Multiplicative Jordan Decomposition in Integral Group Rings

D. S. Passman

University of Wisconsin–Madison

Brussels Conference
June 2017
Jordan Decomposition

Let $\mathbb{Q}[G]$ be the rational group algebra of the finite group $G$. Since $\mathbb{Q}$ is a perfect field, every element $x$ of $\mathbb{Q}[G]$ has a unique additive Jordan decomposition $x = x_s + x_n$, where $x_s$ is semisimple and where $x_n$ commutes with $x_s$ and is nilpotent. If $x$ is a unit, then $x_s$ is also invertible and $x = x_s(1 + x_s^{-1}x_n)$ is a product of a semisimple unit $x_s$ and a commuting unipotent unit $x_u = 1 + x_s^{-1}x_n$. This is the unique multiplicative Jordan decomposition of $x$. 
The Additive Property

Following Hales and Passi, we say that $\mathbb{Z}[G]$ (or $G$) has the additive Jordan decomposition property (AJD) if for every element $x$ of $\mathbb{Z}[G]$, its semisimple and unipotent parts are both contained in $\mathbb{Z}[G]$.

**Theorem**

**(HP) AJD holds in $\mathbb{Z}[G]$ if and only if $G$ is either**

1. abelian, or

2. of the form $G = Q_8 \times E \times A$, namely $G$ is a Dedekind group, where $Q_8$ is the quaternion group of order 8, $E$ is an elementary abelian 2-group, $A$ is abelian of odd order, and the multiplicative order of 2 modulo $|A|$ is odd, or

3. $G = D_{2p}$ is dihedral, where $p$ is an odd prime.
The Multiplicative Property

We say that $\mathbb{Z}[G]$ (or $G$) has the multiplicative Jordan decomposition property (MJD) if for every unit $x$ of $\mathbb{Z}[G]$, its semisimple and unipotent parts are both contained in $\mathbb{Z}[G]$.

- The first two conditions of the AJD theorem are equivalent to $\mathbb{Q}[G]$ having no nilpotent elements.
- AJD is inherited by subgroups and homomorphic images. MJD is inherited by subgroups.
- AJD implies MJD, so MJD is the more interesting property. We discuss the classification problem for MJD.
Wedderburn Components

**Theorem**

(AHP) If \( \mathbb{Z}[G] \) has MJD, then all Wedderburn components of \( \mathbb{Q}[G] \) have degree \( \leq 3 \).

Using a result of Gow and Huppert, one gets

**Corollary**

If \( \mathbb{Z}[G] \) has MJD, then \( G \) has a normal abelian subgroup \( N \) with \( G/N \) being a 2,3-group. In particular, \( G \) is solvable.
Example: $n = 4$

Let $a, b \in \mathbb{Z}$ with $ab \neq -4$. Set

$$x = \begin{bmatrix} 0 & a & 0 & 0 \\ 0 & 0 & a & 0 \\ 0 & 0 & 0 & a \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{and} \quad y = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & b & 0 \end{bmatrix}$$

Then $1 + z = (1 + x)(1 + y)$ is a unit, with

$$z = \begin{bmatrix} 0 & a & 0 & 0 \\ 0 & 0 & a & 0 \\ 0 & 0 & ab & a \\ 0 & 0 & b & 0 \end{bmatrix} \quad \text{and} \quad zs = \begin{bmatrix} 0 & 0 & 0 & a^2/b \\ 0 & 0 & a & 0 \\ 0 & 0 & ab & a \\ 0 & 0 & b & 0 \end{bmatrix}$$
Theorem

(HPW) Let $\mathbb{Z}[G]$ have MJD, let $z$ be a nilpotent element of $\mathbb{Z}[G]$, and let $e$ be a central idempotent of $\mathbb{Q}[G]$. Then $ez \in \mathbb{Z}[G]$.

The trick is to modify the nilpotent elements in the other components to make them separable. For example, when $n = 2$, nilpotent $x$ is similar to $x = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ and if we let $y = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ then

$$(1 + x)(1 + ry) = \begin{bmatrix} r + 1 & 1 \\ r & 1 \end{bmatrix}$$

is a unit with distinct eigenvalues for all $r \in \mathbb{Z}$ with $r \neq 0, -4$. 
Two Consequences

Corollary

**((HPW))** Assume $G$ has MJD. If $1 \neq N \triangleleft G$ and $H \cap N = 1$, then $\mathbb{Q}[H]$ has no nilpotent elements.

Corollary

**((Lp))** Assume $G$ has MJD. If $N \triangleleft G$ and $N \not\subset J$, then $NJ \triangleleft G$. In particular, if $N \triangleleft G$ is not cyclic, then $G/N$ is Dedekind.

Use $e = \hat{N}/|N|$ and $z = \hat{J}g(1 - j)$. 
Theorem

(Lp) Let $G$ be a $p$-group with MJD. Then all noncyclic subgroups are normal.

