JOURNAL OF NUMBER THEORY 45, 92–111 (1993)

Applications of Group Representation Theory to the Easier Waring Problem

LAURENT HABSIEGER

Centre de Recherches en Mathématiques de Bordeaux,
CNRS Unité Associée 226, Université Bordeaux 1,
351, cours de la Libération, 33405 Talence Cedex, France

Communicated by M. Waldschmidt

Received November 7, 1991; revised March 1, 1992

We show how Rao and Vaserstein's identities may be related to the groups S_2^2 and S_3. We then develop a theory that enables us to produce various identities, for any given pair (G, ε) of a group G and a character ε defined on G. When ε is ± 1-valued, these identities may be used to obtain upper bounds for the easier Waring problem over $\mathbb{Z}$ and $\mathbb{Q}$. This approach may be considered as an alternative to the Tarry–Escott problem.

1. INTRODUCTION

In a recent paper [11] Vaserstein mentioned Rao's identity

$$\begin{aligned}(a^5c+bdx)^6+(a^5d-bcx)^6+(b^5c-adx)^6+(b^5d+acx)^6-(a^5c-bdx)^6\\ -(a^5d+bcx)^6-(b^5c+adx)^6-(b^5d-acx)^6\\ =12abcd(c^4-d^4)(a^{24}-b^{24})\,x.\end{aligned}$$

He noticed that Fuchs and Wright [5] were unable to "find similar identities for higher values of k," Rao's identity corresponding to the case $k=6$. He proposed such an identity for $k=8$,[1]

$$\begin{aligned}(a^{56}b^{31}c^{54}x+b^{31}c^{110})^8+(a^{25}c^{116}x+a^{25}b^{88}c^{28})^8\\ +(a^{25}b^{31}c^{85}x+a^{57}b^{63}c^{21})^8+(a^{55}b^{25}c^{61}x-a^7b^{73}c^{61})^8\\ +(a^{20}bc^{120}x-a^{60}b^{81})^8+(a^{31}b^{36}c^{74}x-a^{15}b^{28}c^{98})^8\end{aligned}$$

[1] There were a couple of misprints in the original formula: the linear terms $a^{31}b^{36}c^{74}x \pm a^{15}b^{63}c^{63}$ have to be replaced by $a^{31}b^{36}c^{74}x \pm a^{15}b^{28}c^{98}$, and the last monomial in the definition of e is $a^{80}b^{-16}c^{640}$ instead of $a^{80}b^{229}c^{395}$.

0022-314X/93 $5.00

$$\begin{aligned}
&-(a^{56}b^{31}c^{54}x - b^{31}c^{110})^8 - (a^{25}c^{116}x - a^{25}b^{88}c^{28})^8\\
&-(a^{25}b^{31}c^{85}x - a^{57}b^{63}c^{21})^8 - (a^{55}b^{25}c^{61}x + a^7b^{73}c^{61})^8\\
&-(a^{20}bc^{120}x + a^{60}b^{81})^8 - (a^{31}b^{36}c^{74}x + a^{15}b^{28}c^{98})^8\\
={}&16[a^{56}b^{248}c^{824} + a^{200}b^{616}c^{312} + a^{424}b^{472}c^{232} - a^{440}b^{568}c^{120}\\
&-a^{136}b^{232}c^{760} - a^{104}b^{536}c^{488}]\,x.
\end{aligned}$$

Vaserstein's identity does not seem to be as symmetric as Rao's. However, a tricky change of variables reveals symmetries in Vaserstein's identity. More precisely let us put

$$\begin{aligned}
u &= a^{50/17}b^{21/17}c^{70/17},\\
v &= a^{-35/17}b^{38/17}c^{138/17},\\
w &= a^{67/17}b^{123/17}c^{-49/17},\\
y &= a^{300/17}b^{-316/17}c^{862/17}.
\end{aligned}$$

Then Vaserstein's identity becomes

$$\begin{aligned}
&(u^7v^{10} + u^5w^6y)^8 + (u^7w^{10} - u^5v^6y)^8 + (v^7w^{10} + v^5u^6y)^8\\
&\quad + (v^7u^{10} - v^5w^6y)^8 + (w^7u^{10} + w^5v^6y)^8 + (w^7v^{10} - w^5u^6y)^8\\
&\quad - (u^7v^{10} - u^5w^6y)^8 - (u^7w^{10} + u^5v^6y)^8 - (v^7w^{10} - v^5u^6y)^8\\
&\quad - (v^7u^{10} + v^5w^6y)^8 - (w^7u^{10} - w^5v^6y)^8 - (w^7v^{10} + w^5u^6y)^8\\
&= 16(uvw)^6\,(u^{48}v^{64} + v^{48}w^{64} + w^{48}u^{64} - u^{48}w^{64} - v^{48}u^{64} - w^{48}v^{64})\,y.
\end{aligned}$$

In this identity, the group S_3 of the permutations of $\{u, v, w\}$ appears naturally. In Rao's identity the group occurring was $S_2 \times S_2$, i.e., the permutations of $\{a, b\} \times \{c, d\}$. This led us to develop a theory that would provide identities of this kind for any finite group.

In Section 2 we define a so-called (weak) k-admissibility notion and prove two related lemmas. Section 3 provides some initial inequalities, which motivate a conjecture about the equivalence of k-admissibility and weak k-admissibility. In Section 4 we establish some formulas that help to effectively compute some k-admissibility degrees. We apply these results in Section 5 to dihedral groups and give algorithms to derive identities from a given group; we also make explicit these identities for the dihedral groups D_n for $n \leqslant 3$. Section 6 is concerned with the size of the identities we can obtain this way and some upper bounds are given. We then use these identities to derive some upper bounds in number theory for the easier Waring problem for algebras of characteristic zero over a field (Section 7), the easier Waring problem over $\mathbb{Z}$ (Section 8), and the non-trivial representations of zero as sums or differences of k-powers (Section 9). We end this article by presenting some possible extensions of this work.

2. Definitions and First Properties

Let G be a finite group and let ε be a non-trivial representation of G of dimension 1.

For any finite dimensional representation V of G over a field K of characteristic zero, we will define a notion of k-admissibility. For any nonnegative integer k, we will say that G is k-admissible over V with respect to ε if and only if the following condition is satisfied: $\forall((\lambda_1, \mu_1), ..., (\lambda_k, \mu_k)) \in (\mathbb{Q}^2)^k$, $\exists(\alpha, \beta) \in V^2$ such that

(i) $\forall i \in \{1, ..., k\}, \exists g_i \in G$, with $\varepsilon(g_i) \neq 1$ and $\lambda_i\alpha + \mu_i\beta \in \operatorname{Fix} g_i$,

(ii) $\forall g \in G, \alpha \in \operatorname{Fix} g$ and $\beta \in \operatorname{Fix} g$ imply $\varepsilon(g) = 1$.

Here $\operatorname{Fix} g$ denotes the space of vectors in V invariant under the action of g.

Similarly we will say that G is weakly k-admissible over V with respect to ε if and only if the following condition is satisfied: There exist two polynomials functions $\bar{\alpha}$ and $\bar{\beta}$ in the $((\lambda_i, \mu_i))_{1 \leqslant i \leqslant k}$, with values in V and coefficients in K such that

(i) $\forall i \in \{1, ..., k\}, \exists g_i \in G$, with $\varepsilon(g_i) \neq 1$ and $\lambda_i\bar{\alpha} + \mu_i\bar{\beta} \in \overline{\operatorname{Fix}}\, g_i$,

(ii) $\forall g \in G, \bar{\alpha} \in \overline{\operatorname{Fix}}\, g$ and $\bar{\beta} \in \overline{\operatorname{Fix}}\, g$ imply $\varepsilon(g) = 1$.

Here the action of G on polynomial functions is the one induced by the action of G on V, and $\overline{\operatorname{Fix}}\, g$ denotes the space of invariants for this action.

Remark. In the definition of k-admissibility, we may replace $\mathbb{Q}$ by $\mathbb{Z}$, for the underlying set of the λ_i's and μ_i's. Indeed the conditions (i) and (ii) do not change when λ_i (resp. μ_i) is replaced by $d\lambda_i$ (resp. $d\mu_i$); choosing d to be a common denominator of the λ_i's and μ_i's completes the proof of this remark. The same argument shows that $(\mathbb{Q}^2)^k$ may be replaced by $(\{1\} \times \mathbb{Q} \cup \{(0, 1)\})^k$ or $(\mathbb{Q} \times \{1\} \cup \{(1, 0)\})^k$.

