AUGMENTATION-FILTRATION AND NORMAL DISTRIBUTION

BY

MICHAEL WEIDNER
Department of Mathematics, Albert-Ludwigs-University of Freiburg
Alberstr. 23b, 79104 Freiburg, Germany
e-mail: weidner@sun2.mathematik.uni-freiburg.de

Dedicated to Albrecht Brandis

ABSTRACT

The shape of the augmentation series is an old question in modular group representation theory. Using an asymptotic point of view probability theory provides useful patterns to describe these shapes. Especially for large p-groups the normal distribution is a good approach.

1. Introduction

Throughout this paper p is a fixed prime, G a group, K a field of characteristic p and KG the group algebra. $\mathbf{I}(G) := \{\sum_{g\in G} k_g g : \sum k_g = 0, k_g \in K\}$ is the augmentation ideal. The powers of the augmentation ideal yield a filtration of the group algebra:

$$KG = \mathbf{I}(G)^0 > \mathbf{I}(G) \geq \mathbf{I}(G)^2 \geq \cdots.$$

We are interested in the function $i \to \dim \mathbf{I}(G)^i/\mathbf{I}(G)^{i+1}$.

If one can compute various subgroups of G an explicit formula for these dimensions is available (see Jennings' Theorem 2.1). This will give for every group a function that describes exactly $\dim \mathbf{I}(G)^i/\mathbf{I}(G)^{i+1}$. To be more detailed:

Suppose G is finite. Then there is an l such that $\mathbf{I}(G)^l = \mathbf{I}(G)^{l+1}$. Set $L := \dim KG/\mathbf{I}(G)^l$ and consider $\mathcal{I}_d(G) : i \to \frac{1}{L} \dim \mathbf{I}(G)^i/\mathbf{I}(G)^{i+1}$ as the

Received March 10, 1996 and in revised form September 25, 1996

density of a random variable and define the expectation value $E(\mathcal{I}_d(G)) := \sum_i \mathcal{I}_d(G)i$, the variance $V(\mathcal{I}_d) := E((\mathcal{I}_d - E(\mathcal{I}_d))^2)$ and the normalization $\overline{\mathcal{I}_d} := (\mathcal{I}_d - E(\mathcal{I}_d))/\sqrt{V(\mathcal{I}_d)}$ (so $E(\overline{\mathcal{I}_d}) = 0$ and $V(\overline{\mathcal{I}_d}) = 1$).

Let $\overline{\mathcal{I}_D}(x) := \sum_{i\leq x} \overline{\mathcal{I}_d}(i)$ denote the distribution corresponding to $\overline{\mathcal{I}_d}$. The (normalized) normal distribution is

$$\mathcal{N}_D(x) := \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-t^2/2} dt.$$

THEOREM 1.1: *Let F be a finitely generated, non-abelian free group and $p = \operatorname{char} K$ a prime.*

Then there is a natural series $(N_n)_{n\in\mathbb{N}}$ of normal subgroups of F, such that F/N_n is a finite p-group, $\bigcap_n N_n = \{1\}$ and

$$\lim_{n\to\infty} \overline{\mathcal{I}_D(F/N_n)} = \mathcal{N}_D.$$

In addition, we show that for many (in the sense of the Higman–Sims theorem) finite p-groups $\overline{\mathcal{I}_D}$ is close to the normal distribution.

2. Preliminaries

Throughout this paper p is a fixed prime and G a group.

2.1 FINITE p-GROUPS. Proofs of the facts mentioned in this section can be found in Benson's book [1] (section 3.14, pages 85–89).

Let $\gamma_i(G)$ denote the i-th term of the descending central series of G, i.e. $\gamma_1(G) := G$ and $\gamma_i(G) := [G, \gamma_{i-1}(G)]$.

The i-th p-dimension subgroup of G is

$$D_i(G) := \langle \gamma_j(G)^{p^k} : p^k j \geq i \rangle \ .$$

There are many names (Jennings, Zassenhaus, Brauer or Lazard subgroups) and descriptions for these groups. For example $D_i(G) = \{g \in G : g - 1 \in \mathbf{I}(G)^i\}$.

For the rest of this section assume G is finite.

Define $r_i := \log_p(|D_i(G)/D_{i+1}(G)|)$.

Note that $D_i(G)/D_{i+1}(G)$ is an elementary abelian p-group. Hence it is isomorphic to (the additive group of) an r_i dimensional vector space. Choose a set B_i of representatives in $D_i(G)$ of a basis of this space. Fix a linear ordering $\leq$ on $\bigcup B_i$.

