THE UNIVERSITY OF ALBERTA

University of Alberta

Library Release Form

Name of Author: Brett G. Giles

Title of Thesis: The Unit Groups of Certain Group Rings

Degree: Master of Science

Year this Degree Granted: 2012

. . . .

Brett G. Giles
93 Fonda Green
Calgary, AB
Canada, T2A 5S4

Date: . . . .

University of Alberta

The Unit Groups of Certain Group Rings

by

Brett G. Giles

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfillment of the requirements for the degree of **Master of Science**.

in

Algebra

Department of Mathematics

Edmonton, Alberta
Fall 2012

University of Alberta

Faculty of Graduate Studies and Research

The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies and Research for acceptance, a thesis entitled **The Unit Groups of Certain Group Rings** submitted by Brett G. Giles in partial fulfillment of the requirements for the degree of **Master of Science** in *Algebra*.

. . . .

S. K. Sehgal

. . . .

Gerald Gliff

. . . .

A. Weiss

. . . .

A. Al-Sallam

Date: . . . .

Abstract

This thesis deals with the problem of describing the unit group of specific group rings over the integers. After a brief introduction to remind one of some of the properties of the group ring we start to discuss the unit groups. A few of the basic results as presented by Sehgal [6], Chapter 2, are shown. After this introduction we talk about specifics.

The first method to determine a unit group is then discussed. It is a general method, applicable to any group. However, in practice we see that it is unsuitable for any but a small number of groups. In this section we talk in an expository manner as the proofs of the results are normally very dependant on the particular group. The ones presented by this method later on are S_3, D_4, D_6 and A_4.

Next, we present the method for groups of order p^3, where p is an odd prime. These come from the paper by Ritter and Sehgal [5]. In this paper they also present a method for determining the unit group of a particular group of order p^n. This will not be treated here. I consider both non-abelian groups of order p^3 and descriptions of the unit groups of both of their respective group rings are presented. Later on in the paper I present the method as applied to the groups of order 27.

The last theoretical results are on determining the unit group of the group ring over a group of order pq where $p \equiv 1(\mod q)$. These results come from a paper by Luthar [3]. No practical examples are done of this method.

The next part deals with presenting actual groups and determining the unit structure of their integral group ring. The first two, S_3 and D_4 are from previous authors. The first was done by Hughes and Pearson [2], the second by C. Polcino-Milies [4]. The next, D_6, is new. The last one is merely an expository account of Allen and Hobby's [1] rendering of $\mathcal{U}(\mathbb{Z}\mathrm{A}_4)$. Our other concrete examples deal with the two non-abelian groups of order 27 as presented in [5] by Ritter and Sehgal.

Contents

List of Figures

List of Tables

Chapter 1

Preliminaries

1.1 Generalities

Throughout this paper the term *group ring* shall be taken as follows: The group ring KG of the group G over the ring K (which posesses an identity) is the ring of all formal sums

$$\alpha = \sum \lambda(g)g$$

where $g \in G$ and $\lambda(g) \in K$ so that $\mathrm{supp}(a) = \{g \mid \lambda(g) \neq 0\}$ is a finite set.

The ring structure is inherited from the structures of the group and the ring. The operations on KG are defined as follows:

$$\begin{aligned} \sum \lambda(g)g &= \sum \mu(g)g & \iff \forall g \in G, \lambda(g) = \mu(g) \\ \sum \lambda(g)g + \sum \mu(g)g &= \sum (\lambda(g) + \mu(g))g \\ \sum \lambda(g)g \cdot \sum \mu(g)g &= \sum \nu(g)g \end{aligned}$$

where $\nu(g) = \sum \lambda(x)\mu(y)$ with the last sum being over all $(x, y) \in G \times G$ with $x \cdot y = g$.

In this paper, we will be investigating the *unit group* of the group ring.

Definition 1.1. *The* unit group *of a group ring KG is the group of all elements invertible under the multiplication of KG.*

It should be noted that the multiplicative identity in KG is the element $1e$, where 1 is the multiplicitive identity of K and e the group identity. Obviously, the unit group of KG contains $\pm G$. Further definition of the unit group becomes more interesting.

1.2 Notation

Throughout this paper the following will be assumed.

$\mathbb{Z}$ the ring of integers.

$\mathbb{Q}$ the ring of rational numbers.

R_n the ring of n by n matrices with entries from R.

$\langle c \rangle$ The group generated by the element c. (There may be be more than one element for generating.)

$\Delta(G, N)$ $\langle x - 1 : x \in N \rangle$in $\mathbb{Z}G$ where N is normal in G. This is also

$$\left\{ \sum_{g \in G} \mu(g) g | \sum_{x \in N} \mu(gx) = 0 \ \forall g \in G \right\}.$$

1.3 General results

In this section, I will present a few of the results from Sehgal [6] in order to give the reader a feel as to what the unit group of a group ring may become at times.

Proposition 1.2. *If G is abelian of order n, then*

$$\mathcal{U}\mathbb{Z}G = \pm G \times F$$

where F is a free abelian group of a determinable order. This order is dependent on the number of cyclic subgroups of various orders in G.

The above theorem helps a great deal when dealing with groups, as it is often possible to get a factor or sub-group of your group to fall in this particular category. In particular, this proposition can be used to show that the unit group of $\mathbb{Z}\langle x \rangle$ where $x^2 = 1$ is just $\pm\langle x \rangle$ This fact is used later.

This proposition along with others can be used to prove the following more powerful theorem.

Theorem 1.3. *If G is a torsion group*[1] *then $\mathcal{U}\mathbb{Z}G = \pm G$ if and only if G is one of*

1. *an abelian group with $G^4 = \{1\}$ or*

2. *an abelian group with $G^6 = \{1\}$ or*

3. *a Hamiltonian*[2] *2-group.*

This theorem completely characterizes torsion groups that have trivial $\mathcal{U}\mathbb{Z}G$.