Lemma 1. *If G is (weakly) k-admissible over V with respect to ε, then G is (weakly) l-admissible over V with respect to ε, for any nonnegative integer l less than or equal to k.*

Proof. Let $((\lambda_1, \mu_1), ..., (\lambda_1, \mu_1)) \in (\mathbb{Q}^2)^l$ be given. Let us complete this l-tuple of pairs of scalars by $k-l$ zero pairs. We can apply the k-admissibility property to get the l-admissibility.

Now, if G is weakly k-admissible over V with respect to ε, let us evaluate $\bar{\alpha}$ and $\bar{\beta}$ at $(\lambda', \mu') = ((\lambda_{l+1}, \mu_{l+1}), ..., (\lambda_k, \mu_k))$. The condition (i) is trivially satisfied so we have to concentrate on condition (ii). Let us suppose that this condition is not satisfied, for any $(k-l)$-tuple (λ', μ'). To each element g in G with $\varepsilon(g) \neq 1$, we may define $\mathbb{Q}(g)$ to be the set of all $(k-l)$-tuples (λ', μ') such that the evaluations of $\bar{\alpha}$ and $\bar{\beta}$ at (λ', μ') belong to $\overline{\text{Fix}}\, g$. Then $(\mathbb{Q}^2)^{k-l} = \bigcup_{\varepsilon(g) \neq 1} \mathbb{Q}(g)$. Thus there exists a g_0 in G with $\varepsilon(g_0) \neq 1$, such that $\mathbb{Q}(g_0)$ contains a subset of the form $S_1 \times \cdots \times S_{2k-2l}$, where S_i is an infinite subset of $\mathbb{Q}$ (otherwise $(\mathbb{Q}^2)^{k-l}$ would be a finite union of proper subspaces). Since the conditions $\bar{\alpha} \in \overline{\text{Fix}}\, g_0$ and $\bar{\beta} \in \overline{\text{Fix}}\, g_0$ are algebraic (via the cartesian equations) and satisfied on $S_1 \times \cdots \times S_{2k-2l}$, they are satisfied for all (λ', μ'). This contradicts the k-admissibility hypothesis. Thus there exists (λ'_0, μ'_0) such that the evaluations of $\bar{\alpha}$ and $\bar{\beta}$ at (λ'_0, μ'_0) satisfy the condition (ii). ▮

LEMMA 2. *If G is (weakly) k-admissible over V with respect to ε, then k is less than the order of G.*

Proof. Let us take for (λ, μ) the k-tuple of pairs $((1, 1), (1, 2), ..., (1, k))$. Then, for any subspace W of V, and for any vectors α, β in V, we have

$$\{\alpha + i\beta, \alpha + j\beta\} \subset W \Rightarrow \{\alpha, \beta\} \subset W \qquad \text{when} \quad i \neq j.$$

This implies that the g_i's defined by the condition (i) are all distinct. Thus k is less than the order of G. Similarly, if G is weakly k-admissible, we have for any g

$$\{\lambda_i \bar{\alpha} + \mu_i \bar{\beta}, \lambda_j \bar{\alpha} + \mu_j \bar{\beta}\} \subset \overline{\text{Fix}}\, g \Rightarrow \{\bar{\alpha}, \bar{\beta}\} \subset \overline{\text{Fix}}\, g \qquad \text{when} \quad i \neq j.$$

This also implies that k is less than the order of G, by the same enumerative argument. ▮

This last lemma allows us to define the integer $k_\varepsilon(V; K)$ (resp. $\bar{k}_\varepsilon(V; K)$) to be the greatest integer k such that G is k-admissible (resp. weakly k-admissible) over V with respect to ε. Similarly we define $k_\varepsilon(G; K)$ (resp. $\bar{k}_\varepsilon(G; K)$) to be the maximum of the numbers $k_\varepsilon(V; K)$ (resp. $\bar{k}_\varepsilon(V; K)$), where V runs over all the representations of G over the field K. The next sections will be devoted to inequalities satisfied by these numbers, in order to make them easier to compute.

3. Some Basic Inequalities

One can ask how the notion of (weakly) k-admissibility behaves through the classical operations in representation theory. Some answers are given in the following theorem for the direct sum of two representations of G.

Theorem 1. $k_\varepsilon(V_1 \oplus V_2; K) \geqslant \max(k_\varepsilon(V_1; K), k_\varepsilon(V_2; K))$; $\bar{k}_\varepsilon(V_1 \oplus V_2; K) \geqslant \max(\bar{k}_\varepsilon(V_1; K), \bar{k}_\varepsilon(V_2; K))$.

Proof. If G is k-admissible over V_1, there exists (α_1, β_1) in V_1^2 satisfying the conditions (i) and (ii) for any (λ, μ) in $(\mathbb{Q}^2)^k$. Then the vectors $\alpha_1 + 0$ and $\beta_1 + 0$ in $V_1 \oplus V_2$ will also satisfy these requirements, for the same value of (λ, μ). This shows that

$$k_\varepsilon(V_1 \oplus V_2; K) \geqslant k_\varepsilon(V_1; K).$$

By symmetry we have also $k_\varepsilon(V_1 \oplus V_2; K) \geqslant k_\varepsilon(V_2; K)$ and thus the first part of the theorem holds. Similarly we get the second inequality in the theorem. ▮

Corollary. *If G acts trivially on V_0, we have*

$$k_\varepsilon(V \oplus V_0; K) = k_\varepsilon(V; K) \qquad \textit{and} \qquad \bar{k}_\varepsilon(V \oplus V_0; K) = \bar{k}_\varepsilon(V; K).$$

Proof. Since G acts trivially on V_0, we know that every vector in V_0 is fixed by any element of G. Therefore the condition (ii) cannot be satisfied and $k_\varepsilon(V_0; K) = \bar{k}_\varepsilon(V_0; K) = 0$. Then we deduce from Theorem 1 that

$$k_\varepsilon(V \oplus V_0; K) \geqslant k_\varepsilon(V; K) \qquad \text{and} \qquad \bar{k}_\varepsilon(V \oplus V_0; K) \geqslant \bar{k}_\varepsilon(V; K).$$

Now let us prove the reverse inequalities. If $V \oplus V_0$ is k-admissible, there exists, for any $2k$-tuple (λ, μ), two vectors α and β in $V \oplus V_0$ satisfying the conditions (i) and (ii). Let α' (resp. β') denote the projection of α (resp. β) on V, so that $\alpha - \alpha' \in V_0$ (resp. $\beta - \beta' \in V_0$). Then condition (i) holds in V with α' and β', for the same choice of the g_i's. Moreover, if α' and β' are fixed by an element g in G, the trivial action of G on V_0 ensures us that α and β are fixed by g. Using condition (ii) also in $V \oplus V_0$, we deduce that $\varepsilon(g) = 1$. Therefore condition (ii) also holds in V and V is k-admissible. Thus we have $k_\varepsilon(V \oplus V_0; K) \leqslant k_\varepsilon(V; K)$. The same technique leads to $\bar{k}_\varepsilon(V \oplus V_0; K) \leqslant \bar{k}_\varepsilon(V; K)$ and the proof of the corollary is completed. ▮

These first results show some similarities between the behaviors of $k_\varepsilon(V; K)$ and $\bar{k}_\varepsilon(V; K)$. As a matter of fact we have the following proposition, which justifies the term "weakly."

PROPOSITION 1. $k_\varepsilon(V; K) \leqslant \bar{k}_\varepsilon(V; K)$.

