Théorie des Groupes/*Group Theory*

Arithmetical properties of idempotents in group algebras

Max NEUNHÖFFER

Lehrstuhl D für Mathematik, Templergraben 64, 52062 Aachen, Allemagne
E-mail: max.neunhoeffer@math.rwth-aachen.de

Abstract. We consider a finite group G and a Dedekind ring A of characteristic 0. Let $\mathfrak{p}\neq 0$ be a prime ideal of A. Then the localization $A_\mathfrak{p}$ of A at $\mathfrak{p}$ is a discrete valuation ring. The idempotents in the group algebra $A_\mathfrak{p}G$ play a fundamental rôle in the study of projective modules for G. In this Note we show that for every idempotent $\tilde{e}\in A_\mathfrak{p}G$ there is an idempotent e and a positive integer $n\in\mathbf{N}^*$, such that $A_\mathfrak{p}Ge=A_\mathfrak{p}G\tilde{e}$ and $|G|^n e\in AG$.

Propriétés arithmétiques d'idempotents d'algèbres de groupes

Résumé. Soit G un groupe fini, A un anneau de Dedekind de caractéristique 0, et $\mathfrak{p}\neq 0$ un idéal premier de A. Alors la localisation $A_\mathfrak{p}$ est un anneau de valuation discrète. Les idempotents dans l'algèbre du groupe $A_\mathfrak{p}G$ jouent un rôle fondamental dans l'étude des modules projectifs pour G. Dans cette note, nous démontrons que pour chaque idempotent $\tilde{e}\in A_\mathfrak{p}G$ il existe un idempotent e et un $n\in\mathbf{N}^*$ tel que $A_\mathfrak{p}Ge=A_\mathfrak{p}G\tilde{e}$ et $|G|^n e\in AG$.

Version française abrégée

Soit G un groupe fini, A un anneau de Dedekind de caractéristique 0, et K son corps des fractions. On se fixe un idéal premier $\mathfrak{p}\neq 0$ de A. Alors la localisation $A_\mathfrak{p}$ est un anneau de valuation discrète, dont le corps résiduel est de caractéristique $p>0$. On considère la partie

$$T := A \setminus \Big(\mathfrak{p} \cup \bigcup_{\mathfrak{q}} \mathfrak{q}\Big)$$

de A, où $\mathfrak{q}$ parcourt l'ensemble de tous les idéaux premiers de A tels $|G|\notin\mathfrak{q}$. L'ensemble T est clos par multiplication et on peut donc définir l'anneau des quotients $R := T^{-1}A \subseteq K$.

Remarque 1. – Tout élément de R est de la form a/d avec $a\in A$ et $d\in\mathbf{N}^*$, où d n'est divisible que par des nombres premiers qui divisent l'ordre du groupe G. Autrement dit, pour tout $x\in R$ il existe un $n\in\mathbf{N}^*$ tel que $|G|^n x\in A$, où $|G|$ désigne l'ordre du groupe G.

Remarque 2. – On a $A\subseteq R\subseteq A_\mathfrak{p}\subseteq K$, et $A_\mathfrak{p}$ est aussi la localisation de R dans l'idéal premier de R engendré par $\mathfrak{p}$.

Les résultats principaux de cette Note sont des conséquences du théorème suivant. Remarqons d'abord qu'un R-module de type fini qui est sans torsion est toujours projectif. C'est une conséquence du fait que R — comme localisation d'un anneau de Dedekind — est aussi un anneau de Dedekind (*voir* [2], Theorem 10.4).

preprint, 26 octobre 1999, revised 21 janvier 2000

Théorème 1. – *Soit M un RG-module de type fini qui est projectif comme R-module. Alors M est indécomposable si et seulement si le $A_\mathfrak{p}G$-module $M_\mathfrak{p} := A_\mathfrak{p} \otimes_R M$ est indécomposable.*

En effet, si M est décomposable, alors il est clair que $M_\mathfrak{p}$ est aussi décomposable. Supposons maintenant que $M_\mathfrak{p}$ est décomposable : cela implique qu'il existe une suite exacte

$$(*) \qquad\qquad 0 \to M_1 \to M \to M_2 \to 0,$$

où $M_1 \neq 0$ et $M_2 \neq 0$ sont des RG-modules de type fini et sans torsion, tels que la suite exacte

$$0 \to A_\mathfrak{p} \otimes_R M_1 \to A_\mathfrak{p} \otimes_R M \to A_\mathfrak{p} \otimes_R M_2 \to 0$$

est scindée. Afin de montrer que $(*)$ est aussi scindée, on utilise le principe du "passage du local au global" : la suite $(*)$ est scindée si et seulement si, pour tout idéal premier $\mathfrak{q}$ de R, la suite