THEOREM 2.1 (Jennings [3]): *Let G, r_i and B_i be as above. For all $n \in \mathbf{N}$:*

$$\{(b_1 - 1)\cdots(b_m - 1) \bmod \mathbf{I}^{n+1}\colon b_k \in B_{j(k)}, b_{i+p} \neq b_i \leq b_{i+1}, \sum kj(k) = n\}$$

is a basis of $\mathbf{I}^n/\mathbf{I}^{n+1}$.

The following polynomial equation in t holds:

$$\sum_{i\geq 0} t^i \dim \mathbf{I}^i(G)/\mathbf{I}^{i+1}(G) = \prod_{l:r_l\neq 0} \left(\frac{1-t^{pl}}{1-t^l}\right)^{r_l}.$$

The second part of this theorem implies

$$\begin{aligned} &|\{(b_1 - 1)\cdots(b_m - 1) \bmod \mathbf{I}^{n+1} &&: b_i \in B_{j(i)}, \textstyle\sum j(i)i = n, b_{i+p} \neq b_i \leq b_{i+1}\}| \\ &= |\{(b_1, \ldots, b_m) &&: b_i \in B_{j(i)}, \textstyle\sum j(i)i = n, b_{i+p} \neq b_i \leq b_{i+1}\}| \end{aligned}$$

so no element of the first set is listed twice.

For p-groups the augmentation ideal is the radical. For finite groups G the intersection over all $D_i(G)$ is $O^p(G)$, i.e. the intersection over all normal subgroups of p-power index and $KG\mathbf{I}(O^p(G)) = \bigcap_i \mathbf{I}(G)^i$. This implies $KG/\bigcap_i \mathbf{I}(G)^i \cong K(G/O^p(G))$.

Thus the co-dimension of $\mathbf{I}(G)^i$ in KG depends only on the largest p-factor group of G (provided G is finite).

2.2 Free groups.

Both theorems in this section are proved using Lie rings. The first uses $\mathbb{Z}$ Lie rings and the second is the analog for $\mathbb{Z}/p\mathbb{Z}$-Lie rings. A Lie-ring proof of the theorem in the last section was given in [8].

THEOREM 2.2 (Magnus [6], Witt [15]): *Let F_n denote the free group with n generators. Then $\bigcap_i \gamma_i(F_n) = \{1\}$ and*

$$\Gamma_i(n) := \operatorname{rank}_{\mathbb{Z}} \gamma_i(F_n)/\gamma_{i+1}(F_n) = \frac{1}{i}\sum_{d|i} \mathcal{M}(d) n^{i/d}$$

(here $\mathcal{M}$ denotes the Möbius function and the summation is over all divisors d of i).

For a proof see [5] pages 299 and 468.

In [4] the following is shown:

THEOREM 2.3 (Lazard [4]): *Fix a prime p. Then: $\bigcap_i D_i(F_n) = \{1\}$ and $\dim D_i(F_n)/D_{i+1}(F_n) = \sum \Gamma_{i/p^j}(n)$, where the summation is over all $j \geq 0$ such that p^j is a divisor of i.*

Putting the above formulas together, we get an explicit (but hard to compute) formula for $\overline{\mathcal{I}_D(F_n/D_i)}$.

A rough bound is:

COROLLARY 2.4: $|\dim D_i(F_n)/D_{i+1}(F_n) - n^i/i| \le in^{i/2}$.

2.3 PROBABILITY. As usual, $E(X)$ denotes the expectation value of the random variable X and $V(X)$ the variance. If $V(X) \neq 0$, we define the normalization of X by $\overline{X} := (X - E(X))/\sqrt{V(X)}$. This is a random variable with expectation value 0 and variance 1.

The distribution $D(X)$ of a random variable X is the function from $\mathbf{R}$ to the interval $[0,1]$ defined by: $D(X)(x) := \mu(X^{-1}((-\infty, x))$ where μ is the measure on the probability space on which X lives.

Suppose X_i are random variables on a probability space P and P can be written as $\times P_i$. If $X_i((x_1, x_2, \ldots))$ depends only on x_i (for every i) the X_i's are independent random variables. For our purposes it is enough to have this criteria for independence.

In Shiryayev [13] page 326 a central limit theorem is proved. It states that normalized partial sums of a series of random variables converge to the normal distribution if the variance of the variables does not grow too fast and the dependency between the variables shrinks fast enough.