Proof. Let us put $k = k_\varepsilon(V; K)$. For each k-tuple of pairs of scalars (λ, μ), we may associate a k-tuple $(g_1, ..., g_k)$ of elements of G. As in the proof of Lemma 1, we may find a particular k-tuple $(g_1^0, ..., g_k^0)$ that is associated to a subset of $\mathbb{Q}^{2k}$ of the form $S_1 \times \cdots \times S_{2k}$, where S_i is an infinite subset of $\mathbb{Q}$. Each condition $\lambda_i \alpha + \mu_i \beta \in \operatorname{Fix} g_i^0$ is linear in the coordinates of α and β. Thus to find α and β satisfying to the conditions in (i) with $(g_1^0, ..., g_k^0)$ is equivalent to solving an homogeneous system of linear equations, whose coefficients are proportional to the λ_i's and μ_i's. Similarly, finding $\bar{\alpha}$ and $\bar{\beta}$ is equivalent to solving the same system, in which the λ_i's and μ_i's are now considered as variables; indeed the use of Cramer's rule under suitable assumptions shows that generic solutions will be polynomials in the λ_i's and μ_i's. We just have to check that the rank of this last system is smaller than the number of unknowns allowed. Now the determination of the rank may be done by considering determinants of minors, that are polynomials in the λ_i's and μ_i's. Let P be such a polynomial, obtained from a minor whose order is greater than or equal to the number of unknowns. We know that $P(\lambda, \mu) = 0$, for $(\lambda, \mu) \in S_1 \times \cdots \times S_{2k}$, by hypothesis. Thus $P \equiv 0$ and then we may express the generic solutions as polynomials in the λ_i's and μ_i's.

Now let us suppose that these $\bar{\alpha}$ and $\bar{\beta}$ are fixed under the action of an element g in G with $\varepsilon(g) \neq 1$. The solutions α and β associated to any (λ, μ) in $S_1 \times \cdots \times S_{2k}$ are proportional to the specialization of $\bar{\alpha}$ and $\bar{\beta}$, unless the full-rank system used to determine $\bar{\alpha}$ and $\bar{\beta}$ is degenerate at (λ, μ). Then α and β would be fixed by g, which is impossible. Thus the system is degenerate at (λ, μ), for any (λ, μ) in $S_1 \times \cdots \times S_{2k}$; that is, the determinant of the system vanishes at any (λ, μ) in $S_1 \times \cdots \times S_{2k}$. This shows that this determinant would be identically zero, which is also impossible. As a conclusion we have succeeded in finding polynomial functions $\bar{\alpha}$ and $\bar{\beta}$ satisfying conditions (i) and (ii). ∎

This last proposition motivates the following conjecture.

Conjecture. $k_\varepsilon(V; K) = \bar{k}_\varepsilon(V; K)$.

Indeed, if G is weakly k-admissible over V with respect to ε, one might want to take for α and β the evaluations of $\bar{\alpha}$ and $\bar{\beta}$ at (λ, μ). Then condition (i) would also be satisfied and condition (ii) would almost always be satisfied. Only the exceptional cases where $\{\bar{\alpha}(\lambda, \mu), \bar{\beta}(\lambda, \mu)\} \subseteq \operatorname{Fix} g$ for some g in G with $\varepsilon(g) = 1$ will pose a problem. But these conditions are algebraic in (λ, μ) so the choice $(\alpha, \beta) = (\bar{\alpha}(\lambda, \mu), \bar{\beta}(\lambda, \mu))$ will work for any (λ, μ) in $\mathbb{Q}^{2k}$ but an algebraic variety. Thus the reverse inequality in Proposition 1 is "almost" true.

4. Exact Formulas

A close look at the proof of Proposition 1 shows that the only restriction to be checked is that the number of equations is smaller than the number of unknowns. Thus, if we are able to evaluate both quantities, we will get a closed formula for $\bar{k}_\varepsilon(V; K)$. Such a formula is given by the following theorem.

Theorem 2. *Let us put*

$$k'_\varepsilon(V; K) = \max \left\{ k : \exists g_1, ..., g_k \in G, \varepsilon(g_i) \neq 1 \text{ and } \sum_{i=1}^{k} \operatorname{codim} \operatorname{Fix} g_i < 2 \operatorname{codim} \left(\bigcap_{i=1}^{k} \operatorname{Fix} g_i \right) \right\}.$$

Then $\bar{k}_\varepsilon(V; K) = k'_\varepsilon(V; K)$.

Proof. Firstly, let us prove that the equations $\lambda_i \bar{\alpha} + \mu_i \bar{\beta} \in \overline{\operatorname{Fix}}\, g_i$, for $1 \leqslant i \leqslant k$ are independent. More precisely let us suppose that the condition $v \in \operatorname{Fix} g_i$ is given by the equations E_{ij}, for $1 \leqslant j \leqslant r_i = \operatorname{codim} \operatorname{Fix} g_i$. If we have any dependence relation $0 = \sum_{ij} a_{ij} (\lambda_i E_{ij} + \mu_i E_{ij})$, the choice $(\lambda, \mu) = ((0, ..., 0, 1, 0, ..., 0), \mathbf{0})$ will show that $a_{ij} = 0$ for $1 \leqslant j \leqslant r_i$. Thus all the coefficients have to be zero and the equations $\lambda_i \bar{\alpha} + \mu_i \bar{\beta} \in \overline{\operatorname{Fix}}\, g_i$ are independent; their number is $\sum_{i=1}^k r_i = \sum_{i=1}^k \operatorname{codim} \operatorname{Fix} g_i$.

We now have to evaluate the number of unknowns allowed. Because of condition (ii), the solutions $\bar{\alpha}$ and $\bar{\beta}$ cannot lie in $\bigcap_{i=1}^k \overline{\operatorname{Fix}}\, g_i$. Thus the number of unknowns allowed is less than or equal to $2(\dim V - \dim \bigcap_{i=1}^k \operatorname{Fix} g_i) = 2 \operatorname{codim}(\bigcap_{i=1}^k \operatorname{Fix} g_i)$. Let us prove that the equality holds. Let us suppose that there exists an element g in G such that $\{\bar{\alpha}, \bar{\beta}\} \subset \overline{\operatorname{Fix}}\, g$. Since $\bar{\alpha}$ and $\bar{\beta}$ are the generic solutions of the system $\lambda_i \bar{\alpha} + \mu_i \bar{\beta} \in \overline{\operatorname{Fix}}\, g_i$, any equation defining $\overline{\operatorname{Fix}}\, g$ will be a linear combination of the equations E_{ij}. Again the same specialization of (λ, μ) as before shows that any equation defining $\overline{\operatorname{Fix}}\, g$ is a linear combination of the $(E_{ij})_{1 \leqslant j \leqslant r_i}$, for any $i \in \{1, ..., k\}$. That is $\overline{\operatorname{Fix}}\, g \subseteq \bigcap_{i=1}^k \overline{\operatorname{Fix}}\, g_i$. Thus, if the number of unknowns allowed is greater than or equal to $2 \operatorname{codim}(\bigcap_{i=1}^k \operatorname{Fix} g_i)$, condition (ii) will always be satisfied. This completes the proof of the theorem. ▮

Let us now derive some interesting consequences from the formula given in Theorem 2.

Proposition 2. $\bar{k}_\varepsilon(V_1 \oplus V_2; K) = \max(\bar{k}_\varepsilon(V_1; K), \bar{k}_\varepsilon(V_2; K))$.

Proof. Let us suppose that G is k-admissible over $V_1 \oplus V_2$ with respect to ε. Since V_1 and V_2 are fixed by G, we have

$$2\operatorname{codim}(\operatorname{Fix} g, V_1 \oplus V_2) = 2\operatorname{codim}(\operatorname{Fix} g|_{V_1}, V_1) + 2\operatorname{codim}(\operatorname{Fix} g|_{V_2}, V_2),$$

for any g in G. Thus the condition for $V_1 \oplus V_2$

$$2\operatorname{codim}\left(\bigcap_{i=1}^{k} \operatorname{Fix} g_i, V_1 \oplus V_2\right) > \sum_{i=1}^{k} \operatorname{codim}(\operatorname{Fix} g_i, V_1 \oplus V_2)$$

implies the same condition for V_1 or V_2. This shows that $\max(k'_\varepsilon(V_1; K), k'_\varepsilon(V_2; K)) \geqslant k$. Hence we get the inequality $\max(\bar{k}_\varepsilon(V_1; K), \bar{k}_\varepsilon(V_2; K)) \geqslant \bar{k}_\varepsilon(V_1 \oplus V_2; K)$. Theorem 1 provides us the reverse inequality so the proposition is proved. ▌

Proposition 3. *$\bar{k}_\varepsilon(G; K)$ does not depend on K; it will be denoted by $\bar{k}_\varepsilon(G)$.*

