

ON PARTIAL AUGMENTATIONS OF ELEMENTS IN INTEGRAL GROUP RINGS

VICTOR BOVDI AND ATTILA MARÓTI

ABSTRACT. Inner relations are derived between partial augmentations of certain elements (units or idempotents) in group rings.

1. INTRODUCTION

Let KG be the group ring of a group G over a commutative ring K with identity. Let $U(KG)$ be the group of units of KG . The subgroup

$$V(KG) = \left\{ \sum_{g \in G} \alpha_g g \in U(KG) \quad \mid \quad \alpha_g \in K, \quad \sum_{g \in G} \alpha_g = 1 \right\}$$

of $U(KG)$ is called the *normalized group of units* of KG . It is easy to see that if $U(K)$ denotes the group of units of the ring K , then

$$U(KG) = V(KG) \times U(K)$$

and that G is a subgroup of $V(KG)$.

For $g \in G$ let g^G denote the conjugacy class of g in G . Let $u = \sum_{g \in G} \alpha_g g \in KG$. For $y \in G$ let $\nu_y(u) = \sum_{g \in y^G} \alpha_g$ be the *partial augmentation* of u with respect to y . Observe that $\nu_x(u)$ is the same for all $x \in y^G$.

The element $\text{Tr}^{(n)}(u) = \sum_{g \in G\{n\}} \alpha_g \in K$ is called the n^{th} *generalized trace* of the element u (see [2, p.2932]), where $G\{n\}$ is the set of elements of order p^n of G where n is a non-negative integer and p is a prime. Clearly, $\text{Tr}^{(0)}(u)$ coincides with $\nu_1(u) = \alpha_1$ of $u \in KG$.

Let $K = \mathbb{Z}$, the ring of integers. Let $u = \sum_{g \in G} \alpha_g g \in V(\mathbb{Z}G)$ be a torsion unit, that is, an element of finite order $|u|$. There are several connections between $|u|$, the partial augmentations $\nu_g(u)$ ($g \in G$) and $\text{Tr}^{(i)}(u)$ for $i = 0, 1, \dots, |u|$. Such a relationship was first obtained by Higman and Berman (see [2, p.2932] or [14]), namely that $\nu_1(u) = 0$ for a finite group G . More generally, it is also a consequence of the Higman-Berman Theorem that $\nu_g(u) = 0$ for every central element g of a finite group G . The Higman-Berman Theorem was extended for arbitrary groups G by Bass and Bovdi (see [2, Fact 1.2, p.2932] or [3, Proposition 8.14, p.185] and [4]).

Key words and phrases. group ring, partial augmentation, unit, idempotent.

Note that it is still an open question whether $\nu_g(u) = 0$ for every central element g of an arbitrary group G ?

The *spectrum* of a group is the set of orders of its torsion elements. A main unsolved problem in the theory of integral group rings is the *Spectrum Problem* (SP) which says that the spectra of G and $V(\mathbb{Z}G)$ coincide. A stronger version of SP was the *Zassenhaus Conjecture* (ZC), which says that for a finite group G each torsion unit of $V(\mathbb{Z}G)$ is rationally conjugate to an element of G . The ZC can also be reformulated in terms of conditions on $\nu_g(u)$ for each torsion unit $u \in V(\mathbb{Z}G)$. A historical overview of this topic may be found in the survey [13].

For certain finite groups G , the cornerstone for solving the ZC is the so-called *Luthar-Passi method* introduced in [12]. Together with results such as [9, Proposition 5], [10, Proposition 3.1], [11, Proposition 2.2], [7] and (p, q) -character theory from [6], the Luthar-Passi method provides ZC for certain groups G (see [13]) as well as a counterexample to ZC (see [8]).

After the negative solution of the ZC a question asked by Bovdi (see [2, Fact 1.5, p. 2932]) is gaining relevance. Is it true that if u is a torsion unit of $\mathbb{Z}G$ of order p^n where p is a prime and n is a positive integer, then $\text{Tr}^{(i)}(u) = 0$ for all $i < n$ and $\text{Tr}^{(n)}(u) = 1$?

