $G/N$ such that

$$(G/N)/(M/N) \simeq \beta_{\mathcal{I}}(G/N)$$

then $G/M \simeq \beta_{\mathcal{I}}(G/N) \simeq \beta_{\mathcal{I}}(G)$. Hence as noted above $Q_{G,M} \notin \mathcal{I}$, and since $Q_{G,M}$ is a multiple of $Q_{G,N}$, it follows that $Q_{G,N} \notin \mathcal{I}$. Hence c) holds.

If c) holds, then by proposition 4.3 the group $\beta_{\mathcal{I}}(G)$ is a quotient of $G/N$, and a) holds. □

There are generally several normal subgroups $M$ of $G$ such that $G/M \simeq \beta_{\mathcal{I}}(G)$. They are related as follows:

**(4.5) Proposition:** *Let $G$ be a finite group, and $\mathcal{I}$ be a prime ideal of $\mathcal{R}$. Let $M$ and $N$ be normal subgroups of $G$ such that*

$$G/M \simeq G/N \simeq \beta_{\mathcal{I}}(G)$$

*Let $]M \cap N, M[^G$ denote the poset of normal subgroups of $G$ which contain strictly $M \cap N$ and are strictly contained in $M$, and let $n_G(M,N)$ denote its reduced Euler-Poincaré characteristic (with the convention $n_G(M,N) = 1$ if $M = N$). Then:*

1. *There exists an automorphism $\theta$ of the group $G/M \cap N$ such that*

$$\theta(M/M \cap N) = N/M \cap N$$

*Hence the posets $]M \cap N, M[^G$ and $]M \cap N, N[^G$ are isomorphic, and in particular $n_G(M, N) = n_G(N, M)$.*

2. *The group $M/M \cap N \simeq N/M \cap N$ is isomorphic to a direct product of simple groups.*

3. $Q_{G,N} \equiv Q_{G,M\cap N} n_G(M, N)|K_{G/M\cap N}(M/M \cap N, N/M \cap N)|$ *(mod. $\mathcal{I}$).*

**Proof:** Since $Q_{G,N} = Q_{G,M\cap N} Q_{G/M\cap N, N/M\cap N}$ by Corollary 3.2, replacing $G$ by $G/M \cap N$ shows that it suffices to consider the case $M \cap N = 1$. In this case the groups $M$ and $N$ centralize each other.

By proposition 4.3, since moreover $G/M \simeq G/N$ implies $L \cap M = L \cap N$ whenever $LM = LN = G$ and $L \cap N \leq L \cap M$

$$Q_{G,N} \equiv \sum_{\substack{L \leq G \\ LM=LN=G \\ L\cap M = L\cap N = 1}} \mu(L, G) \pmod{\mathcal{I}}$$

In other words

$$Q_{G,N} \equiv \sum_{L \in K_G(M,N)} \mu(L, G) \pmod{\mathcal{I}}$$

Since $Q_{G,N} \notin \mathcal{I}$, this shows in particular that $K_G(M, N) \neq \emptyset$.

Now fix $L \in K_G(M, N)$, and define a map $\phi$ from $M$ to $N$ by $\phi(m) = n$ if $mn \in L$. This is well defined since $L \in K_G(M, N)$. Moreover if $m$ and $m'$ are in $M$, and if $n = \phi(m)$ and $n' = \phi(m')$, then

$$mnm'n' = mm'nn' \in L$$

since $M$ and $N$ commute. This shows that $\phi(mm') = nn'$, hence $\phi$ is a group homomorphism from $M$ to $N$. By symmetry, the map $\psi$ from $N$ to $M$ defined by $\psi(n) = m$ if $nm \in L$ is also a group homomorphism, which is clearly the inverse of $\phi$, since $M$ and $N$ commute. Moreover the maps $\phi$ and $\psi$ are clearly $L$ equivariant.

Now define a map $\theta : G \to G$ by

$$\theta(ml) = \phi(m)l \qquad \forall m \in M,\ \forall l \in L$$

Then for $m$, $m'$ in $M$ and $l$, $l'$ in $L$

$$\theta(mlm'l') = \theta(m.{}^l m'.ll') = \phi(m).{}^l\phi(m').ll' = \phi(m)l\phi(m')l' = \theta(ml)\theta(m'l')$$

This shows that $\theta$ is a group homomorphism, which is clearly an automorphism of $G$.

By construction $\theta(M) = N$, thus $\theta$ induces an isomorphism of posets from $]1, M[^G$ to $]1, N[^G$, and $n_G(M, N) = n_G(N, M)$. This shows assertion 1).