Proof. It is enough to show that $\bar{k}_\varepsilon(G; K) = \bar{k}_\varepsilon(G; \mathbb{Q})$. Let V be a rational representation of G. Let $V = V_1 \oplus \cdots \oplus V_j$ be a decomposition of V into irreducible representations over K. Then $\bar{k}_\varepsilon(V; \mathbb{Q}) = \bar{k}_\varepsilon(V; K) = \max_{1 \leqslant i \leqslant j} \bar{k}_\varepsilon(V_i; K) \leqslant \bar{k}_\varepsilon(G; K)$. Hence $\bar{k}_\varepsilon(G; \mathbb{Q}) \leqslant \bar{k}_\varepsilon(G; K)$. Let us prove now the reverse inequality. Similarly we have $\bar{k}(G; K) \leqslant \bar{k}_\varepsilon(G; \bar{K})$, where $\bar{K}$ is an algebraic closure of K. Thus we may suppose without loss of generality that K is algebraically closed. If $V_1, ..., V_h$ denote the irreducible representations of G over K we have $\bar{k}_\varepsilon(G; K) = \max_{1 \leqslant i \leqslant h} \bar{k}_\varepsilon(V_i; K)$. Now the regular representation of G is rational and every V_i $(1 \leqslant i \leqslant h)$ appears in it [10]. So we have

$$\bar{k}_\varepsilon(G; \mathbb{Q}) \geqslant \bar{k}_\varepsilon(V_{\text{reg}}; \mathbb{Q}) = \bar{k}_\varepsilon(V_{\text{reg}}; K) = \max_{1 \leqslant i \leqslant h} \bar{k}_\varepsilon(V_i; K) = \bar{k}_\varepsilon(G; K).$$

This completes the proof of Proposition 3. ▌

Remarks. (1) The last proof shows that $\bar{k}_\varepsilon(G) = \bar{k}(G; \mathbb{C}) = \max_i \bar{k}_\varepsilon(V_i; \mathbb{C})$, where V_i runs over all the irreducible complex representations of G. Since $\bar{k}_\varepsilon(V_i; \mathbb{C})$ may be determined in a finite number of steps by using Theorem 2, $\bar{k}_\varepsilon(G)$ may be found after a finite number of verifications.

(2) We also get from Proposition 3, $\bar{k}_\varepsilon(G) = \bar{k}_\varepsilon(G; \mathbb{Q}) = \bar{k}_\varepsilon(V_{\text{reg}}; \mathbb{Q})$. So we may find the vectors $\bar{\alpha}$ and $\bar{\beta}$ with integral coordinates.

Let us now apply these various properties to some particular groups.

5. Examples and Identities

Let us consider the dihedral group D_n as the group of isometries of a regular n-polygon. Let us take for ε the determinantal mapping, so that $\varepsilon(g)=1$ if g is a rotation in D_n and $\varepsilon(g)=-1$ if g is a symmetry. Then we have the following proposition.

Proposition 4. *We have* $k_\varepsilon(D_n; \mathbb{Q}) = \bar{k}_\varepsilon(D_n) = n$ *for* $n \leqslant 3$ *and* $\bar{k}_\varepsilon(D_n)=3$ *for* $n \geqslant 3$.

Proof. Let us suppose first that $n \geqslant 3$. One can check (see, e.g., [9, p. 37]) that for any two-dimensional irreducible representation V of D_n we have $\operatorname{codim} \operatorname{Fix} g=1$ when $\varepsilon(g)=-1$. Thus, if V is weakly k-admissible, we get the inequality $k < 2 \operatorname{codim} \bigcap_{i=1}^{k} \operatorname{Fix} g_i \leqslant 4$. Then $k \leqslant 3$ and $\bar{k}_\varepsilon(V; \mathbb{C}) \leqslant 3$. Since $n \geqslant 3$, we can choose three distinct symmetries in D_n, so that $\bigcap_{i=1}^{3} \operatorname{Fix} g_i=\{0\}$. This shows that $k'_\varepsilon(V; \mathbb{C}) \geqslant 3$. Hence $\bar{k}_\varepsilon(D_n)=3$.

Let us study now the cases $n=1, 2, 3$.

(1) For $n=1$, $D_1=S_2$. Let us take the regular representation of D_1, and let us put $(\alpha, \beta)=((\mu_1, 0), (0, \lambda_1))$ if $(\lambda_1, \mu_1) \neq (0, 0)$. If $(\lambda_1, \mu_1)=(0, 0)$, put $(\alpha, \beta)=((1, 0), (0, 0))$. Then we have $\lambda_1\alpha+\mu_1\beta \in \operatorname{Fix}(12)$ and $\{\alpha, \beta\} \not\subset \operatorname{Fix}(12)$, which shows that $k_\varepsilon(V_{\mathrm{reg}}, \mathbb{Q}) \geqslant 1$. Since $k'_\varepsilon(D_1)=1$, we have $k_\varepsilon(D_1; \mathbb{Q})=1$.

(2) For $n=2$, $D_2 \simeq S_2 \times S_2$. Let us take the product of the regular representations of S_2 and let us put $(\alpha, \beta)=((\alpha_1, \alpha_2), (\beta_1, \beta_2))$, where (α_1, β_1) and (α_2, β_2) are obtained as in (1). This shows that $k_\varepsilon(V; \mathbb{Q}) \geqslant 2$. Since one can easily check that $k'_\varepsilon(D_2) \leqslant 2$, the announced result follows.

(3) For $n=3$, $D_3 \simeq S_3$. Let us take the natural three-dimensional representation of S_3. For any $(\lambda_1, \lambda_2, \lambda_3, \mu_1, \mu_2, \mu_3)$ in $\mathbb{Q}^6$ let us put $(\alpha, \beta)=((\mu_1\mu_2\lambda_3, \mu_1\lambda_2\mu_3, \lambda_1\mu_2\mu_3), (\lambda_1\lambda_2\mu_3, \lambda_1\mu_2\lambda_3, \mu_1\lambda_2\lambda_3))$, if $(\lambda_2\mu_3-\mu_2\lambda_3)(\lambda_1\mu_3-\lambda_3\mu_1)(\lambda_1\mu_2-\lambda_2\mu_1) \neq 0$. This last condition ensures us that $(\alpha, \beta) \not\subset \operatorname{Fix} g$, for any transposition g. It corresponds to the equation of the algebraic variety described at the end of Section 3 and means that the three vectors (λ_1, μ_1), (λ_2, μ_2), (λ_3, μ_3) are pairwise independent, so that the conditions $\lambda_i\alpha+\mu_i\beta \in \operatorname{Fix} g_i$ are not redundant. If this condition is not satisfied, replace (λ, μ) by (λ', μ') such that the condition is satisfied for (λ', μ') and the lines $(\lambda_i, \mu_i)\,\mathbb{C}$ $(1 \leqslant i \leqslant 3)$ belong to $\{(\lambda'_i, \mu'_i)\,\mathbb{C}\colon 1 \leqslant i \leqslant 3\}$; then compute the corresponding value for (α, β). For instance (1, 2, 3, 0, 4, 6) may be replaced by (1, 2, 3, 0, 4, 1) without loss of generality. This shows that $k_\varepsilon(V; \mathbb{Q}) \geqslant 3$. By the first part of the proposition we have $k_\varepsilon(V; \mathbb{Q})=\bar{k}_\varepsilon(D_3)=3$. ∎

Let us see now how the notion of k-admissibility applies to get various polynomial identities. Let G be a finite group and ε a non-trivial representation of G of dimension 1. Let us assume that $\varepsilon(G)=\{-1, +1\}$.