Note that the above methods work exclusively only when G is finite. With the exception of the Bass-Bovdi Theorem, there is no result which gives a restriction for $\nu_g(u)$ where G is an infinite group and u is a torsion unit.

Recall that the Möbius function μ is defined on the set of positive integers as follows: $\mu(1) = 1$, $\mu(n) = 0$ if n is divisible by the square of a prime, and $\mu(n) = (-1)^\ell$ if $n = \prod_{i=1}^\ell p_i$ where p_1, \dots, p_ℓ are distinct primes.

Our first result is a new relation between partial augmentations of a torsion unit of $\mathbb{Z}G$ where G is a finite group.

Theorem 1. *Let $u \in V(\mathbb{Z}G)$ be a torsion unit of the integral group ring $\mathbb{Z}G$ of a finite group G . Let k, n be positive integers such that k is coprime to the exponent of G . If n and k are both congruent to 1 modulo $|u|$, then for every $s \in G$ we have*

$$(1) \quad \nu_s(u) = \sum_{r|t|n} \mu(r) \cdot \left(\sum_{\substack{x^G, \exists y \in G: \\ y^{(knr)}/t = x^k \sim s}} \nu_x(u) \right).$$

Formula (9), which is part of the proof of Theorem 1, may be of independent interest. The proof of Theorem 1 also depends on the following result in which G is not necessarily a finite group and u is not necessarily a unit.

Theorem 2. *Let u be an element of the integral group ring $\mathbb{Z}G$ of a group G . Let p be a prime and $q = q' \cdot m$ a positive integer such that m is the p -part of q and q' is not divisible by p . For every $s \in G$ we have*

$$(2) \quad \nu_s(u^q) \equiv \sum_{r|t|q'} \mu(r) \cdot \left(\sum_{\substack{x^G, \exists y \in G: \\ y^{\frac{qr}{t}} = x^m \sim s}} \nu_x(u^{q'}) \right) \pmod{p}.$$

In the special case when G is a finite group and $u \in \mathbb{Z}G$ is a torsion unit the main result of Wagner (see [15]) could be compared with our Theorem 2.

Note that Theorem 2 may be applied to the case when u is a nilpotent element of $\mathbb{Z}G$ with nilpotency index larger than q' .

Let G be a finite group. Let \mathbb{Q} and \mathbb{C} be the fields of rational and complex numbers respectively. If e is an idempotent of $\mathbb{C}G$, then $\nu_1(e) \in \mathbb{Q}$ and $0 < \nu_1(e) < 1$ unless $e \in \{0, 1\}$ (see [17]). Furthermore, $|\nu_g(e)|^2 \leq |g^G| \cdot \nu_1(e)$ (see [16, Theorem 2, p. 208]) and $\sum_{i=1}^m |\nu_i(e)|^2 / |a_i^G| \leq 1$, where $\{a_1, \dots, a_m\}$ is a set of representatives of the conjugacy classes of G (see [9, Corollary 2.6, p. 2330]).

A consequence of Theorem 2 is a new relation between the partial augmentations of an idempotent in $\mathbb{Q}G$ where G is an arbitrary group.

Corollary 1. *Let e be an idempotent of $\mathbb{Q}G$ of a group G . Let $\beta \in \mathbb{Z}$ such that $u = \beta e \in \mathbb{Z}G$. Let p be a prime and $q = q' \cdot m$ a positive integer such that m is the p -part of q and q' is not divisible by p . If p does not divide β , then for every $s \in G$ we have*

$$(3) \quad \nu_s(u) \equiv \sum_{r|t|q'} \mu(r) \cdot \left(\sum_{\substack{x^G, \exists y \in G: \\ y^{\frac{qr}{t}} = x^m \sim s}} \nu_x(u) \right) \pmod{p}.$$

Moreover, if G is finite and $p > 4q' \cdot |\beta| \cdot |G|^{3/2}$, then in (3) equality holds.