$$(**) \qquad\qquad 0 \to R_\mathfrak{q} \otimes_R M_1 \to R_\mathfrak{q} \otimes_R M \to R_\mathfrak{q} \otimes_R M_2 \to 0$$

est scindée. Une version généralisée du théoreme de Maschke (*voir* [1], (25.12)) montre qu'il suffit de considérer les idéaux premiers $\mathfrak{q} \subset R$ tels que $|G| \in \mathfrak{q}$. Or, par la construction de R (*voir* remarque 1), il y a au plus un idéal premier de R qui contient $|G|$: c'est l'idéal engendré par $\mathfrak{p}$. Dans ce cas-là, la suite $(**)$ est scindée par hypothèse, ce qui démontre le théorème 1.

En appliquant le théorème 1 aux modules de la forme RGe, où $e \in RG$ est un idempotent, on obtient le corollaire suivant :

Corollaire. – *Un idempotent $e \in RG$ est primitif si et seulement si e est primitif vu comme idempotent dans $A_\mathfrak{p}G$. De plus, pour tout idempotent $\tilde{e} \in A_\mathfrak{p}G$ il existe un idempotent $e \in RG$ et un $n \in \mathbf{N}^*$ tel que $A_\mathfrak{p}G\tilde{e} = A_\mathfrak{p}Ge$ et $|G|^n e \in AG$.*

En particulier, si on a $1 = e_1 + \cdots + e_r$ oú $e_1, \ldots, e_r$ sont des idempotents primitifs dans RG qui sont deux á deux orthogonaux, alors la même chose est vraie dans $A_\mathfrak{p}G$.

Les idempotents jouent un rôle fondamental dans l'étude des modules projectifs de $\hat{A}_\mathfrak{p}G$, où $\hat{A}_\mathfrak{p}$ est la complétion de $A_\mathfrak{p}$: tout $\hat{A}_\mathfrak{p}G$-module projectif et indécomposable est isomorphe à un module de la forme $\hat{A}_\mathfrak{p}G\hat{e}$, où $\hat{e} \in \hat{A}_\mathfrak{p}G$ est un idempotent primitif (*voir* [1], (6.17)).

Proposition. – *Supposons K assez gros pour que KG soit deployée. Alors tout $\hat{A}_\mathfrak{p}G$-module projectif et indécomposable est isomorphe à un module de la forme $\hat{A}_\mathfrak{p}Ge$, où e est un idempotent tel que $|G|^n e \in AG$ pour un $n \in \mathbf{N}^*$.*

En effet, soit k le corps résiduel de $\hat{A}_\mathfrak{p}$. Comme KG est deployé, tout idempotent de kG peut être relevé pas seulement à un idempotent dans $\hat{A}_\mathfrak{p}G$ mais à un idempotent dans $A_\mathfrak{p}G$ (*voir* [1], Ex. 6.16). Donc, tout $\hat{A}_\mathfrak{p}G$-module projectif et indécomposable est isomorphe à un module de la forme $\hat{A}_\mathfrak{p}G\tilde{e}$, où $\tilde{e} \in A_\mathfrak{p}G$ est un idempotent primitif. Il reste à utiliser le corollaire et la remarque 1.

1. Introduction

Idempotents in the group algebra of a finite group G over a ring of p-adic integers play a fundamental rôle in the study of modular representations of G. In this Note we are concerned with the problem of obtaining arithmetical conditions on the coefficients of such an idempotent when expressed as a linear combination of group elements. Our main results are statements about the denominators in these coefficients: each equivalence class of idempotents (under conjugation in the group algebra) always contains a representative in which the only prime divisors of the denominators are primes which divide the order of G. This is established as a consequence of a more general result about the behaviour of indecomposable RG-lattices under scalar extension from R to a ring of p-adic integers, where R is a certain non-local ring. The proof uses a local-global principle and some properties of Dedekind rings and maximal orders. The results about idempotents in group algebras over Dedekind domains answer a question of Meinolf Geck (posed in the problem book in Oberwolfach in 1992) positively.

2. The Main Theorem

Let G be a finite group, A a Dedekind ring of characteristic 0, and K its field of fractions. We fix a non-zero prime ideal $\mathfrak{p}$ of A. Since A is Dedekind, the localization $A_\mathfrak{p}$ is a discrete valuation ring, with residue field of characteristic $p > 0$, say. We consider the following subset of A:

$$T := A \setminus \Big(\mathfrak{p} \cup \bigcup_{\mathfrak{q}} \mathfrak{q}\Big),$$

where $\mathfrak{q}$ runs over all prime ideals of A such that $|G| \notin \mathfrak{q}$. The set T is multiplicatively closed and so we can form the ring of quotients $R := T^{-1}A \subseteq K$.