THEOREM 3. *Let V be a finite dimensional rational representation of G such that G is k-admissible over V with respect to ε. Then there exist $2\,|G|$ polynomials of degree one in x with coefficients in $\mathbb{Q}\backslash\{0\}$, namely $(f_g(x))_{g\in G}$ and $(f'_g(x))_{g\in G}$, such that*

$$\sum_{g\in G} (f_g(x)^{2k+1} - f_g(-x)^{2k+1}) = Cx \qquad \textit{for some} \quad C\in\mathbb{Q},$$

$$\sum_{g\in G} (f'_g(x)^{2k+2} - f'_g(-x)^{2k+2}) = C'x \qquad \textit{for some} \quad C'\in\mathbb{Q}.$$

Proof. Let $(e_1, ..., e_d)$ be a basis of V. Let us define a formal exponential on V by

$$e^{\alpha} = x_1^{\alpha_1} \cdots x_d^{\alpha_d} \qquad \text{if} \quad \alpha = \sum_{i=1}^{d} \alpha_i e_i.$$

Now let us choose $(\lambda, \mu) = ((3, 2k-2), (5, 2k-4), ..., (2k+1, 0)) \in (\mathbb{Q}^2)^k$. Then we are able to find $(\alpha, \beta) \in V^2$ such that conditions (i) and (ii) of k-admissibility are satisfied. For $g\in G$, let us put $f_g(x) = \varepsilon(g)\, e^{g\cdot\alpha}x + e^{g\cdot\beta}$ and $F(x) = \sum_{g\in G} f_g(x)^{2k+1}$. The polynomial $F(x) - F(-x)$ is odd, of degree less than or equal to $2k+1$. Let us compute the coefficient S_i of $2\binom{2k+1}{2i+1}\, x^{2i+1}$, for $1 \leqslant i \leqslant k$. We have

$$\begin{aligned} S_i &= \sum_{g\in G} (\varepsilon(g)\, e^{g\cdot\alpha})^{2i+1}\, (e^{g\cdot\beta})^{(2k+1)-(2i+1)} = \sum_{g\in G} \varepsilon(g)\, e^{g\cdot(\lambda_i\alpha+\mu_i\beta)} \\ &= \sum_{g\in G} \varepsilon(gg_i)\, e^{g\cdot(g_i\cdot(\lambda_i\alpha+\mu_i\beta))} = \varepsilon(g_i) \sum_{g\in G} \varepsilon(g)\, e^{g\cdot(\lambda_i\alpha+\mu_i\beta)} \\ &= \varepsilon(g_i)\, S_i. \end{aligned}$$

Since $\varepsilon(g_i) \neq 1$, we deduce from this equality that $S_i = 0$. Thus $F(x) - F(-x) = 2(2k+1)\, S_1 x$, as required. The second equality corresponds to the choice $(\lambda, \mu) = ((3, 2k-1), (5, 2k-3), ..., (2k+1), 1))$. It is interesting to note that different specializations of the formal variables x_i will lead to different identities. Let us also remark that condition (ii) in the definition of k-admissibility ensures us that the forms are distinct. ∎

The proof of Theorem 3 provides an algorithm to construct identities from a k-admissible group. Since Proposition 4 gives us k-admissibility results for dihedral groups, let us make explicit some identities we can deduce from the proofs of Proposition 4 and Theorem 3.

(1) For $n=1$, let us consider $G=D_1=S_2$ and $(\lambda, \mu)=(3, 0)$. Let us put $a=e^{(3,0)}$ and $b=e^{(0,3)}$. Then we get the identity

$$(x+a)^3+(-x+b)^3+(x-a)^3+(-x-b)^3=6(a^2-b^2)\,x. \tag{1}$$

Now if $(\lambda, \mu)=(3, 1)$, we obtain by putting $a=e^{(1,0)}$ and $b=e^{(0,1)}$,

$$(ax+b^3)^4+(-bx+a^3)^4-(ax-b^3)^4-(bx+a^3)^4=8ab(b^8-a^8)\,x. \tag{2}$$

This identity is due to Norrie [3].

(2) For $n=2$, let us consider $G=D_2=S_2\times S_2$ and $(\lambda, \mu)=((3, 5), (2, 0))$. We find $\alpha=(2, 0, 0, 0)$ and $\beta=(0, 3, 0, 5)$. Let us put $a=e^{(1,0,0,0)}$, $b=e^{(0,1,0,0)}$, $c=e^{(0,0,5,0)}$, and $d=e^{(0,0,0,5)}$. Then we get

$$\begin{aligned}&(a^2x+b^3d)^5+(-a^2x+b^3c)^5+(-b^2x+a^3d)^5+(b^2x+a^3c)^5\\&\quad+(a^2x-b^3d)^5+(-a^2x-b^3c)^5+(-b^2x-a^3d)^5+(b^2x-a^3c)^5\\&=10a^2b^2(b^{10}-a^{10})(d^4-c^4)\,x.\end{aligned} \tag{3}$$

Now if $(\lambda, \mu)=((3, 5), (3, 1))$ we get by the same method Rao's identity

$$\begin{aligned}&(a^5c+bdx)^6+(a^5d-bcx)^6+(b^5c-adx)^6+(b^5d+acx)^6\\&\quad-(a^5c-bdx)^6-(a^5d+bcx)^6-(b^5c+adx)^6-(b^5d-acx)^6\\&=12abcd(c^4-d^4)(a^{24}-b^{24})\,x\end{aligned} \tag{4}$$

(3) For $n=3$, let us consider $G=D_3=S_3$ and $(\lambda, \mu)=((3, 4), (5, 2), (7, 0))$. We find $\alpha=(56, 0, 0)$ and $\beta=(0, 42, 140)$. Putting $a=e^{(14,0,0)}$, $b=e^{(0,14,0)}$, and $c=e^{(0,0,14)}$ leads to the identity

$$\begin{aligned}&(a^4x+b^3c^{10})^7+(b^4x+a^{10}c^3)^7+(c^4x+a^3b^{10})^7+(a^4x-b^3c^{10})^7\\&\quad+(b^4x-a^{10}c^3)^7+(c^4x-a^3b^{10})^7+(-a^4x+b^{10}c^3)^7\\&\quad+(-b^4x+a^3c^{10})^7+(-c^4x+a^{10}b^3)^7+(-a^4x-b^{10}c^3)^7\\&\quad+(-b^4x-a^3c^{10})^7+(-c^4x-a^{10}b^3)^7\\&=14(abc)^4\,(c^7-a^7)(b^7-a^7)(c^7-b^7)\\&\quad\times(a^{14}+b^{14}+c^{14}+a^7b^7+b^7c^7+a^7c^7)\,x.\end{aligned} \tag{5}$$

Now if $(\lambda, \mu) = ((3, 5), (5, 3), (7, 1))$ we get by the same method Vaserstein's identity

$$\begin{aligned}
&(u^7v^{10} + u^5w^6y)^8 + (u^7w^{10} - u^5v^6y)^8 + (v^7w^{10} + v^5u^6y)^8\\
&\quad + (v^7u^{10} - v^5w^6y)^8 + (w^7u^{10} + w^5v^6y)^8 + (w^7v^{10} - w^5u^6y)^8\\
&\quad - (u^7v^{10} - u^5w^6y)^8 - (u^7w^{10} + u^5v^6y)^8 - (v^7w^{10} - v^5u^6y)^8\\
&\quad - (v^7u^{10} + v^5w^6y)^8 - (w^7u^{10} - w^5v^6y)^8 - (w^7v^{10} + w^5u^6y)^8\\
&= 16(uvw)^6\,(w^{16} - u^{16})(v^{16} - u^{16})(w^{16} - v^{16})\\
&\quad \times (u^{32}v^{32} + u^{32}w^{32} + v^{32}w^{32} + (uvw)^{16}\,(u^{16} + v^{16} + w^{16}))\, x. \qquad (6)
\end{aligned}$$

One can also get non-trivial identities between k-powers by using the following theorem.

THEOREM 4. *In the notation of Theorem* 3, *there exist* $2\,|G|$ *polynomials of degree one in* x *with coefficients in* $\mathbb{Q}\setminus\{0\}$, *namely* $(f_g(x))_{g\in G}$ *and* $(f'_g(x))_{g\in G}$, *such that*

$$\sum_{g\in G} (f_g(x)^{2k-1} - f_g(-x)^{2k-1}) = 0,$$

$$\sum_{g\in G} (f'_g(x)^{2k} - f'_g(-x)^{2k}) = 0.$$

Proof. The proof is essentially the same as the proof of Theorem 3. We just have to make the new choices $(\lambda, \mu) = ((1, 2k-2), ..., (2k-1, 0))$ and $(\lambda, \mu) = ((1, 2k-1), ..., (2k-1, 1))$. ∎

As before, let us make explicit the identities we can get from Proposition 4 and Theorem 4.