Now the maps

$$X \in [1, N]^L \mapsto LX \in [L, G] \qquad Y \in [L, G] \mapsto Y \cap N \in [1, N]^L$$

are inverse isomorphisms of posets. Moreover $[1, N]^L = [1, N]^{LM} = [1, N]^G$ since $M$ and $N$ commute. Thus $\mu(L, G)$ is equal to the reduced Euler-Poincaré characteristic of the poset $]1,N[^G = [1,N]^G - \{1,N\}$, and this does not depend on the choice of $L$ in $K_G(M,N)$. Thus

$$Q_{G,N} \equiv \tilde{\chi}(]1,N[^G)|K_G(M,N)| \pmod{\mathcal{I}}$$

and this proves assertion 3).

Since $Q_{G,N} \notin \mathcal{I}$, it follows from Crapo complementation formula that every normal subgroup of $G$ contained in $N$ has a complement in $N$, invariant by $G$. This can only happen if $N$ is a direct product of simple groups, and this completes the proof of the proposition. □

(**4.6**) **Example:** The case of $b$-groups discussed in [2] corresponds to the ideal $\mathcal{I}$ generated by all $X_S - |S|$, for $S \in \mathcal{S}$. In this case if $G$ is a $p$-group, then $\beta_{\mathcal{I}}(G)$ is trivial if $G$ is cyclic, and isomorphic to $(C_p)^2$ otherwise. This follows from Proposition 14 of [2], but I will give another more general proof here in Corollary 7.4.

If $\Phi(G)$ is the Frattini subgroup of $G$, and if the order of $G/\Phi(G)$ is at least $p^3$, then there are several normal subgroups $N$ of $G$ such that $G/N \simeq (C_p)^2$, but all those subgroups contain $\Phi(G)$, and are conjugate by the automorphism group of $G/\Phi(G)$.

## 5. Example: the ideal of valuation

(**5.1**) **Notation:** *I denote by $\mathcal{V}$ the ideal of $\mathcal{R}$ generated by all $X_S$, for $S \in \mathcal{S}$.*

In other words, the ideal $\mathcal{V}$ is the ideal of polynomial with constant term equal to zero. Clearly the quotient ring $\mathcal{R}/\mathcal{V}$ is isomorphic to $\mathbb{Z}$, thus $\mathcal{V}$ is a prime ideal.

By definition, if $N$ is a normal subgroup of the finite group $G$, then

$$Q_{G,N} = \sum_{\substack{L \leq G \\ LN=G}} \mu(L,G)P(L \cap N)$$

In this sum, the monomial $P(L \cap N)$ is in $\mathcal{V}$, unless $L \cap N = 1$. It follows that

$$Q_{G,N} \equiv \sum_{L \in K_G(N)} \mu(L,G) \pmod{\mathcal{V}}$$

If $N$ is a minimal normal subgroup of $G$, and if $N$ is abelian, then by Proposition 2.3

$$Q_{G,N} \equiv -|K_G(N)| \pmod{\mathcal{V}}$$

In particular $Q_{G,N} \in \mathcal{V}$ if and only if $K_G(N) = \emptyset$. This is equivalent to requiring $N$ to be contained in each maximal subgroup $L$ of $G$, i.e. $N$ to be contained in $\Phi(G)$.

(**5.2**) **Notation:** *If $G$ is a finite group, I denote by $M(G)$ the subgroup generated by all minimal normal subgroups of $G$.*

(**5.3**) **Proposition:** *Let $G$ be a solvable finite group. Then $G$ is a $\mathcal{V}$-group if and only if $M(G) \leq \Phi(G)$.*

**Proof:** This follows clearly from the previous discussion. □

(**5.4**) **Remark:** If $G$ is an arbitrary finite group, and if $M(G) \leq \Phi(G)$, then $G$ is a $\mathcal{V}$-group, but the converse is false in general: for example, a simple group $S$ is a $\mathcal{V}$-group if and only if $\mu(1, S) = 0$. This happens for instance if $S$ is the simple group of order 168. Still $M(S) = S$ is not contained in $\Phi(S) = 1$.

This remark and Proposition 4.4 suggest the following variation:

(**5.5**) **Notation:** *I denote by $\mathcal{A}$ the ideal of $\mathcal{R}$ generated by all $X_p$, for $p$ prime.*

Clearly $\mathcal{R}/\mathcal{A}$ is isomorphic to the ring $\mathbb{Z}[(X_S)_{S\in\mathcal{S}^0}]$ of polynomials on the set $\mathcal{S}^0$ of isomorphism classes of *non−abelian* simple groups. Hence $\mathcal{A}$ is a prime ideal of $\mathcal{R}$.

