Journal of Algebra and Its Applications

APPENDIX - MULTIPLICATIVE JORDAN DECOMPOSITION IN GROUP RINGS OF 2, 3-GROUPS

Chia-Hsin Liu

Department of Mathematics,
National Taiwan Normal University,
Taipei, Taiwan, R.O.C.
chliu@math.ntnu.edu.tw

D. S. Passman

Department of Mathematics,
University of Wisconsin-Madison,
Madison, Wisconsin 53706, USA
passman@math.wisc.edu

In this appendix, we offer a reasonably self-contained proof that the "generalized quaternion group" Q_{12} of order 12 has the MJD property.

1. Appendix

In this appendix, we consider just one group of order 12, namely

$$G = \langle x, y \mid x^3 = 1,\, y^4 = 1,\, y^{-1}xy = x^{-1}\rangle.$$

Our goal is to show that $\mathbb{Z}[G]$ satisfies MJD. Note that $\langle x\rangle \triangleleft G$, $G = \langle x\rangle \rtimes \langle y\rangle$, and y^2 is central in G. For convenience, let ω denote a primitive complex cube root of 1 and let $i = \sqrt{-1}$. Then $\mathbb{Q}[G]$ has three homomorphisms of interest.

$$\theta_1 \colon \mathbb{Q}[G] \to \mathbb{Q}[G/G'] \cong \mathbb{Q}[\langle y\rangle],$$

$$\theta_2 \colon \mathbb{Q}[G] \to \mathrm{M}_2(\mathbb{Q}[\omega, i])$$

given by

$$x \mapsto \begin{pmatrix} \omega & 0 \\ 0 & \bar{\omega} \end{pmatrix}, \qquad y \mapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

and

$$\theta_3 \colon \mathbb{Q}[G] \to \mathrm{M}_2(\mathbb{Q}[\omega])$$

given by

$$x \mapsto \begin{pmatrix} \omega & 0 \\ 0 & \bar{\omega} \end{pmatrix}, \qquad y \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Note that θ_2 and θ_3 are not epimorphisms as written, but we do have

$$\mathbb{Q}[G] \cong \theta_1(\mathbb{Q}[G]) \oplus \theta_2(\mathbb{Q}[G]) \oplus \theta_3(\mathbb{Q}[G]).$$

We use this notation in the following two results.

Lemma 1.1. *Let G, θ_1 and θ_2 be as above, and let α be a unit of $\mathbb{Z}[G]$.*

i. $\theta_1(\alpha) = \pm\theta_1(y^t)$, *so* $\alpha = \pm y^t\big(1+(1-x)\beta\big)$ *for some* $\pm$ *sign, some* $0 \le t \le 3$, *and some* $\beta \in \mathbb{Z}[G]$.

ii. $\theta_2(\mathbb{Q}[G])$ *is a division algebra.*

iii. $\theta_2(\alpha) = \pm\theta_2(y^t x^j)$, *so* $\alpha = \pm y^t\big(x^j + (1+y^2)\gamma + (1+x+x^2)\delta\big)$ *for some* $\gamma, \delta \in \mathbb{Z}[G]$ *and* $0 \le j \le 2$. *Here* $\pm y^t$ *is as given in (i).*

Proof. (i) The kernel of the homomorphism $\theta_1 \colon \mathbb{Z}[G] \to \mathbb{Z}[G/G']$ is $(1-x)\mathbb{Z}[G]$, and $\mathbb{Z}[G/G']$ is naturally isomorphic to $\mathbb{Z}[\langle y\rangle]$. Since $|\langle y\rangle| = 4$, [Hi, Theorem 6] implies that $\mathbb{Z}[G/G']$ has only trivial units. Thus $\theta_1(\alpha) = \theta_1(\pm y^t)$ for some t, and hence $(\pm y^{-t})\alpha \in 1 + (1-x)\mathbb{Z}[G]$, as required.

(ii) Now $\theta_2(y^2) = -1$, so $1 + y^2 \in \ker\theta_2$. Also $1 + x + x^2 \in \ker\theta_2$. Since the four elements $\theta_2(1), \theta_2(x), \theta_2(y)$ and $\theta_2(xy)$ are easily seen to be $\mathbb{Q}$-linearly independent, it follows that these form a $\mathbb{Q}$-basis for $\theta_2(\mathbb{Q}[G])$ and that

$$\ker\theta_2 = (1+y^2)\mathbb{Q}[G] + (1+x+x^2)\mathbb{Q}[G].$$

Suppose $\tau \in \theta_2(\mathbb{Q}[G])$. Then

$$\begin{aligned}\tau &= a\theta_2(1) + b\theta_2(x) + c\theta_2(y) + d\theta_2(xy)\\ &= \begin{pmatrix} a+b\omega & i(c+d\omega)\\ i(c+d\overline{\omega}) & a+b\overline{\omega}\end{pmatrix}\end{aligned}$$

for suitable $a, b, c, d \in \mathbb{Q}$. Thus

$$\begin{aligned}\det\tau &= (a+b\omega)(a+b\overline{\omega}) + (c+d\omega)(c+d\overline{\omega})\\ &= a^2 + b^2 - ab + c^2 + d^2 - cd\\ &= \big(a^2 + b^2 + (a-b)^2 + c^2 + d^2 + (c-d)^2\big)/2\end{aligned}$$