(1) For $n = 1$,

$$(x + a) + (-x + b) + (x - a) + (-x - b) = 0, \qquad (1')$$

$$(ax + b)^2 + (bx - a)^2 = (ax - b)^2 + (bx + a)^2. \qquad (2')$$

(2) For $n = 2$,

$$\begin{aligned}
&(a^2x + bd)^3 + (-b^2x + ad)^3 + (-a^2x + bc)^3 + (b^2x + ac)^3\\
&\quad = (-a^2x + bd)^3 + (b^2x + ad)^3 + (a^2x + bc)^3 + (-b^2x + ac)^3, \qquad (3')\\
&(a^3cx + bd^3)^4 + (a^3dx - bc^3)^4 + (b^3cx - ad^3)^4 + (b^3dx + ac^3)^4\\
&\quad = (a^3cx - bd^3)^4 + (a^3dx + bc^3)^4 + (b^3cx + ad^3)^4 + (b^3dx - ac^3)^4. \qquad (4')
\end{aligned}$$

(3) For $n=3$,

$$\begin{aligned}&(a^4x+bc^6)^5+(b^4x+ca^6)^5+(c^4x+ab^6)^5+(-a^4x+cb^6)^5\\&\quad+(-b^4x+ac^6)^5+(-c^4x+ba^6)^5\\&\quad=(-a^4x+bc^6)^5+(-b^4x+ca^6)^5+(-c^4x+ab^6)^5\\&\quad+(a^4x+cb^6)^5+(b^4x+ac^6)^5+(c^4x+ba^6)^5, \qquad (5')\end{aligned}$$

$$\begin{aligned}&(a^6bx+bc^6)^6+(b^6cx+ca^6)^6+(c^6ax+ab^6)^6+(-a^6bx+cb^6)^6\\&\quad+(-b^6ax+ac^6)^6+(-c^6bx+ba^6)^6\\&\quad=(-a^6bx+bc^6)^6+(-b^6cx+ca^6)^6+(-c^6ax+ab^6)^6\\&\quad+(a^6cx+cb^6)^6+(b^6ax+ac^6)^6+(c^6bx+ba^6)^6. \qquad (6')\end{aligned}$$

Remarks. (1) The identity (1′) is trivial. The specialization $x=b/a$ in (2′) gives the well-known parametrization for Pythagorean triples (cf. [6, p. 190])

$$(2ab)^2+(b^2-a^2)^2=(b^2+a^2)^2.$$

(2) The size of these identities seems to grow linearly with k. This behavior follows from the fact that $k_\varepsilon(D_n;\mathbb{Q})=n$ for the lower values of n. We will see in the next section that this does not hold anymore for larger values of k.

6. Optimization Problems

Let n be a positive integer. Let us put $U_n=\{z\in\mathbb{C}: z^n=1\}$ and $\zeta_n=\exp(2i\pi/n)$. We will define the integer $g_n(k)$ to be the smallest cardinality of a group G such that $k_\varepsilon(G;\mathbb{Q})\geqslant k$, for some ε satisfying $\varepsilon(G)=U_n$. Then the number of polynomials in Theorems 3 and 4 will be at least $2g_2(k)$. Since the applications in number theory require short identities, we will try to minimize the $g_n(k)$'s.

Lemma 3. $k_{\varepsilon_1\otimes\varepsilon_2}(G_1\times G_2;K)\geqslant k_{\varepsilon_1}(G_1;K)+k_{\varepsilon_2}(G_2;K)$.

Proof. Let us assume that $k_{\varepsilon_i}(G_i;K)=k_{\varepsilon_i}(V_i;K)=k_i$, for $i=1,2$. If (λ,μ) is any $2(k_1+k_2)$-tuple of scalars, we will consider the vectors $\alpha=\alpha_1\otimes\alpha_2$ and $\beta=\beta_1\otimes\beta_2$ in $V=V_1\otimes V_2$, where α_i and β_i are the vectors in V_i obtained by the k_i-admissibility of G_i with respect to ε_i. Then α and β satisfy to the conditions (i) and (ii), with the choice of elements of $G_1\times G_2$ $(g_1\times 1,\ldots,g_{k_1}\times 1,\ 1\times g'_1,\ldots,1\times g'_{k_2})$. This shows that $k_{\varepsilon_1\otimes\varepsilon_2}(V_1\otimes V_2;K)\geqslant k_1+k_2$ and the lemma is proved. ∎

PROPOSITION 5. *For any $k, n \in \mathbb{N}^*$, we have*:

(1) $g_1(k) = +\infty$,

(2) $g_n(k) < +\infty$ *for* $n \geqslant 2$,

(3) $g_n(k)$ *is a multiple of* n.

Proof. (1) If $n = 1$, the character ε has to be trivial, which is impossible by hypothesis. Thus no group satisfies the conditions defining $g_n(k)$ and then $g_1(k) = +\infty$.

(2) If $n \geqslant 2$, let us consider the cyclic group C_n of order n and the character ε_n defined on C_n by $\varepsilon_n(i) = \zeta_n^i$. Let us prove that $k_{\varepsilon_n}(C_n; \mathbb{Q}) = 1$. Since C_n is abelian, all its irreducible complex representations are one-dimensional. Also, for $g \in C_n$ with $\varepsilon_n(g) \neq 1$, we have codim Fix $g = 1$ and, by Theorem 2, $k'_{\varepsilon_n}(C_n; \mathbb{C}) < 2$. Using Propositions 1 and 3 we get

$$k_{\varepsilon_n}(C_n; \mathbb{Q}) \leqslant \bar{k}_{\varepsilon_n}(C_n; \mathbb{Q}) = \bar{k}_{\varepsilon_n}(C_n; \mathbb{C}) = k'_{\varepsilon_n}(C_n; \mathbb{C}) \leqslant 1.$$

Let us consider now any one-dimensional representation V of C_n. Let us define (α, β) to be $(-\mu, \lambda)$ if $(\lambda, \mu) \neq (0, 0)$ and $(1, 0)$ if $(\lambda, \mu) = (0, 0)$. Then (α, β) satisfies the requirements of 1-admissibility, which shows that $k_{\varepsilon_n}(C_n; \mathbb{Q}) = 1$. Then we just have to apply Lemma 3 to get $k_{\varepsilon_n}(C_n^k; \mathbb{Q}) \geqslant k$ and the assertion follows.

(3) If $\varepsilon(G) = U_n$, there exists an element in G of order n and thus $|G|$ is a multiple of n. Then the definition of $g_n(k)$ implies the desired result. ▌

Remarks. (1) In the definition of $g_n(k)$, the condition $\varepsilon(G) = U_n$ can be replaced by the more convenient condition $\varepsilon(G) \subseteq U_n$ to define a new function $g'_n(k)$. Since $\varepsilon(G) = U_d$ for some positive integer d dividing n, we have the formula

$$g'_n(k) = \min_{d \mid n} g_d(k).$$

This implies that $g'_n(k) = g_n(k)$ when n is a prime.

(2) The preceding proofs show that $g'_n(k) \leqslant |C_n^k| = n^k$. This upper bound is fairly weak and we will try to improve it. However, when $k = 1$, it gives the exact formula $g_n(1) = n$, due to Proposition 5(3). Using the first remark leads us to $g'_n(1) = \min\{p \text{ prime: } p \text{ divides } n\}$.

Let us study the case $n = 2$. We will then have $g_2(k) = g'_2(k)$ by Remark 1 and $g_2(k)$ even by Proposition 5.

THEOREM 5. (1) $g_2(1) = 2$, $g_2(2) = 4$, $g_2(3) = 6$, $g_2(4) = 12$.

(2) $g_2(3k + r) \leqslant 2^r 6^k$.

Proof. (1) The first equality is a special case of the general formula $g_n(1)=n$ for $n\geqslant 2$. Applying Lemma 3 gives $g_2(2)\leqslant 2^2=4$. Thus $g_2(2)\in\{2, 4\}$. The only group of order 2 is S_2, with only one non-trivial character ε, for which $k_2(S_2; \mathbb{Q})=1$ by Proposition 4. This shows that $g_2(2)=4$.

Applying again Proposition 4 gives us the upper bound $g_2(3)\leqslant 6$ and thus $g(3)\in\{4, 6\}$. When $|G|=4$, there are at most two elements in G whose character value is -1; since the g_i's occurring in the definition of the k-admissibility are distinct we will have $k_\varepsilon(G)\leqslant 2$ for any $\{-1, +1\}$-valued character ε defined on G. This shows that $g_2(3)=6$. Using Lemma 3 and the same arguments as before, we have $g_2(4)\in\{8, 10, 12\}$. Moreover we have the inequality

$$k_\varepsilon(D_n; \mathbb{Q})\leqslant \bar{k}_\varepsilon(D_n; \mathbb{Q})=3,$$

for $n\in\{4, 5\}$ and for any character ε on D_n, by a proof similar to that of Proposition 4. Computing also the $k'_\varepsilon(G)$ for any $G\in\{C_8, C_2\times C_4, C_2\times C_2\times C_2, H_4, C_{10}\}$ and for any character $\varepsilon\colon G\to\{-1, +1\}$ shows that $g_2(4)=12$.