(**5.6**) **Proposition:** *Let $G$ be a finite group. Then $G$ is an $\mathcal{A}$-group if and only if $M(G) \leq \Phi(G)$.*

**Proof:** If $M(G) \leq \Phi(G)$, since $\Phi(G)$ is nilpotent, all minimal normal subgroups of $G$ are abelian, and have no complement in $G$. If $N$ is a minimal normal subgroup of $G$, isomorphic to $(C_p)^n$, for a prime number $p$ and a positive integer $n$, then by Proposition 2.3

$$Q_{G,N} = X_p^n - |K_G(N)| = X_p^n \in \mathcal{A}$$

Hence $G$ is an $\mathcal{A}$-group.

Conversely, if $G$ is an $\mathcal{A}$-group and $N$ is a minimal normal abelian subgroup of $G$, isomorphic to $(C_p)^n$, then

$$Q_{G,N} = X_p^n - |K_G(N)| \equiv -|K_G(N)| \pmod{\mathcal{A}}$$

Thus $Q_{G,N} \in \mathcal{A}$ if and only if $K_G(N) = \emptyset$, or equivalently since $N$ is abelian, if $N \leq \Phi(G)$.

Now suppose $N$ is a non-abelian minimal normal subgroup of $G$. Then $N \simeq S^n$, for some non-abelian simple group $S$ and some positive integer $n$. But

$$Q_{G,N} = \sum_{\substack{H\leq G\\ HN=G}} \mu(H,G)P(H\cap N)$$

and the term of highest degree in this expression is obtained for $H = G$, and it is equal to $P(N) = X_S^n$. But the ideal $\mathcal{A}$ consists of linear combinations of monomials $\prod_{S\in\mathcal{S}} X_S^{\alpha_S}$ for which the exponent $\alpha_S$ is positive at least for one abelian simple group $S$ (i.e. the monomials in which some variable $X_p$ for $p$ prime appears). This shows that $Q_{G,N}$ cannot belong to $\mathcal{A}$ if $N$ is non-abelian.

Hence all the minimal normal subgroups of $G$ are abelian, and it follows that $M(G) \leq \Phi(G)$, as was to be shown. □

(**5.7**) **Corollary:** *Let $G$ be a finite group. Then there exists a factor group $H$ of $G$, characterized uniquely up to isomorphism by the following properties:*

1. $M(H) \leq \Phi(H)$.

2. *If $K = G/N$ is a quotient of $G$ such that $M(K) \leq \Phi(K)$, and if $M \trianglelefteq G$ is such that $G/M \simeq H$, then there exists a subgroup $L$ of $G$ with*

$$LM = LN = G \qquad L \cap M \leq L \cap N$$

*and in particular $K$ is a quotient of $H$.*

**Proof:** Of course $H = \beta_{\mathcal{A}}(G)$. ☐

(**5.8**) **Example:** When $G$ is a $p$-group, for some prime $p$, it is possible to describe explicitly the quotient $\beta_{\mathcal{V}}(G) = \beta_{\mathcal{A}}(G)$. Indeed, this quotient is obtained by considering a normal subgroup $N$ of $G$, maximal subject to $Q_{G,N} \notin \mathcal{V}$. With the notation of Proposition 2.4, if

$$1 = N_{-1} < N_0 < \ldots < N_k = G$$

is a chief series for $G$, and if $N = N_l$, for $-1 \leq l \leq k$, then

$$Q_{G,N} = \tilde{P}(G)/\tilde{P}(G/N) = \prod_{i=0}^{l}(X_p^{n_i} - m_i) \equiv (-1)^{l+1}\prod_{i=0}^{l} m_i \pmod{\mathcal{V}}$$

Thus $N$ is a maximal normal subgroup such that all the $m_i$'s are non-zero. In particular, every minimal normal subgroup of $G$ contained in $N$ must have a complement in $G$, hence in $N$. It follows that $N$ is elementary abelian, and $G$-semi-simple. Hence $N$ is central.

Moreover if $L_i/N_{i-1} \in K_{G/N_{i-1}}(N_i/N_{i-1})$, for $0 \leq i \leq l$, then it is easy to see that $L_0 \cap L_1 \cap \ldots \cap L_l$ is a complement of $N_l = N$ in $G$. Thus $G$ can be split as a direct product

$$G = N \times L$$

Moreover $L$ is a $\mathcal{V}$-group, thus $M(L) \leq \Phi(L)$. Since $L$ is a $p$-group, all the minimal normal subgroups of $L$ are central of order $p$. It follows that no central subgroup of order $p$ can have a complement in $L$. Hence $N$ is a maximal elementary abelian central subgroup of $G$ having a complement in $G$, and $\beta_{\mathcal{V}}(G)$ is the quotient of $G$ by its "largest elementary abelian direct summand".