It follows that $\det\tau \ge 0$ and that $\det\tau = 0$ if and only if $\tau = 0$. Since τ satisfies its characteristic polynomial, $\tau \ne 0$ implies that $\tau^{-1} \in \theta_2(\mathbb{Q}[G])$, and hence $\theta_2(\mathbb{Q}[G])$ is a division ring.

(iii) Now suppose again that α is a unit in $\mathbb{Z}[G]$ and write $\tau = \theta_2(\alpha)$. Then τ is a unit in $\mathrm{M}_2(\mathbb{Z}[\omega, i])$, so $\det\tau$ is a unit in $\mathbb{Z}[\omega, i]$. Since the preceding paragraph implies that $\det\tau$ is a nonnegative rational number, it follows that $\det\tau = 1$. In particular, if τ is written as above, then

$$2 = 2\,\det\tau = \big(a^2 + b^2 + (a-b)^2\big) + \big(c^2 + d^2 + (c-d)^2\big)$$

with $a, b, c, d \in \mathbb{Z}$. Note that, if two of a, b, $a-b$ are 0, then so is the third. Thus either $a = b = 0$ or $a^2 + b^2 + (a-b)^2 \ge 2$. With this, we see that there are just twelve possibilities for τ, namely

$$\begin{array}{lll} c = d = 0, & a = \pm 1,\, b = 0, & \tau = \pm\theta_2(1) \\ & a = 0,\, b = \pm 1, & \tau = \pm\theta_2(x) \\ & a = b = \pm 1, & \tau = \pm\theta_2(x^2) \end{array}$$

and similarly

$$\begin{array}{lll} a = b = 0, & c = \pm 1,\, d = 0, & \tau = \pm\theta_2(y) \\ & c = 0,\, d = \pm 1, & \tau = \pm\theta_2(xy) \\ & c = d = \pm 1, & \tau = \pm\theta_2(x^2 y). \end{array}$$

Since $\theta_2(y^2) = -1$, we conclude that $\theta_2(\alpha) = \tau = \theta_2(g)$ for some $g \in G$. Furthermore, since the kernel of $\theta_2 \colon \mathbb{Z}[G] \to \mathrm{M}_2(\mathbb{Z}[\omega, i])$ is easily seen to be given by $(1+y^2)\mathbb{Z}[G] + (1+x+x^2)\mathbb{Z}[G]$, we have $\alpha = g + (1+y^2)\gamma + (1+x+x^2)\delta$ for suitable $\gamma, \delta \in \mathbb{Z}[G]$.

It remains to relate g to the $\pm y^t$ term given in part (i). To this end, we can replace α by $(\pm y^{-t})\alpha$ and assume that $\alpha = 1 + (x-1)\beta$. Then $\theta_1(\alpha) = 1$, so

$$\begin{aligned} 1 = \theta_1(\alpha) &= \theta_1\big(g + (1+y^2)\gamma + (1+x+x^2)\delta\big) \\ &= y^k + (1+y^2)\sigma_1 + 3\sigma_2 \end{aligned}$$

for suitable $\sigma_1, \sigma_2 \in \mathbb{Z}[\langle y\rangle]$ and $0 \le k \le 3$. Since $(1-y^2)(1+y^2) = 0$, we get

$$(1-y^2)(1-y^k) = 3(1-y^2)\sigma_2 \in 3\,\mathbb{Z}[\langle y\rangle].$$

Clearly $k \ne 1, 2$ or 3, so $k = 0$ and $\theta_1(g) = 1$. Thus $g \in G' = \langle x\rangle$ and $g = x^j$ for some j. This completes the proof. □

With this, we can prove

Proposition 1.2. *The group* G *of order* 12 *given by*

$$G = \langle x, y \mid x^3 = 1,\, y^4 = 1,\, y^{-1}xy = x^{-1}\rangle$$

satisfies MJD. Indeed, if α *is a nonsemisimple unit of* $\mathbb{Z}[G]$*, then its semisimple part is given by* $\alpha_s = \pm y^{2k}$ *for* $k = 0$ *or* 1.