2. PROOFS

Proof of Theorem 2. For elements x and y in G we write $x \sim y$ if x is conjugate to y .

Let $s \in G$. We wish to give an expression for $\nu_s(u^q)$. We need some notation.

Consider the set $\mathcal{K} = \{(g_1, \dots, g_q) \in G^q \mid g_1 \cdots g_q \sim s\}$. There is a permutation π acting on \mathcal{K} by sending $(g_1, g_2, \dots, g_q) \in \mathcal{K}$ to $(g_2, \dots, g_q, g_1) \in \mathcal{K}$. Let t be a positive divisor of q . Let the union of those $\langle \pi \rangle$ -orbits on \mathcal{K} which have lengths dividing t be denoted by

$$\mathcal{K}_t = \{(g_1, \dots, g_q) \in \mathcal{K} \mid g_{i+t} = g_i \text{ for every } i \text{ with } 1 \leq i \leq q - t\}$$

and let the union of orbits length t on \mathcal{K} be \mathcal{K}_t^* . Observe that $\mathcal{K} = \mathcal{K}_q$ and $\mathcal{K}_t = \cup_{r|t} \mathcal{K}_r^*$.

Write $u = \sum_{g \in G} \alpha_g g \in \mathbb{Z}G$. It is easy to see that

$$(4) \quad \nu_s(u^q) = \sum_{(g_1, \dots, g_q) \in \mathcal{K}} \prod_{j=1}^q \alpha_{g_j} = \sum_{t|q} \sum_{(g_1, \dots, g_q) \in \mathcal{K}_t^*} \prod_{j=1}^q \alpha_{g_j}.$$

Since \mathcal{K}_t^* is the union of all $\langle \pi \rangle$ -orbits of length exactly t , the multiplicity of each summand in the sum $\sum_{(g_1, \dots, g_q) \in \mathcal{K}_t^*} \prod_{j=1}^q \alpha_{g_j}$ is divisible by t . Thus (4) provides

$$(5) \quad \begin{aligned} \nu_s(u^q) &\equiv \sum_{\substack{t|q \\ p \nmid t}} \sum_{(g_1, \dots, g_q) \in \mathcal{K}_t^*} \prod_{j=1}^q \alpha_{g_j} \equiv \sum_{t|q'} \sum_{(g_1, \dots, g_q) \in \mathcal{K}_t^*} \prod_{j=1}^q \alpha_{g_j} \\ &\equiv \sum_{t|q'} \sum_{(g_1, \dots, g_q) \in \mathcal{K}_t^*} \left(\prod_{j=1}^{q'} \alpha_{g_j} \right)^m \equiv \sum_{t|q'} \sum_{(g_1, \dots, g_q) \in \mathcal{K}_t^*} \prod_{j=1}^{q'} \alpha_{g_j} \pmod{p}. \end{aligned}$$

If f_1 and f_2 are two functions from \mathbb{Z} to \mathbb{Z} such that $f_1(t) = \sum_{r|t} f_2(r)$, then $f_2(t) = \sum_{r|t} \mu(r) f_1(t/r)$. This is the Möbius inversion formula (see [1, Theorem 2.9, p. 32]).

For positive integers t and r , put

$$f_1(t) = \sum_{(g_1, \dots, g_q) \in \mathcal{K}_t} \prod_{j=1}^{q'} \alpha_{g_j} \quad \text{and} \quad f_2(r) = \sum_{(g_1, \dots, g_q) \in \mathcal{K}_r^*} \prod_{j=1}^{q'} \alpha_{g_j}.$$

The Möbius inversion formula then yields

$$(6) \quad \sum_{(g_1, \dots, g_q) \in \mathcal{K}_t^*} \prod_{j=1}^{q'} \alpha_{g_j} = \sum_{r|t} \mu(r) \sum_{(g_1, \dots, g_q) \in \mathcal{K}_{t/r}} \prod_{j=1}^{q'} \alpha_{g_j}.$$