In this case, one can say exactly how many subgroups $N$ such that $G/N \simeq \beta_{\mathcal{V}}(G)$ there are: indeed with the previous notations, the group $M(L)$ is equal to the subgroup $\Omega_1\big(Z(L)\big)$ generated by the central elements of order $p$ of $L$. But

$$\Phi(G) = 1 \times \Phi(L)$$

and

$$\Omega_1\big(Z(G)\big) = N \times \Omega_1\big(Z(L)\big) \tag{5.9}$$

Taking the intersection of those two equations gives

$$\Phi(G) \cap \Omega_1\big(Z(G)\big) = 1 \times \Omega_1\big(Z(L)\big)$$

It follows from 5.9 that $N$ must be a complement of $\Phi(G) \cap \Omega_1\big(Z(G)\big)$ in $\Omega_1\big(Z(G)\big)$.

Conversely, if $N$ is such a complement, there exists a subgroup $K$ of $G$, containing $\Phi(G)$, such that $K/\Phi(G)$ is a complement of $N\Phi(G)/\Phi(G)$ in $G/\Phi(G)$, since $G/\Phi(G)$ is elementary abelian. In other words

$$KN = G \qquad K \cap N\Phi(G) = \Phi(G)$$

It follows that $K \cap N \leq N \cap \Phi(G) = 1$, thus $K$ is a complement of $N$. Clearly now $N$ is $G$-semi-simple, and it follows that $Q_{G,N} \notin \mathcal{V}$.

Thus the subgroups $N$ such that $G/N \simeq \beta_{\mathcal{I}}(G)$ are exactly the complements of $\Phi(G) \cap \Omega_1\big(Z(G)\big)$ in $\Omega_1\big(Z(G)\big)$.

## 6. Direct products

(**6.1**) **Notation:** *Let $G$ and $H$ be finite groups. Denote by $p_1$ and $p_2$ the projections from $G \times H$ to $G$ and $H$ respectively. If $L$ is a subgroup of $G \times H$, set*

$$p_1(L) = \{g \in G \mid \exists h \in H,\ (g,h) \in L\} \qquad k_1(L) = \{g \in G \mid (g,1) \in L\}$$

$$p_2(L) = \{h \in H \mid \exists g \in G,\ (g,h) \in L\} \qquad k_2(L) = \{h \in H \mid (1,h) \in L\}$$

*Then $k_i(L) \trianglelefteq p_i(L)$ for $i = 1,2$, and the quotients $q(L) = L/\big(k_1(L) \times k_2(L)\big)$, $p_1(L)/k_1(L)$ and $p_2(L)/k_2(L)$ are canonically isomorphic.*

(**6.2**) **Proposition:** *Let $G$ and $H$ be finite groups. Then*

$$\tilde{P}(G)\tilde{P}(H) = \sum_{\substack{L \leq G \times H \\ p_1(L)=G \\ p_2(L)=H}} \tilde{P}(L)$$

**Proof:** This is a consequence of the definition of the polynomials $\tilde{P}$ by Möbius inversion. Indeed for any finite groups $G$ and $H$

$$P(G \times H) = \sum_{L \leq G \times H} \tilde{P}(L) \tag{6.3}$$

Now setting

$$\sigma(G,H) = \sum_{\substack{L \leq G \times H \\ p_1(L)=G \\ p_2(L)=H}} \tilde{P}(L)$$

the right hand side of equation 6.3 can be written as

$$\sum_{\substack{A \leq G \\ B \leq H}} \sigma(A,B)$$

Thus

$$\begin{aligned}\sum_{\substack{C\le G\\ D\le H}} \mu(C,G)\mu(D,H)P(C\times D) &= \sum_{\substack{C\le G\\ D\le H}}\sum_{\substack{A\le C\\ B\le D}} \mu(C,G)\mu(D,H)\sigma(A,B)\\ &= \sum_{\substack{A\le G\\ B\le H}}\Big(\sum_{\substack{A\le C\le G\\ B\le D\le H}} \mu(C,G)\mu(D,H)\Big)\sigma(A,B)\\ &= \sigma(G,H)\end{aligned}$$

The proposition follows, since the left hand side is equal to $\tilde{P}(G)\tilde{P}(H)$, because $P(C\times D)=P(C)P(D)$ for any $C\le G$ and $D\le H$. □