(2) Using Lemma 3 and Proposition 4 we get

$$k_{\varepsilon_1^k\otimes\varepsilon_2^r}(S_3^k\times S_2^r; \mathbb{Q})\geqslant 3k+r.$$

Since $|S_3^k\times S_2^r|=2^r6^k$, the second part of the theorem follows. ∎

The upper bound given in (2) is fairly weak and should be easily improved for larger values of k. It would also be interesting to get lower bounds for $g_n(k)$.

7. Applications to the Easier Waring's Problem over Algebras of Zero Characteristic

Let $\mathscr{A}$ be an algebra of zero characteristic. For $k\in\mathbb{N}^*$ one defines [12, 13] the function $v_k(\mathscr{A})$ to be the least integer s for which the equation $x=\pm x_1^k\pm\cdots\pm x_s^k$ has always a solution $(x_1, ..., x_s)$ for any x in $\mathscr{A}$. When $\mathscr{A}=\mathbb{Q}$, the function $v_k(\mathbb{Q})$ coincides with the function $\rho(k)$ introduced by Chowla and Cowles [2].

Vaserstein [13] uses solutions to the Tarry–Escott problem to bound $v_k(\mathscr{A})$. If there exists rational integers $(a_1, ..., a_s, b_1, ..., b_s)$ such that

$$\sum_{i=1}^{s} a_i^h=\sum_{i=1}^{s} b_i^h \quad \text{for} \quad 0\leqslant h\leqslant k-2 \quad \text{and} \quad \sum_{i=1}^{s} a_i^{k-1}\neq\sum_{i=1}^{s} b_i^{k-1}, \qquad \text{(T)}$$

we have an identity defined for any x in $\mathscr{A}$

$$\sum_{i=1}^{s} ((x+a_i)^k - (x+b_i)^k) = cx + d, \qquad \text{with} \quad c \neq 0.$$

Replacing x by $x/c - d$ will show that $v_k(\mathscr{A}) \leqslant 2s$. Wright [14] has defined $T(k)$ as the smallest number s such that (T) has a solution. Bastien [1] proved that $T(k) \geqslant k-1$ and one conjectures that the equality holds. The best upper bound has been found by Hua [7] and behaves as $k^2 \log k$ when k goes to infinity.

We can use Theorem 3 to sharpen some of these upper bounds for $v_k(\mathscr{A})$. Indeed if C and C' are non-zero, we will get the inequality $v_k(\mathscr{A}) \leqslant 2\,|G|$. Thus we have almost surely the upper bound $v_{2k+i}(\mathscr{A}) \leqslant 2g_2(k)$, for $i = 1, 2$. For instance the identities (1)–(6) lead to the upper bounds $v_3(\mathscr{A}) \leqslant 4$, $v_4(\mathscr{A}) \leqslant 4$, $v_5(\mathscr{A}) \leqslant 8$, $v_6(\mathscr{A}) \leqslant 8$, $v_7(\mathscr{A}) \leqslant 12$, $v_8(\mathscr{A}) \leqslant 12$. This improves the upper bounds given by the Tarry–Escott approach when $k \in \{4, 6, 8\}$. This was already noticed by Vaserstein [13] for $k = 6$ (Rao's identity) and $k = 8$ (Vaserstein's identity).

The identities we used involve a large number of parameters. However, some specializations may improve the theoretical upper bound $2g_2(k)$. For instance we can get this way $v_{10}(\mathscr{A}) \leqslant 20 < 24 = 2g_2(4)$. Indeed the equation associated to $S_2 \times S_3$ by Lemma 3 and Proposition 4 is

$$F(a, b, u, v, w; x) - F(a, b, u, v, w; -x) = C(a, b, u, v, w)\, x,$$

where

$$\begin{aligned} F(a, b, u, v, w; x) = {} & (av^3w^{21} + bu^9v^2x)^{10} + (aw^3u^{21} + bv^9w^2x)^{10} \\ & + (au^3v^{21} + bw^9u^2x)^{10} + (bv^3w^{21} - au^9v^2x)^{10} \\ & + (bw^3u^{21} - av^9w^2x)^{10} + (bu^3v^{21} - aw^9u^2x)^{10} \\ & + (aw^3v^{21} - bu^9w^2x)^{10} + (au^3w^{21} - bv^9u^2x)^{10} \\ & + (av^3u^{21} - bw^9v^2x)^{10} + (bw^3v^{21} + au^9w^2x)^{10} \\ & + (bu^3w^{21} + av^9u^2x)^{10} + (bv^3u^{21} + aw^9v^2x)^{10} \end{aligned}$$

and

$$\begin{aligned} C(a, b, u, v, w) = {} & 20ab(uvw)^9\,(a^8 - b^8) \\ & \times (v^{20}w^{180} + w^{20}u^{180} + u^{20}v^{180} - v^{20}u^{180} - w^{20}v^{180} - u^{20}w^{180}). \end{aligned}$$

If we want to have $av^3w^{21}+bu^9v^2x=bw^3u^{21}+av^9w^2x$, we have to choose $w=vt^3$, $u=vt^4$, $a=bt^{30}$, for some t. Setting $b=v=1$, factorizing out t^{90}, and replacing x by xt^3 leads to

$$G(t;x)-G(t;-x)=C'(t)\,x,$$

where

$$\begin{aligned}G(t;x)=(t^{114}+x)^{10}&+(t^{33}+t^{29}x)^{10}+(t^{54}-t^{60}x)^{10}+(t^3-t^{59}x)^{10}\\&+(t^{30}-t^{36}x)^{10}+(t^{96}-t^2x)^{10}+(t^{105}-t^{21}x)^{10}\\&+(1+t^{66}x)^{10}+(t^{66}+t^{32}x)^{10}+(t^{75}+t^{51}x)^{10}\end{aligned}$$

and

$$C'(t)=20t^{66}(t^{240}-1)(t^{180}-1)(t^{160}-1)(t^{380}+t^{200}+t^{20}-1-t^{160}-t^{320}).$$

In this case, the upper bound $v_{10}(\mathscr{A})\leqslant 20$ is weaker than the upper bound 18 provided by solutions to the Tarry–Escott problem. However, we believe it can be useful to try to simplify general identities by specializing the parameters.

8. Applications to the Easier Waring's Problem over $\mathbb{Z}$

Let us put $v(k)=v_k(\mathbb{Z})$. The only known values of the function $v(k)$ are $v(1)=1$ and $v(2)=3$ (cf. [6, p. 327]) and $v(4)\in\{9,10\}$ [8]. Updated bounds may be found in [13] for larger values of k. The best general upper bound is furnished by the trivial inequality $v(k)\leqslant G(k)+1$ and asymptotic estimates of $G(k)$. However, when k is small, the elementary method given by Fuchs and Wright [5] gives the best results. This method consists of finding an identity of the form $Cx=\Sigma\pm f_i(x)^k$ to reduce the problem modulo C; then we just have to apply the results in [4] to find an upper bound for $v(k)$. For instance (cf. [6, p. 327]), we have the identities $6x=(x+1)^3+(x-1)^3-2x^3$ and $6x+3=x^3-(x-4)^3+(2x-5)^3-(2x-4)^3$ and we know that, modulo 3, any residue class is a cube; thus $v(3)\leqslant 4+1=5$.

Applying this method with identities (1)–(6) leads to the following upper bounds:

$$v(3)\leqslant 8,\quad v(4)\leqslant 12,\quad v(5)\leqslant 13,\quad v(6)\leqslant 14,\quad v(7)\leqslant 16,\quad v(8)\leqslant 28.$$

The identity involving $G(t;x)$ at the end of Section 7 also gives $v(10)\leqslant 32$. The best upper bounds found so far for $v(k)$, $k=3$, 4, 5, 6, 7, 8, 10 are 5, 10, 10, 14, 14, 28, 30, respectively. The only cases where this approach gives better results than the Tarry–Escott problem are $k=6$ (due to Rao's identity) and $k=8$ (due to Vaserstein's identity). We believe also that the asymptotic bound for $\nu(k)$ cannot be improved this way. It is interesting to note that, in some sense, Rao and Vaserstein's identities were the only identities that can apply usefully to the easier Waring problem over $\mathbb{Z}$.