A special case is:

THEOREM 2.5: *Let p denote a prime and suppose $(Y_i)_{i \in \mathrm{N}}$ are independent random variables uniformly distributed on $\{0, 1, \ldots, p-1\}$.*

Assume $y_i \in \mathbf{R} \setminus \{0\}$ and $\lim_{i \to \infty} y_i/\sqrt{i} = 0$. Define $X_i := y_i Y_i$. Then the limit (for $n \to \infty$) of the distributions of $\overline{\sum_{i \le n} X_i}$ is the normalized normal distribution.

Note that: $E := E(Y_i) = (p-1)/2$, $V := V(Y_i) = (p^2-1)/12$, $E(\sum_{i \le n} X_i) = \sum_{i \le n} y_i E$ and $V(\sum_{i \le n} X_i) = \sum_{i \le n} {y_i}^2 V$.

3. Proof of Theorem 1.1

As mentioned in the introduction $\mathcal{I}_D$ is the distribution of a random variable. We construct such a random variable.

Fix a finite group G and a basis B_i of $\mathbf{I}(G)^i/\mathbf{I}(G)^{i+1}$. Define $B := \bigcup_i B_i$. We regard B as a measure space, where the measure is defined by $\mu(A) := |A|/|B|$.

Define $\mathcal{I}_R(G)$: $B \to \mathbf{R}$ by $\mathcal{I}_R(G)(b) := i$ if $b \in B_i$. This is a random variable. Obviously the distribution of $\mathcal{I}_R(G)$ is $\mathcal{I}_D(G)$.

The remark following Jennings theorem 2.1 shows that $\mathcal{I}_R(G)$ is an independent sum of $\sum r_l = \log_p(|G/O^p(G)|)$ random variables.

Suppose $F = F_n$ is a free group with $n > 1$ generators.

We claim that $D_i(F) =: N_i$ satisfies the conclusion of Theorem 1.1.

1. F/D_i is a finite p-group (the order can be computed by Theorem 2.3).
2. $\bigcap_{i \in \mathbb{N}} D_i = 1$ is the first part of Theorem 2.3.
3. We want to apply Theorem 2.5.

   For each i there is exactly one l such that $\sum_{j<l} r_j < i \leq \sum_{j\leq l} r_j$ (there $r_i := \dim D_i(F)/D_{i+1}(F)$). Define $y_i := l$ and Y_i as in Theorem 2.5. By Theorem 2.1 we have: $\mathcal{I}_R(F/D_i) = \sum_{k \leq \sum_{j<i} r_j} y_k Y_k$.

   By Corollary 2.4 we have $r_k = n^k/k + x_k$ for some x_k with $|x_k| \leq kn^{k/2}$. Thus
   $$0 \leq \lim_{i\to\infty} y_i/\sqrt{i} \leq \lim_{k\to\infty} \frac{k}{\sqrt{\sum_{j<k} r_j}} = 0$$
   and the central limit theorem 2.5 proves our Theorem 1.1.

Suppose F is the free group generated by $(e_i)_{i\in\mathbb{N}}$.

Define $N_i := D_i(\langle e_1, \ldots, e_i\rangle)\langle e_k\colon k > i\rangle$. As above we conclude that $(N_i)_{i\in\mathbb{N}}$ satisfies the conclusions of Theorem 1.1.

4. Remarks

1. Let $p^{A(n,p)n^3}$ be the number of isomorphism classes of p-groups of order p^n and p^{Bn^3} be the number of isomorphism classes of p-groups of order p^n, whose Frattini subgroup is central and elementary abelian (for p-groups $D_2(G)$ is the Frattini subgroup of G).

   G. Higman [9] and C. Sims [2] proved (see [9]):
   $$O(n^{-1/3}) = A(n,p) - \frac{2}{27} \geq B(n,p) - \frac{2}{27} \geq O(n^{-1}).$$

   Lemma 4.1: *If G is a finite p-group with elementary abelian central Frattini subgroup $\Phi(G)$, then $D_{p+1}(G) = \{1\}$.*

   Proof: $[G, \Phi(G)] = \{1\} = \{g^p : g \in \Phi(G)\}$ as Φ is central and elementary abelian. As $G/\Phi(G)$ is elementary abelian $\Phi(G)$ contains γ_2 and γ_1^p. Thus $\gamma_1^{p^2}, \gamma_2^p, \gamma_3$ and $[\gamma_1^p, \gamma_1]$ are trivial. Hence D_{p+1} is trivial too. ∎

So, for such groups $\mathcal{I}_R(G) \cong \sum_{i \leq \log_p(|G|)} y_i Y_i$ for Y_i as in Theorem 2.5 and for some $y_i \leq p$.