(**6.4**) **Corollary:** *If $G$ and $H$ have no non-trivial isomorphic factor group, then*

$$\tilde{P}(G\times H)=\tilde{P}(G)\tilde{P}(H)$$

**Proof:** Indeed in this case, the only subgroup $L$ of $G\times H$ such that $p_1(L)=G$ and $p_2(L)=H$ is $G\times H$ itself, since $q(L)$ is a quotient of both $G$ and $H$, hence it is trivial. □

(**6.5**) **Proposition:** [[2] Lemme 22] *Let $G$ and $H$ be finite groups. Then*

$$\tilde{P}(G\times H)=\tilde{P}(G)\tilde{P}(H)\sum_{\substack{L\le G\times H\\ p_1(L)=G\\ p_2(L)=H}} \frac{\tilde{\chi}(]1,q(L)[^{q(L)})}{\tilde{P}\big(q(L)\big)} \tag{6.6}$$

**Proof:** Denote by $K$ the group $G\times H$, and by $M$ and $N$ the normal subgroups $G\times 1$ and $1\times H$ of $K$. Then by proposition 3.1 since $M\cap N=1$

$$Q_{K,N}=\sum_{\substack{L\le K\\ LM=LN=K}} \mu(L,K)Q_{K/M,(L\cap N)M/M}$$

The condition $LM=LN=K$ is equivalent to $p_1(L)=G$ and $p_2(L)=H$. In this case moreover, the maps

$$X\in]L,K[\mapsto k_1(X)/k_1(L)\in]1,G/k_1(L)[^G$$

$$Y/k_1(L)\in]1,G/k_1(L)[^G\mapsto\{(g,h)\in G\times H\mid \exists a\in G,\ (a,h)\in L,\ ga^{-1}\in Y\}$$

are mutual inverse isomorphisms of posets. Since $G/k_1(L)\simeq q(L)$, it follows that $\mu(L,G)=\tilde{\chi}(]1,q(L)[^{q(L)})$.

Moreover

$$Q_{K/M,(L\cap N)M/M}=Q_{L/L\cap M,(L\cap N)(L\cap M)/L\cap M}=\frac{\tilde{P}(L/L\cap M)}{\tilde{P}\big(L/(L\cap N)(L\cap M)\big)}$$

But $L/L\cap M\simeq K/M\simeq H$ and

$$L/(L\cap N)(L\cap M)=L/k_1(L)\times k_2(L)=q(L)$$

It follows that

$$Q_{K,N} = \tilde{P}(H) \sum_{\substack{L \leq G\times H \\ p_1(L)=G \\ p_2(L)=H}} \frac{\tilde{\chi}(]1, q(L)[^{q(L)})}{\tilde{P}\big(q(L)\big)}$$

The proposition follows, since $Q_{K,N} = \tilde{P}(K)/\tilde{P}(K/N) = \tilde{P}(K)/\tilde{P}(G)$. □

(**6.7**) **Corollary:** *Let $G$ and $H$ be finite groups, and denote by $G_s$, $H_s$ and $(G \times H)_s \simeq G_s \times H_s$ the respective largest semi-simple quotients of $G$, $H$ and $G \times H$. Then*

$$\frac{\tilde{P}(G \times H)}{\tilde{P}\big((G \times H)_s\big)} = \frac{\tilde{P}(G)}{\tilde{P}(G_s)} \frac{\tilde{P}(H)}{\tilde{P}(H_s)}$$

**Proof:** The only non-zero terms in the formula 6.6 correspond to subgroups $L$ of $G \times H$ such that $q(L)$ is semi-simple. Moreover since $p_1(L) = G$ and $p_2(L) = H$, the group $q(L)$ is a quotient of $G$ and $H$. It follows that if $M$ and $N$ are normal subgroups of $G$ and $H$ respectively, such that $G/M \simeq G_s$ and $H/N \simeq H_s$, then $L \geq M \times N$. Then the group $L' = L/M \times N$ is a subgroup of $G_s \times H_s \simeq (G \times H)_s$, and

$$\begin{aligned} q(L) &= L/k_1(L) \times k_2(L) \simeq (L/M \times N)/\big(k_1(L) \times k_2(L)/M \times N\big) \\ &\simeq L'/\big(k_1(L)/M\big) \times \big(k_2(L)/N\big) = q(L') \end{aligned}$$

The corollary follows, since the correspondence $L \mapsto L'$ from

$$\{K \leq G \times H \mid \ p_1(K) = G,\ p_2(K) = H,\ K \geq M \times N\}$$

to the set

$$\{K' \leq G_s \times H_s \mid p_1(K') = G_s,\ p_2(K') = H_s\}$$

is clearly one to one. □

Corollary 6.7 gives a way to compute $\tilde{P}(G \times H)$ knowing $\tilde{P}(G)$, $\tilde{P}(H)$, and the groups $G_s$ and $H_s$. The following notation will be convenient:

(**6.8**) **Notation:** *If $G$ and $H$ are finite groups, I denote by $s(G,H)$ the number of surjective group homomorphisms from $G$ to $H$.*

*If $n, m \in \mathbb{N}$, I set*

$$F(G,n) = \prod_{i=0}^{n-1} \big(\tilde{P}(G) - s(G^i, G)\big)$$

$$B(G,m,n) = \frac{F(G,m+n)}{F(G,m)F(G,n)}$$

Here the letter $F$ stands for "factorial", and the letter $B$ for "binomial". Note that $B(G,m,n)$ is an element of the field of fractions of $\mathcal{R}$.