Theorem

Let $G$ be a non-Dedekind $p$-group all of whose noncyclic subgroups are normal. Then $G$ is one of the following:

1. A metacyclic group with $|G'| = p$.
2. $G = ZG_0$, the central product of a cyclic group $Z$ with a nonabelian $p$-group $G_0$ of order $p^3$.
3. $p = 2$ and $G = Z \times Q_8$, where $Z$ is cyclic.
4. One of a number of $2$-groups of order $\leq 2^7$.
5. A nonregular group of order $3^4$. 
Theorem

(HPW) Let $G$ be a 2-group of order $\geq 64$. The $\mathbb{Z}[G]$ has MJD if and only if $G$ is a Dedekind group.

- The answer is known for all 2-groups of smaller order.
- The original HPW proof was impressive and technical. It first classified all 2-groups of order $\leq 32$ with MJD. Then used induction to handle all 267 groups of order 64. Then used induction to finish the proof.
- Later, Liu offered a shorter proof using the preceding work. In particular, one knows which are the important groups to test.
Wedderburn Components of Degree 3

Theorem

**(Lp)** Let \( \mathbb{Q}[G] \) have a Wedderburn component \( W \) of degree 3. If \( \mathbb{Z}[G] \) has a unit whose projection to \( W \) is central and of infinite multiplicative order, then \( \mathbb{Z}[G] \) does not have MJD.

The idea is to use a unit \( x \) of the form

\[
x = \begin{bmatrix} 1 & a & 0 \\ 0 & 1 & a \\ 0 & 0 & b \end{bmatrix} \quad \quad x_s = \begin{bmatrix} 1 & 0 & a^2/(b - 1) \\ 0 & 1 & a \\ 0 & 0 & b \end{bmatrix}
\]

with \( b \neq 1 \) a central unit and \( a \neq 0 \). To construct this element, we need \( (b - 1)e_{3,3} \in \mathbb{Z}[G] \), so \( (b - 1) \in m\mathbb{Z}[G] \) for some integer \( m \). We obtain \( b \) by taking a suitably large power of the given central unit.
Two Consequences

Corollary

(Lp) Let $G$ be a nonabelian 3-group. If $G$ has a cyclic central subgroup of order 9, then $\mathbb{Z}[G]$ does not have MJD.

Corollary

(Lp) Let $G$ be the noncommutative semidirect product $G = C_p \rtimes C_{3^k}$ where $C_p$ is cyclic of prime order $p$, $C_{3^k} = \langle g \rangle$ is cyclic of order $3^k$, and $g^3$ centralizes $C_p$. If $p \neq 7$, then $\mathbb{Z}[G]$ does not have MJD.

For the latter, suppose $\varepsilon$ is a primitive $p^{th}$ root of unity and let $\sigma$ be an automorphism of $\mathbb{Z}[\varepsilon]$ of order 3. Then $R = \mathbb{Z}[\varepsilon]^{\sigma}$ has degree $(p - 1)/3$ over $\mathbb{Z}$. Hence $R$ has a unit of infinite multiplicative order provided $p > 7$. If $p = 7$ and $k = 1$, it is known, by (A), that $G$ has MJD.
Theorem

(Lp) If $G$ is a 3-group, then $\mathbb{Z}[G]$ has MJD if and only if $G$ is abelian or one of the two nonabelian groups of order $3^3 = 27$.

The original proof was painfully slow and appeared in three different papers. Later, using the fact that all noncyclic subgroups are normal and the material on Wedderburn components of degree 3, a fairly efficient proof could be offered.
2, 3-Groups

Theorem

**\textbf{(Lp)}** Let $G$ be a nonabelian $2, 3$-group with order divisible by 6. Then $\mathbb{Z}[G]$ has MJD if and only if

1. $G = \text{Sym}_3$, the symmetric group of degree 3,

2. $G = \langle x, y \mid x^3 = 1, y^4 = 1, y^{-1}xy = x^{-1} \rangle$, the “generalized quaternion group” of order 12, or

3. $G = Q_8 \times C_3$, the direct product of the quaternion group of order 8 with the cyclic group of order 3.

At this point, we are fairly close to the end.
The Remaining Groups

According to (HPW) there are three families of nonabelian groups that remain to be considered:

1. $G = Q_8 \times C_p$, where $p$ is a prime $\geq 5$. Furthermore 2 has even multiplicative order modulo $p$. (Recall that if 2 has odd order modulo $p$, then $\mathbb{Z}[G]$ has AJD and hence MJD.)

2. $G = C_7 \rtimes C_{3^k}$, where $C_{3^k} = \langle g \rangle$, is cyclic of order $3^k$ and $g^3$ acts trivially on $C_7$. (Recall that Arora showed that $\mathbb{Z}[G]$ has MJD when $k = 1$.) It follows from work of Amitsur that $\mathbb{Q}[G]$ has only one Wedderburn component of degree $> 1$, namely the one where $g^3$ maps to 1. Indeed, if $k > 1$, then $G$ embeds in a division ring.

3. $G = C_p \rtimes C_{2^k}$, where $C_p$ is cyclic of prime order $p \geq 5$, $C_{2^k} = \langle g \rangle$, is cyclic of order $2^k$, and $g$ acts like the inverse map on $C_p$. If $k = 1$, then $G$ is dihedral, so $\mathbb{Z}[G]$ satisfies AJD and hence MJD. If $k = 2$, then $G$ is “generalized quaternion” and satisfies MJD by (AHP). The problem is open for $k \geq 3$. 