Remark 1. – Every element of R is of the form a/d with $a \in A$ and $d \in \mathbf{N}^*$, where d is only divisible by prime numbers which divide the order of G. In other words, for each $x \in R$ there exists an $n \in \mathbf{N}^*$ such that $|G|^n x \in A$, where $|G|$ denotes the order of G.

This is seen as follows: by definition, every element of R is of the form a/t with $a \in A$ and $t \in T$. Since A is Dedekind, the principal ideal $|G|A$ can be written in an essentially unique way as a product of prime ideals $\mathfrak{p}_j$ in A:

$$|G|A = \mathfrak{p}_1^{i_1} \cdot \dots \cdot \mathfrak{p}_m^{i_m} \quad (i_k > 0 \text{ for } 1 \le k \le m).$$

We now conclude from the construction of T that the principal ideal tA decomposes into a product of prime ideals, such that only prime ideals dividing $|G|$ occur, so renumbering yields for some $l \le m$:

$$tA = \mathfrak{p}_1^{j_1} \cdot \dots \cdot \mathfrak{p}_l^{j_l} \quad (j_k > 0 \text{ for } 1 \le k \le l).$$

This means that there is some exponent $n > 0$ such that $|G|^n A \subseteq tA$. But then $|G|^n \in tA$ and so there is a $g \in A$ with $|G|^n = tg$. Hence we have $a/t = (ag)/(|G|^n)$. □

Remark 2. – We have $A \subseteq R \subseteq A_\mathfrak{p} \subseteq K$, and $A_\mathfrak{p}$ is also the localization of R at the prime ideal of R generated by $\mathfrak{p}$.

Note that R as ring of quotients of a Dedekind ring is also Dedekind (see for example Theorem 10.4(1) in [2]). Therefore a finitely generated R-module M is projective if and only if it is torsion free. An RG-lattice is a finitely generated R-projective RG-module.

THEOREM 1. – *An RG-lattice M is indecomposable if and only if the $A_\mathfrak{p}G$-lattice $M_\mathfrak{p} := A_\mathfrak{p} \otimes_R M$ obtained by localization at $\mathfrak{p}$ is indecomposable.*

Proof:
"$\Longleftarrow$" is clear: From $M = M' \oplus M''$ as RG-lattices, it follows, that $M_\mathfrak{p} = M'_\mathfrak{p} \oplus M''_\mathfrak{p}$, because localization preserves direct sums.
"$\Longrightarrow$": for this direction we have to show that if $M_\mathfrak{p}$ is decomposable, also M itself is decomposable. More explicitly: If $M_\mathfrak{p} = \tilde{M}' \oplus \tilde{M}''$ with two non-trivial $A_\mathfrak{p}G$-submodules $\tilde{M}'$ and $\tilde{M}''$, then M is a direct sum of two proper submodules.

So let $M_{\mathfrak{p}} = \tilde{M}' \oplus \tilde{M}''$. Because M is R-torsion free as RG-lattice, the map

$$M \hookrightarrow M_{\mathfrak{p}}, \qquad m \mapsto m/1$$

is an embedding. Invoking Proposition (23.12) in [1] we get an RG-submodule M' of M with $M' = M \cap \tilde{M}'$ and $\tilde{M}' = M'_{\mathfrak{p}}$. We consider the following short exact sequence of RG-lattices (note that M/M' is R-torsion free because $M_{\mathfrak{p}}/\tilde{M}'_{\mathfrak{p}}$ is $A_{\mathfrak{p}}$-torsion free and M' is the intersection of $\tilde{M}'$ and M):

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M/M' \longrightarrow 0 \qquad (*)$$

and its localization at $\mathfrak{p}$:

$$0 \longrightarrow \tilde{M}' \longrightarrow M_{\mathfrak{p}} \longrightarrow (M/M')_{\mathfrak{p}} \longrightarrow 0$$

As $\tilde{M}'$ is, by hypothesis, a direct summand of $M_{\mathfrak{p}}$, the latter sequence splits.