(**6.9**) **Proposition:**

1. *If $S$ is a finite simple group and $n \in \mathbb{N}$, then $\tilde{P}(S^n) = F(S,n)$. Moreover $s(S^n, S)$ is equal to $p^n - 1$ if $S \simeq C_p$, and to $n|Aut(S)|$ if $S$ is non-abelian.*

2. *Let $G$ and $H$ be finite groups. If $S \in \mathcal{S}$, denote by $a_S = \nu_S(G_s)$ and $b_S = \nu_S(H_s)$ the multiplicity of $S$ as a factor of $G_s$ and $H_s$ respectively. Then*
$$\tilde{P}(G \times H) = \tilde{P}(G)\tilde{P}(H) \prod_{S \in \mathcal{S}} B(S, a_S, b_S)$$

**Proof:** The first formula follows from an easy induction argument, using 6.2 or 6.6. Using this, the second formula follows from 6.4 and 6.7. □

(**6.10**) **Lemma:** *Let $\mathcal{I}$ be a prime ideal of $\mathcal{R}$. If $G$ and $H$ are $\mathcal{I}$-groups, and if they have no non-trivial isomorphic factor group, then $G \times H$ is an $\mathcal{I}$-group.*

**Proof:** Since $G$ and $H$ are quotients of $G \times H$, it follows that they are quotients of $\beta_{\mathcal{I}}(G \times H)$. Hence there is a group homomorphism

$$\phi : \beta_{\mathcal{I}}(G \times H) \to G \times H$$

such that $p_1 \circ \phi$ and $p_2 \circ \phi$ are surjective. Let $K$ denote the image of $\phi$. Then $p_1(K) = G$ and $p_2(K) = H$. Thus $q(K)$ is a quotient of both $G$ and $H$, hence it is trivial. It follows that $K = G \times H$, hence $\beta_{\mathcal{I}}(G \times H) \simeq G \times H$. Thus $G \times H$ is an $\mathcal{I}$-group. □

(**6.11**) **Proposition:** *Let $\mathcal{I}$ be a prime ideal of $\mathcal{R}$, and $G$ and $H$ be finite groups having no non-trivial isomorphic factor group.*

1. *If $M \trianglelefteq G$ and $N \trianglelefteq H$, then*
$$Q_{G \times H, M \times N} = Q_{G,M} Q_{H,N}$$

2. *Moreover*
$$\beta_{\mathcal{I}}(G \times H) \simeq \beta_{\mathcal{I}}(G) \times \beta_{\mathcal{I}}(H)$$

3. *The group $G \times H$ is an $\mathcal{I}$-group if and only if $G$ and $H$ are $\mathcal{I}$-groups.*

**Proof:** Let $M$ be a normal subgroup of $G$ and $N$ be a normal subgroup of $H$. Then by Corollary 6.4, since $G/M$ and $H/N$ have no non-trivial isomorphic factor group

$$\begin{aligned} \tilde{P}(G \times H) &= \tilde{P}(G)\tilde{P}(H) \\ \tilde{P}(G \times H / M \times N) &= \tilde{P}(G/M \times H/N) \\ &= \tilde{P}(G/M)\tilde{P}(H/N) \end{aligned}$$

Taking the quotient of those equations gives assertion 1)

$$Q_{G \times H, M \times N} = Q_{G,M} Q_{H,N}$$

Clearly $\beta_{\mathcal{I}}(G)$ and $\beta_{\mathcal{I}}(H)$ have no common non-trivial factor group. Hence by Lemma 6.10 $\beta_{\mathcal{I}}(G) \times \beta_{\mathcal{I}}(H)$ is an $\mathcal{I}$-group, and it is a quotient of $G \times H$. Hence it is a quotient of $\beta_{\mathcal{I}}(G \times H)$.