9. The Function $\theta(k)$

Chowla and Cowles [2] defined the function $\theta(k)$ to be the least integer s for which the equation $\pm x_1^k \pm \cdots \pm x_s^k = 0$ has a non-trivial solution. They showed that $\theta(k) \leqslant 2k$, by proving the existence of a non-trivial solution to the equation $x_1^k + \cdots + x_k^k = y_1^k + \cdots + y_k^k$. They also improved this general upper bound when $k = 9$ by proving that $\theta(9) \leqslant 17$. Fermat's last theorem would imply that $\theta(k) > 3$ for $k \geqslant 3$. Euler conjectured that the equation $y^k = x_1^k + \cdots + x_k^k$ always has a non-trivial solution over the integers. Euler's conjecture would imply that $\theta(k) \leqslant k+1$. However, even the case $k = 6$ is still not proved; on the other hand better results are known when $k = 4, 5$. Elkies [4] found solutions to the equation $A^4 + B^4 + C^4 = D^4$ and Frye found the smallest solution $(A, B, C, D) = (95800, 217519, 414560, 422481)$; this shows that $\theta(4) = 4$. Lander and Parkin [9] found the identity $27^5 + 84^5 + 110^5 + 133^5 = 144^5$, which implies that $\theta(5) \in \{4, 5\}$.

The method used by Chowla and Cowles to prove $\theta(9) \leqslant 17$ consists in finding an identity of the form $Cx = \Sigma \pm f_i(x)^k$, in which they put $x = C^{k-1}y^k$. When we apply this method with the identities (1)–(6), we find some new formulas such as

$$(6(a^2-b^2))^3 = (36(a^2-b^2)^2+a)^3 + (36(a^2-b^2)^2-a)^3 + (-36(a^2-b^2)^2+b)^3 + (-36(a^2-b^2)^2-b)^3.$$

From this we deduce that

$$\theta(3) \leqslant 5, \quad \theta(4) \leqslant 5, \quad \theta(5) \leqslant 9, \quad \theta(6) \leqslant 9, \quad \theta(7) \leqslant 13, \quad \theta(8) \leqslant 13.$$

The last three results improve the previous bounds quoted. Let us remark that solutions to the Tarry–Escott problem would lead to the inequality $\theta(k) \leqslant 2k-1$; in particular the bounds $\theta(6) \leqslant 9$ and $\theta(8) \leqslant 13$ cannot be reached.

Another method consists in considering identities of the form $0 = \Sigma \pm f_i(x)^k$ and taking x to be a zero of some $f_i(x)$. For instance, putting $x = bd/a^2$ in (3′) gives

$$(2a^2bd)^3 + (-b^3d+a^3d)^3 + (-a^2bd+a^2bc)^3 + (b^3d+a^3c)^3 = (b^3d+a^3d)^3 + (a^2bd+a^2bc)^3 + (-b^3d+a^3c)^3.$$

From (2′)–(5′) we deduce that

$$\theta(2)\leqslant 3, \quad \theta(3)\leqslant 7, \quad \theta(4)\leqslant 7, \quad \theta(5)\leqslant 11, \quad \theta(6)\leqslant 11.$$

These bounds are weaker than the ones we obtained first. This is due to the fact that $g_2(k+1)>g_2(k)+1$, for the values of k we considered.

10. Problems and Possible Extensions

In Section 3, we conjectured that $k_\varepsilon(V;K)=\bar{k}_\varepsilon(V;K)$. If this is true, it would make $k_\varepsilon(G;K)$ much easier to compute, using Theorem 2 and character tables. An exact formula for $k_\varepsilon(G;\mathbb{Q})$ would be of special interest.

More specifically, one could try to calculate $k_\varepsilon(G;\mathbb{Q})$ for special cases. For instance one could try to generalize Proposition 4 to any Coxeter group, the character ε being the signature.

Section 6 provides only partial results on the function $g_n(k)$. It would be interesting to investigate the asymptotic behavior of this function for large k.

All the applications to number theory we gave in Sections 7, 8, and 9 are consequences of the case $\varepsilon(G)\subset\{-1,+1\}$, i.e., $n=2$. Larger values of n would also give significant results in other rings than $\mathbb{Z}$. For instance the case $n=4$ would provide information about the ring of Gaussian integers.

One can also try to generalize the k-admissibility notion in the following way. First consider the scalars $(\lambda_1, ..., \lambda_k, \mu_1, ..., \mu_k)$ as the coefficients of a $k\times 2$ matrix. Then one can define a notion of (k, l)-admissibility by considering any $k\times l$ matrix. It would imply the existence of l vectors $\alpha_1, ..., \alpha_l$ such that:

(i) $\lambda_{i1}\alpha_1+\cdots+\lambda_{il}\alpha_l\in \operatorname{Fix} g_i$ for some g_i with $\varepsilon(g_i)\neq 1$;

(ii) For any $g\in G$, $\{\alpha_1, ..., \alpha_l\}\subset \operatorname{Fix} g \Rightarrow \varepsilon(g)=1$.

Most of the propositions and theorems given here would extend. It would also imply number-theoretic identities by using the l-multinomial theorem instead of the binomial theorem. However, the size of these identities would grow too fast to be useful. One could recover at most some of the results obtained in the $l=2$ case. For instance we can obtain the identity

$$\begin{aligned}(6a^2x^2+6ab^5x-b^{10})^3&+(-6a^2x^2+6ab^5x+b^{10})^3\\&+(-6b^2x^2+6ba^5x+a^{10})^3+((6b^2x^2-6ba^5x-a^{10})^3\\&=72ab(b^{24}-a^{24})\,x,\end{aligned}$$

and get again the inequality $\theta(3)\leqslant 5$.

By duality one can also define a k-admissibility notion for compact groups. In this case we obtain identities involving integrals over the group with respect to the Haar measure (instead of sums over the finite groups). These identities are proven the same way by using Fubini's theorem.

References

1. L. Bastien, Sphinx-Oedipe, **8** (1913), 171–172.
2. S. Chowla and M. Cowles, Remarks on equations related to Fermat's last theorem, *in* "Number Theory Related to Fermat's Last Theorem," pp. 255–261, Proceedings of the Conference Sponsored by the Vaughn Foundation (Neal Koblitz, Ed.), Progress in Mathematics, Vol. 26, Birkhäuser, Boston/Basel/Stuttgart, 1982.
3. Dickson, "History of the Theory of Numbers," Vol. 2, p. 729.
4. N. D. Elkies, On $A^4+B^4+C^4=D^4$, *Math. Comp.* **51** *(1988)*, 825–835.
5. W. H. Fuchs and E. M. Wright, The "easier" Waring problem, *Quart. J. Math. Oxford* **10** (1939), 190–209.
6. G. H. Hardy and E. M. Wright, "An introduction to the Theory of Numbers," 5th ed., Oxford Univ. Press, London/New York.
7. Loo-Keng Hua, On Tarry's problem, *Quart. J. Math. Oxford* **9** (1938), 315–320.
8. W. Hunter, The representation of numbers by sums of fourth powers, *J. London Math. Soc.* **16** (1941), 177–179.
9. C. J. Lander and T. R. Parkin. A counterexample to Euler's sum of powers conjecture, *Math. Comp.* **21** (1967), 101–103.
10. J. P. Serre, "Linear Representations of Finite Groups," Graduate Texts in Mathematics, Vol. 42, Springer-Verlag, New York/Heidelberg/Berlin.
11. L. N. Vaserstein, Every integer is a sum or difference of 28 integral eight powers, *J. Number Theory* **28** (1988), 66–68.
12. L. N. Vaserstein, Waring's problem for commutative rings, *J. Number Theory* **26** (1987), 299–307.
13. L. N. Vaserstein, Waring's problem for algebras over fields, *J. Number Theory* **26** (1987), 286–298.
14. E. M. Wright, The Tarry–Escott and the "easier" Waring problem, *J. Reine Angew. Math.* **311/312** (1979), 170–173.