Hence, for a large class of p-groups G (i.e. more than $p^{B(n,p)n^3}$ of order p^n for each n) $\overline{\mathcal{I}_D(G)}$ is almost normal distributed (i.e. for every $\epsilon > 0$, there is an $n \in \mathbf{N}$ such that $\sup_{x \in \mathrm{R}} |\overline{\mathcal{I}_D(G)}(x) - \mathcal{N}_D(x)| < \epsilon$ for all p-groups G with $D_{p+1}(G) = 1$ and $|G| > p^n$).

2. For $\mathbb{Z}$ (i.e. the free group in one generator) and any normal subgroup $n\mathbb{Z}$, we have a uniform distribution $\mathcal{I}_D(\mathbb{Z}/n\mathbb{Z})$ (compare [11]).

3. A finite group G is a p-group if and only if $\mathbf{I}(G) = \mathbf{J}(G)$ (the Jacobson radical of KG, see [1] page 86).

   We can consider the filtration of the powers of the (nilpotent) radical $\mathbf{J}(G)$ of KG and define $\mathcal{J}_D(G)(i) := \dim \mathbf{J}^i/|G|$.

   If $G = G_1 \oplus G_2$, then $\mathcal{J}_R(G)$ is the independent sum of $\mathcal{J}_R(G_i)$ (not difficult to prove). Thus, if H is a group with $\mathcal{J}_R(H)$ not constant (i.e. p divides $|H|$) then $\lim_{n \to \infty} \overline{\mathcal{J}_D(H^n)} = \mathcal{N}_D$. See [14].

4. A function $f : \{1, \ldots, n\} \to \mathbf{N}$ is unimodal if there is an integer m such that $f(i) \leq f(i+1)$ if $i \leq m$ and $f(i) \geq f(i+1)$ if $i > m$. The results of this paper suggest that, for p-groups G, the function $i \to \dim \mathbf{J}^i/\mathbf{J}^{i+1}$ is close to unimodal.

   The unimodality question is an open problem for $p > 3$ but there are partial positive results. e.g. Manz and Staszewski in [7] and Shalev in [10]. On the other hand there are counter-examples for $p = 2$.

References

[1] D. J. Benson, *Representations and Cohomology I*, Cambridge University Press, 1991.

[2] G. Higman, *Enumerating p-groups I*, Proceedings of the London Mathematical Society (3) **10** (1960), 24–30.

[3] S. Jennings, *The structure of the group ring of a p-group over a modular field*, Transactions of the American Mathematical Society **50** (1941), 175–185.

[4] M. Lazard, *Sur les groupes nilpotents et les anneaux de Lie*, Annales Scientifiques de l'École Normale Supérieure **71** (1954), 101–109.

[5] H. Lüneburg, *Tools and Fundamental Constructions of Combinatorial Mathematics*, BI-Wiss.-Verlag, Mannheim, Wien, Zürich, 1989.

[6] W. Magnus, *Über Beziehungen zwischen höheren Kommutatoren*, Journal für die reine und angewandte Mathematik **177** (1937), 105–117.

[7] O. Manz and R. Staszewski, *On the number of generator and the modular group-ring of a finite p-group,* Proceedings of the American Mathematical Society **98** (1986), 189–195.

[8] D. G. Quillen, *On the associated graded ring of a group ring,* Journal of Algebra **10** (1968), 411–418.

[9] C. C. Sims, *Enumerating p-groups,* Proceedings of the London Mathematical Society (3) **15** (1965), 151–66.

[10] A. Shalev, *Dimension subgroups, nilpotency indices, and the number of ideals in a p-group algebra,* Journal of Algebra **129** (1990), 412–438.

[11] A. Shalev, *Uniserial permutation modules,* The Quarterly Journal of Mathematics. Oxford (2) **42** (1991), 375–378.

[12] A. Shalev, *Finite p-groups,* in *Finite and Locally Finite Groups* (B. Hartley, G. M. Seitz, A. V. Borovik and R. M. Bryant, eds.), NATO Advances Science Institutes Series, Kluwer Academic Publishers, Dordrecht, Boston, London, 1995, pp. 401–451.

[13] A. N. Shiryayev, *Probability,* Springer-Verlag, New York, Berlin, Tokyo, 1984.

[14] M. Weidner, *Loewy-Reihen, Codes und Markov-Ketten,* Habilitationsschrift, Freiburg, 1995.

[15] E. Witt, *Treue Darstellungen Liescher Ringe,* Journal für die reine und angewandte Mathematik **177** (1937), 152–160.