Conversely if $M \trianglelefteq G$ is such that $G/M \simeq \beta_{\mathcal{I}}(G)$, and $N \trianglelefteq H$ is such that $H/N \simeq \beta_{\mathcal{I}}(H)$, then $Q_{G,M} \notin \mathcal{I}$ and $Q_{H,N} \notin \mathcal{I}$, thus $Q_{G\times H,M\times N} \notin \mathcal{I}$ by assertion 1) since $\mathcal{I}$ is prime. By Proposition 4.3 the group $\beta_{\mathcal{I}}(G \times H)$ is a quotient of

$$(G \times H)/(M \times N) \simeq \beta_{\mathcal{I}}(G) \times \beta_{\mathcal{I}}(H)$$

Assertion 2) follows.

Finally $G\times H$ is an $\mathcal{I}$-group if and only if $G\times H = \beta_{\mathcal{I}}(G\times H)$. By assertion 2), this is equivalent to $G = \beta_{\mathcal{I}}(G)$ and $H = \beta_{\mathcal{I}}(H)$, which proves assertion 3). □

## 7. Nilpotent $\mathcal{I}$-groups

It is possible to describe all the nilpotent $\mathcal{I}$-groups, when $\mathcal{I}$ is a prime ideal of $\mathcal{R}$. Since any nilpotent group is isomorphic to the direct product of its Sylow $p$-subgroups, for prime numbers $p$, it follows from proposition 6.11 that a nilpotent group is an $\mathcal{I}$-group if and only if all its Sylow subgroups are $\mathcal{I}$-groups. Thus in order to describe the nilpotent $\mathcal{I}$-groups, it suffices to describe the $p$-groups which are also $\mathcal{I}$-groups.

(**7.1**) **Proposition:** *Let $\mathcal{I}$ be a prime ideal of $\mathcal{R}$, let $p$ be a prime number, and let $G$ be a finite $p$-group. Then:*

1. *If $G$ is elementary abelian of order $p^n$, then $G$ is an $\mathcal{I}$-group if and only if $n = 0$ or $n \geq 1$ and $X_p - p^{n-1} \in \mathcal{I}$.*
2. *If $G$ is not elementary abelian, then $G$ is an $\mathcal{I}$-group if and only if $X_p \in \mathcal{I}$ and one of the following holds:*
   *(a) $p \in \mathcal{I}$.*
   *(b) $\Omega_1\big(Z(G)\big) \leq \Phi(G)$, or equivalently, the group $G$ cannot be written $G \simeq C_p \times H$, for some finite group $H$.*

**Proof:** Suppose $G$ is non-trivial, and let $N$ be a minimal normal subgroup of $G$. Then $N$ is central of order $p$, and

$$Q_{G,N} = X_p - |K_G(N)|$$

since any proper subgroup $L$ of $G$ such that $LN = G$ is a complement of $G$, and $L$ is a maximal subgroup of $G$ in this case.

Suppose that $G$ is elementary abelian of order $p^n$. If $n = 0$, then $G$ is trivial and $G$ is an $\mathcal{I}$-group. If $n \geq 1$, and if $N$ is a subgroup of $G$ of order $p$, then

$$Q_{G,N} = X_p - p^{n-1}$$

since there are $p^{n-1}$ complements of $N$ in $G$. This proves assertion 1).

If $G$ is not elementary abelian, then there exists a central subgroup $N$ of $G$ of order $p$ contained in $\Phi(G)$. If $N$ is such a subgroup, then $K_G(N) = \emptyset$, and

$$Q_{G,N} = X_p \tag{7.2}$$

Now if $M$ is a central subgroup of $G$ of order $p$, and $M \not\leq \Phi(G)$, then

$$Q_{G,N} = X_p - |K_G(M)| \tag{7.3}$$

Moreover in this case $K_G(M) \neq \emptyset$, thus there exists a group $H$ such that $G \simeq M \times H$, and

$$|K_G(M)| = |\mathrm{Hom}(H, M)|$$

is a power of $p$, and different from 1 since $H$ is non trivial (if $H = 1$, then $G$ has order $p$ and $G$ is elementary abelian).

Hence if $G$ is an $\mathcal{I}$-group, then $X_p \in \mathcal{I}$ by 7.2. Now if $\Omega_1\big(Z(G)\big) \not\leq \Phi(G)$, it follows from 7.3 that $|K_G(M)| \in \mathcal{I}$. This is a power of $p$, different from 1, thus $p \in \mathcal{I}$ since $\mathcal{I}$ is prime.

Conversely, if $X_p \in \mathcal{I}$ and $p \in \mathcal{I}$, then clearly $Q_{G,N} \in \mathcal{I}$ by 7.2 and 7.3 for any central subgroup $N$ of order $p$ of $G$. Then $G$ is an $\mathcal{I}$-group.