Proof. Assume that α is a unit in $\mathbb{Z}[G]$ that is not semisimple. Since the previous lemma implies that $\theta_1(\alpha) = \pm\theta_1(y^t)$ and $\theta_2(\alpha) = \theta_2(\pm y^t x^j)$ are both semisimple, it follows that $\theta_3(\alpha) \in \mathrm{M}_2(\mathbb{Z}[\omega])$ is not semisimple. In particular, $\theta_3(\alpha)$ must have two identical eigenvalues λ, so that $\operatorname{tr}\theta_3(\alpha) = 2\lambda$ and $\det\theta_3(\alpha) = \lambda^2$.

Note that θ_3 is similar to the representation

$$\theta_3' \colon \mathbb{Q}[G] \to \mathrm{M}_2(\mathbb{Q})$$

given by

$$x \mapsto \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \qquad y \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

so $\operatorname{tr}\theta_3(\alpha) = \operatorname{tr}\theta_3'(\alpha) \in \mathbb{Z}$ and $\det\theta_3(\alpha) = \det\theta_3'(\alpha) \in \mathbb{Z}$. In particular, $2\lambda \in \mathbb{Z}$ and λ^2 is a unit in $\mathbb{Z}$. It follows that $\lambda^2 = 1$ and $\lambda = \pm 1$. Replacing α by $-\alpha$ if necessary, we can assume that $\lambda = 1$, $\operatorname{tr}\theta_3(\alpha) = 2$ and $\det\theta_3(\alpha) = 1$. This clearly implies that $\theta_3(\alpha)$ is unipotent.

Observe that

$$\theta_3(1-x) = \begin{pmatrix} 1-\omega & 0 \\ 0 & 1-\overline{\omega} \end{pmatrix} = (1-\omega)\begin{pmatrix} 1 & 0 \\ 0 & -\overline{\omega} \end{pmatrix},$$

so $\operatorname{tr}\theta_3\big((1-x)\beta\big)$ is divisible by $1-\omega$ for any $\beta \in \mathbb{Z}[G]$.

Now $\alpha = \pm y^t\big(1+(1-x)\beta\big) = \pm y^t + (1-x)\beta'$, so

$$\begin{aligned} 2 = \operatorname{tr}\theta_3(\alpha) &= \operatorname{tr}\theta_3(\pm y^t) + \operatorname{tr}\theta_3\big((1-x)\beta'\big) \\ &= \operatorname{tr}\theta_3(\pm y^t) + (1-\omega)\sigma \end{aligned}$$

for some $\sigma \in \mathbb{Z}[\omega]$. Since the Galois norm of $1-\omega$ is $N(1-\omega) = (1-\omega)(1-\overline{\omega}) = 3$, it follows that $\operatorname{tr}\theta_3(\pm y^t) \neq 0, -2$. Thus $t \neq 1$ or 3, and only the plus sign can occur. In other words, $\alpha = y^{2k}\big(1+(1-x)\beta\big)$. Since y^{2k} is central, it commutes with α, and we now show that this is the multiplicative Jordan decomposition of α.

Replacing α by $y^{-2k}\alpha$, if necessary, we can assume that $\alpha = 1+(1-x)\beta$. Our goal is to show that α is unipotent. Certainly, $\theta_1(\alpha) = 1$ is unipotent, and $\theta_3(\alpha)$ is unipotent, since $\theta_3(y^{2k}) = 1$ implies that $\theta_3(\alpha)$ has not changed. It remains to study $\theta_2(\alpha)$.

To this end, note that the previous lemma implies that

$$\alpha = x^j + (1+y^2)\gamma + (1+x+x^2)\delta$$

for some j. Thus $\theta_2(\alpha) = \theta_2(x^j)$ and $\theta_3(\alpha) = \theta_3(x^j) + 2\,\theta_3(\gamma)$. Since $\operatorname{tr}\theta_3(\alpha) = 2$ is even, it follows that $\operatorname{tr}\theta_3(x^j)$ is also even. But $\operatorname{tr}\theta_3(x) = \operatorname{tr}\theta_3(x^2) = -1$, so we must have $j = 0$ and $\theta_2(\alpha) = \theta_2(x^0) = 1$, as required. □

See [AHP1, Proposition 3.1] for an alternate, but similar, discussion of this group. Also see [AHP2, Theorem 6.1] for analogous results on "generalized quaternion groups" of order $4p$, with p an odd prime.

References

[AHP1] S. R. Arora, A. W. Hales and I. B. S. Passi, *Jordan decomposition and hypercentral units in integral group rings*, Comm. Algebra **21** (1993), 25–35.

[AHP2] S. R. Arora, A. W. Hales and I. B. S. Passi, *The multiplicative Jordan decomposition in group rings*, J. Algebra **209** (1998), 533–542.

[Hi] G. Higman, *The units of group rings*, Proc. London Math. Soc. (2) **46** (1940), 231–248.