Formulas (5) and (6) yield

$$\begin{aligned} \nu_s(u^q) &\equiv \\ &\equiv \sum_{t|q'} \left(\sum_{r|t} \mu(r) \sum_{(g_1, \dots, g_q) \in \mathcal{K}_{t/r}} \prod_{j=1}^{q'} \alpha_{g_j} \right) \equiv \sum_{r|t|q'} \mu(r) \cdot \left(\sum_{(g_1, \dots, g_q) \in \mathcal{K}_{t/r}} \prod_{j=1}^{q'} \alpha_{g_j} \right) \\ &\equiv \sum_{r|t|q'} \mu(r) \cdot \left(\sum_{\substack{(g_1, \dots, g_{q'}) \in G^{q'} \\ (g_1 \cdots g_{t/r})^{qr/t} = (g_1 \cdots g_{q'})^{m \sim s}}} \prod_{j=1}^{q'} \alpha_{g_j} \right) \\ &\equiv \sum_{r|t|q'} \mu(r) \cdot \left(\sum_{\substack{x^G, \exists y \in G: \\ y^{qr/t} = x^{m \sim s}}} \nu_x(u^{q'}) \right) \pmod{p}. \end{aligned}$$

□

Proof of Theorem 1. Let s, p, q, q' and m be as in Theorem 2. Let $n = q'$ and $m = p$. By (2) of Theorem 2 we have

$$(7) \quad \nu_s(u^{np}) \equiv \sum_{r|t|n} \mu(r) \cdot \left(\sum_{\substack{x^G, \exists y \in G: \\ y^{npr/t} = x^p \sim s}} \nu_x(u^n) \right) \pmod{p}.$$

Let k be a positive integer coprime to the exponent e of G . Choose p such that $p \equiv k \pmod{e}$. There are infinitely many such primes by Dirichlet's theorem on arithmetic progressions [1, Chapter 7].

Since $p \equiv k \pmod{e}$, in (7) we have $y^{\frac{npr}{t}} = y^{\frac{nk r}{t}}$ and $x^p = x^k$. Moreover, $u^{np} = u^{nk}$ by the Cohn-Livingstone Theorem [7, Corollary 4.1]. This yields

$$(8) \quad \nu_s(u^{nk}) \equiv \sum_{r|t|n} \mu(r) \cdot \left(\sum_{\substack{x^G, \exists y \in G: \\ y^{nkr/t} = x^k \sim s}} \nu_x(u^n) \right) \pmod{p}.$$

The absolute value of every partial augmentation of G is at most $\sqrt{|G|}$ (really $\nu_y(x)^2 \leq |y^G|$) by [9, Corollary 2.3, p. 2329] or [5]. The number of summands on the right-hand side of (8) is at most $(2\sqrt{n})^2 \cdot |G|$. Choose p such that $p > (2\sqrt{n})^2 \cdot |G|^{3/2}$. Since both sides of the congruence (8) have absolute value less than p ,

$$(9) \quad \nu_s(u^{nk}) = \sum_{r|t|n} \mu(r) \cdot \left(\sum_{\substack{x^G, \exists y \in G: \\ y^{(knr)/t} = x^k \sim s}} \nu_x(u^n) \right).$$

If k and n are both congruent to 1 modulo $|u|$, then we get (1). \square

Proof of Corollary 1. Let s, p, q, q' and m be as in Theorem 2. Since $u^r = \beta^{r-1}u$, we get $\nu_s(u^r) = \nu_s(\beta^{r-1}u) = \beta^{r-1}\nu_s(u)$, where $r \in \{q, q'\}$. Theorem 2 gives

$$\beta^{q-q'} \nu_s(u) \equiv \sum_{r|t|q'} \mu(r) \cdot \left(\sum_{\substack{x^G, \exists y \in G: \\ y^{qr/t} = x^m \sim s}} \nu_x(u) \right) \pmod{p}.$$

Congruence (3) follows by observing that $\beta^{q-q'} = (\beta^m)^{q'} \beta^{-q'} \equiv 1 \pmod{p}$ since m is a p -power.