And if $X_p \in \mathcal{I}$ and $\Omega_1\big(Z(G)\big) \leq \Phi(G)$, then any central subgroup $N$ of order $p$ of $G$ is contained in $\Phi(G)$, hence $Q_{G,N} \in \mathcal{I}$ by 7.2. Thus $G$ is an $\mathcal{I}$-group, and this completes the proof of the proposition. □

Proposition 7.1 can be reformulated as follows:

(**7.4**) **Corollary:** *Let $\mathcal{I}$ be a prime ideal of $\mathcal{R}$, let $p$ be a prime number, and let $G$ be a finite $p$-group. Then:*

- *If $X_p \in \mathcal{I}$ and $p \in \mathcal{I}$, then $G$ is an $\mathcal{I}$-group if and only if $G \not\simeq C_p$.*
- *If $X_p \in \mathcal{I}$ and $p \notin \mathcal{I}$, then $G$ is an $\mathcal{I}$-group if and only if $\Omega_1\big(Z(G)\big) \leq \Phi(G)$.*
- *If $X_p \notin \mathcal{I}$, then let $h, k \in \mathbb{N} \cup \{\infty\}$ defined by*

$$\begin{aligned} h &= \mathrm{Inf}\,\{l \in \mathbb{N} \mid X_p - p^l \in \mathcal{I}\} \\ k &= \mathrm{Inf}\,\{l \in \mathbb{N} - \{0\} \mid 1 - p^l \in \mathcal{I}\} \end{aligned}$$

  *Then $G$ is an $\mathcal{I}$-group if and only if $G$ is elementary abelian of order $p^n$ with $n = 0$, or $n \equiv h + 1\ (k)$ if $h \neq \infty$ and $k \neq \infty$, or $n = h + 1$ if $h \neq \infty$ and $k = \infty$.*

**Proof:** Indeed, if $X_p \in \mathcal{I}$ and $p \in \mathcal{I}$, then by Proposition 7.1, the only case where $G$ is not an $\mathcal{I}$-group is the case $G \simeq C_p$.

If $X_p \in \mathcal{I}$ and if a non-trivial elementary abelian $p$-group of order $p^n$ is an $\mathcal{I}$-group, then $p^{n-1} \in \mathcal{I}$, hence $1 \in \mathcal{I}$ or $p \in \mathcal{I}$. Thus if $p \notin \mathcal{I}$, then no non-trivial elementary abelian $p$-group can be an $\mathcal{I}$-group, and $G$ is an $\mathcal{I}$-group if and only if $\Omega_1\big(Z(G)\big) \leq \Phi(G)$.

Finally if $X_p \notin \mathcal{I}$, then $G$ is an $\mathcal{I}$-group if and only if $G$ is elementary abelian of order $p^n$ with $n = 0$ or $n \geq 1$ and $X_p - p^{n-1} \in \mathcal{I}$. This cannot happen if $h = \infty$, and if $h \in \mathbb{N}$, this is equivalent to

$$p^h - p^{n-1} = p^h(1 - p^{n-h-1}) \in \mathcal{I}$$

But $p^h \notin \mathcal{I}$, since otherwise $X_p = (X_p - p^h) + p^h \in \mathcal{I}$, and this is equivalent to $1 - p^{n-h-1} \in \mathcal{I}$, or $n \equiv h + 1\ (k)$, which has to be viewed as an equality if $k = \infty$. □

(**7.5**) **Remark:** The last case of Corollary 7.4 should be compared with Theorem 8.2 of [3], which deals with "$b$-groups in characteristic $q$", i.e. with the case where $\mathcal{I}$ is generated by a prime number $q \neq p$ (or $q = 0$), and by $X_S - |S|$, for all simple groups $S$.

## References


[1] S. Bouc. Homologie de certains ensembles ordonnés. *C. R. Acad. Sc. Paris*, t.299(2):9–12, 1984. Série I.

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

[3] S. Bouc and J. Thévenaz. The group of endo-permutation modules. *Invent. Math.*, 1998. To appear.

[4] K. Brown. The coset poset and the probabilistic zeta function of a finite group. Preprint, 1999.

[5] K. Brown and J. Thévenaz. A generalization of Sylow's third theorem. *Journal of Algebra*, 115:414–430, 1988.

[6] H. Crapo. The Möbius function of a lattice. *J. Comb. Theory.*, 1:126–131, 1966.

[7] W. Gaschütz. Die Eulersche Funktion endlicher auflösbarer Gruppen. *Illinois J. Math.*, 3:469–476, 1959.

[8] P. Hall. The Eulerian functions of a group. *Quart. J. Math.*, 7:134–151, 1936.