We now use Proposition (4.2.iii) in [1] which states, that $(*)$ splits if and only if all its localizations at prime ideals of R split. A generalized version of Maschke's theorem (*see* [1], (25.12)) shows that we have $|G| \cdot \mathrm{Ext}^1_{R_{\mathfrak{q}}G}((M/M')_{\mathfrak{q}}, M'_{\mathfrak{q}}) = 0$ for all prime ideals $\mathfrak{q}$ of R. Thus, we only need to consider those prime ideals $\mathfrak{q}$ such that $|G| \in \mathfrak{q}$. But, by the construction of R (cf. Remark 1), there is at most one such prime ideal of R, namely, the prime ideal generated by $\mathfrak{p}$. In this case, the localization of $(*)$ splits by assumption. So $(*)$ is split and the theorem is proved. □

3. Application to idempotents

We use the same notations as in the last section. An idempotent e in the group algebra RG generates a left ideal RGe which is, as a left RG-module, a direct summand of the left regular RG-module and therefore RG-projective. Being also R-projective, it is an RG-lattice. Conversely, every direct summand of the left regular RG-module is generated by an idempotent. So a direct summand of RG is indecomposable if and only if the corresponding idempotent is primitive. Thus we have the following corollary:

Corollary 1. – *An idempotent $e \in RG$ is primitive if and only if it is primitive as idempotent in $A_{\mathfrak{p}}G$.*

But the situation is even better: If $\tilde{e}$ is an idempotent in $A_{\mathfrak{p}}G$ we can apply the same kind of argument as in the proof of Theorem 1 to the left regular $A_{\mathfrak{p}}$-module $\tilde{M} := A_{\mathfrak{p}}G$. That module is the localization of the left regular RG-module $M := RG$ and it has a direct summand $\tilde{M}' := A_{\mathfrak{p}}G\tilde{e}$. Again by using Proposition (23.12) in [1], we get a submodule M' of RG with $M' = M \cap \tilde{M}' = RG \cap A_{\mathfrak{p}}G\tilde{e}$ and $A_{\mathfrak{p}}G\tilde{e} = M'_{\mathfrak{p}}$. The exact sequence $0 \longrightarrow M' \longrightarrow M \longrightarrow M/M' \longrightarrow 0$ splits by the same argument as in the theorem, showing that M' is a direct summand of $M = RG$. So there must be an idempotent $e \in RG$ such that $RGe = M'$. Because $M' = RG \cap A_{\mathfrak{p}}G\tilde{e}$, we have $e \in A_{\mathfrak{p}}G\tilde{e}$ and therefore $M' = A_{\mathfrak{p}}Ge$. Invoking Remark 1 we conclude that there is a natural number n such that $|G|^n e \in AG$. We have thus proved:

Corollary 2. – *Let $\tilde{e}$ be an idempotent in $A_{\mathfrak{p}}G$. Then there is an idempotent e in RG and a natural number n such that $A_{\mathfrak{p}}G\tilde{e} = A_{\mathfrak{p}}Ge$ and $|G|^n e \in AG$.*

In particular, if we consider a decomposition of 1 into a sum of pairwise orthogonal primitive idempotents $1 = e_1 + \cdots + e_r$ in RG (existence is clear because R is noetherian), we conclude from Corollary 1 that this is also a decomposition of 1 into pairwise orthogonal primitive idempotents for $A_{\mathfrak{p}}G$.

Idempotents play a fundamental rôle in the study of projective $\hat{A}_{\mathfrak{p}}G$-modules, where $\hat{A}_{\mathfrak{p}}$ denotes the completion of $A_{\mathfrak{p}}$. Indeed, every projective indecomposable $\hat{A}_{\mathfrak{p}}G$-module is isomorphic to a module of the form $\hat{A}_{\mathfrak{p}}G\hat{e}$, where $\hat{e} \in \hat{A}_{\mathfrak{p}}G$ is a primitive idempotent (*see* [1], (6.17)).

Proposition. – *Assume that K is a splitting field for G and let $\hat{A}_{\mathfrak{p}}$ be the completion of $A_{\mathfrak{p}}$. Then every projective indecomposable $\hat{A}_{\mathfrak{p}}G$-module is isomorphic to a module of the form $\hat{A}_{\mathfrak{p}}Ge$, where e is an idempotent such that $|G|^n e \in AG$ for some $n \in \mathbf{N}^*$.*

Indeed, let k be the residue field of $\hat{A}_{\mathfrak{p}}$. Since KG is split semisimple, we can lift idempotents from kG to $A_{\mathfrak{p}}G$ (*see* [1], Ex. 6.16). So every projective indecomposable $\hat{A}_{\mathfrak{p}}G$-module is isomorphic to a module of the form $\hat{A}_{\mathfrak{p}}G\tilde{e}$, where $\tilde{e} \in A_{\mathfrak{p}}G$ is a primitive idempotent. It remains to use Corollary 2 and Remark 1.

Acknowledgements. I thank Meinolf Geck for his excellent suggestions which helped to improve the exposition of this note.

References

[1] Curtis, Charles W., Reiner, Irving, Methods of Representation Theory, volume I, John Wiley & Sons, New York, Chichester, Brisbane, Toronto, Singapore, 1981.
[2] Jacobson, Nathan, Basic Algebra, volume II, W. H. Freeman and Company, New York, 1989.