The absolute value of the left-hand side of (3) is at most $|\beta| \cdot \sqrt{|G|}$ and the absolute value of the right-hand side of (3) is at most $(2\sqrt{q'})^2 \cdot |G| \cdot |\beta| \cdot \sqrt{|G|}$, by [16, Theorem 2, p. 208]. If $p > 4q' \cdot |\beta| \cdot |G|^{3/2}$, then equality in (3) holds. \square

REFERENCES

- [1] T. Apostol. *Introduction to analytic number theory*. Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1976.
- [2] V. A. Artamonov and A. A. Bovdi. Integral group rings: groups of invertible elements and classical K -theory. In *Algebra. Topology. Geometry, Vol. 27 (Russian)*, Itogi Nauki i Tekhniki, pages 3–43, 232. Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1989. Translated in J. Soviet Math. **57** (1991), no. 2, 2931–2958.
- [3] H. Bass. Euler characteristics and characters of discrete groups. *Invent. Math.*, 35:155–196, 1976.
- [4] A. Bovdi. On the isomorphism of integer group rings. *Proceedings XXIX Sci. Conf. Prof.-Teacher. composition Uzhgorod University. Section. Mat.Sci. Uzhgorod University, Uzhgorod*, pages 104–109, ibid. Dep. at VINITI 10.111.1976, No. 705–76 Dep. (RZhMat, 1976, 7A332), 1975.
- [5] V. Bovdi and M. Hertweck. Zassenhaus conjecture for central extensions of S_5 . *J. Group Theory*, 11(1):63–74, 2008.
- [6] V. A. Bovdi and A. B. Konovalov. Torsion units in integral group ring of Higman-Sims simple group. *Studia Sci. Math. Hungar.*, 47(1):1–11, 2010.
- [7] J. A. Cohn and D. Livingstone. On the structure of group algebras. I. *Canadian J. Math.*, 17:583–593, 1965.
- [8] F. Eisele and L. Margolis. A counterexample to the first Zassenhaus conjecture. *Adv. Math.*, 339:599–641, 2018.
- [9] A. W. Hales, I. S. Luthar, and I. B. S. Passi. Partial augmentations and Jordan decomposition in group rings. *Comm. Algebra*, 18(7):2327–2341, 1990.
- [10] M. Hertweck. On the torsion units of some integral group rings. *Algebra Colloq.*, 13(2):329–348, 2006.
- [11] M. Hertweck. Torsion units in integral group rings of certain metabelian groups. *Proc. Edinb. Math. Soc. (2)*, 51(2):363–385, 2008.
- [12] I. S. Luthar and I. B. S. Passi. Zassenhaus conjecture for A_5 . *Proc. Indian Acad. Sci. Math. Sci.*, 99(1):1–5, 1989.
- [13] L. Margolis and A. del Río. Finite subgroups of group rings: a survey. *Adv. Group Theory Appl.*, 8:1–37, 2019.
- [14] R. Sandling. Berman’s work on units in group rings. In *Representation theory, group rings, and coding theory*, volume 93 of *Contemp. Math.*, pages 47–66. Amer. Math. Soc., Providence, RI, 1989.
- [15] R. Wagner. Zassenhausvermutung über die Gruppen $\mathrm{PSL}(2, p)$. *Diplomarbeit, Universität*, 1995.
- [16] A. Weiss. Idempotents in group rings. *J. Pure Appl. Algebra*, 16(2):207–213, 1980.
- [17] A. E. Zalesskiĭ. A certain conjecture of Kaplansky. *Dokl. Akad. Nauk SSSR*, 203:749–751, 1972.

DEPARTMENT OF MATHEMATICAL SCIENCES, UAEU, AL-AIN, UNITED ARAB EMIRATES
Email address: vbovdi@gmail.com

ALFRÉD RÉNYI INSTITUTE OF MATHEMATICS, EÖTVÖS LORÁND RESEARCH NETWORK, P.O.
 BOX 127, H-1364, BUDAPEST, HUNGARY
Email address: maroti.attila@renyi.hu