In conclusion, we note that there are many different areas one can explore when determining unit groups. These range from finding unit groups of particular integral group rings to determining when torsion-free groups have trivial unit groups in their integral group ring.

[1] See definition A.5 in the appendix.

[2] See definition A.2

Chapter 2

Theoretical considerations

2.1 Representation theory method

This method enables us to give a concrete description of the unit groups of certain group rings involving $\mathbb{Z}$. The first two, S_3 and D_4 were done by Hughes and Pearson, and Polcino-Milies, respectively. The third, which is D_6, was done by myself by extending the method of Polcino-Milies. The last one, A_4, which is included only in an expository way, was done by Allen and Hobby. The general manner in which to apply this method is described below.

Consider the group G. We may use representation theory to determine its non-equivalent irreducible representations. Call these θ_i. These will be maps from $\mathbb{Q}G$ to matrices over $\mathbb{Q}$.

If one takes these θ_i that we have obtained, one may now define a map $\theta : \mathbb{Q}G \to \mathbb{Q}_{i1} \bigoplus \ldots \bigoplus \mathbb{Q}_{in}$, by, if $a \in \mathbb{Q}G$, then $\theta(a) = (\theta_1(a), \ldots, \theta_n(a))$. Considering both sides of the mapping as vector spaces over $\mathbb{Q}$, it is readily seen that θ is a linear mapping. Let A be the matrix of θ. It will be noticed that $\theta\mathbb{Z} \subset \bigoplus \mathbb{Z}_n$. Next, by using the matrix A and its inverse we will be able to deduce a system of linear congruences that give us the restrictions needed for an element of $\bigoplus \mathbb{Z}_n$ to be in $\mathbb{Z}G$. These, together with the fact that a matrix with coefficients in $\mathbb{Z}$ has to have an integral determinant in order to have an integral inverse determine the proper group.

Naturally one sees that a significant problem with this method is the size of the matrix A involved. It is a square matrix of size $o(G)$. Another problem is that we have no guarantee that the system of congruences will lead to a usable situation.

A further difficulty with the method is that the end result may turn out to be a direct product of matrix rings. In this case, it is just as difficult to determine properties from this description as it was from the original.

Despite these difficulties, the method is sufficiently useful enough to apply it to a few groups of small size.

2.2 Second Method - Groups of order p^3

In this section, we intend to study the unit groups of the integral group rings of groups of order p^3, where p is an odd prime. The first type, the commutative groups of order p^3, are uninteresting as their unit groups are just + G.

In dealing with the non-commutative groups of order p^3, we note that there are two non-isomorphic groups of that order. They are:

$$H = \langle a, b | a^{p^2} = e = b^p, b^{-1}ab = a^{p+1}\rangle \text{and}$$

$$G = \langle a, b, c | (a, b) = a^{-1}b^{-1}ab = c, ca = ac, cb = bc, a^p = e = b^p = c^p\rangle.$$

Throughout this section we reserve the letters G and H to mean these two groups.

2.2.1 Fibre product

We must now define a concept that we will be using throughout this section — that of the fibre product.

To understand what a fibre product of rings is, consider the ring R with the two ideals I, J of R such that $I \cap J = 0$. Then we have the diagram

$$\begin{tikzcd}
R \arrow[r] \arrow[d] & R/J \arrow[d, "\tilde{}"] \\
R/I \arrow[r, "\hat{}"'] & R/(I+J)
\end{tikzcd}$$

Then R is the fibre product of I and J in the sense that

$$R \cong \{(\alpha, \beta) | \alpha \in R/I, \beta \in R/J, \hat{\alpha} = \tilde{\beta}\},$$

where ˆ is the map from R/I to $R/(I + J)$ and ˜ is the map from R/J to $R/(I + J)$.

From the above we can deduce a fibre product of the unit groups as is given by the following diagram.

$$\begin{tikzcd}
\mathcal{U}(R) \arrow[r] \arrow[d] & \mathcal{U}(R/J) \arrow[d] \\
\mathcal{U}(R/I) \arrow[r] & \mathcal{U}(R/(I+J))
\end{tikzcd}$$

2.2.2 Use of Fibre Product

In this section, we are going to apply this to the Group Ring $\mathbb{Z}X$ with $J = \Delta(X, N)$ as the kernel of the natural homomorphism of $\mathbb{Z}X \longrightarrow \mathbb{Z}X/N$ with N normal in X and $I = \hat{N}\mathbb{Z}G$ where $N = \sum_{x \in N} x$. From here on in, we shall write $\hat{x}$ for $\langle \hat{x} \rangle$.

Pseudo-diagonals of matrices.

To present the proofs of this section, we will need to number certain matrices by their pseudo-diagonals. If the $n \times n$ matrix $A = [a_{ij}]$ is considered, then the j-th pseudo-diagonal is given by the elements

$$a_{1,j+1}, a_{2,j+2}, \ldots, a_{n-1,j-1}, a_{nj}$$

where the second subscript is considered $\mod n$ and $j = 0, 1, 2, 3, ..., n-1$.

Some of the matrices that we will be dealing with from here on will be numbered via their pseudo-diagonals. As an example the matrix $B = [b_{i,j}]$, if numbered by pseudo-diagonals means that the element $b_{i,j}$ is located on the i-th pseudo-diagonal at the j-th spot. When using this indexing scheme, we have $0 \leq i, j \leq n-1$.

For convenience, since we will be dealing with many diagonal-like matrices, we introduce the following notation:

$$A = \mathrm{PDIAG}_i(x_0, \ldots, x_{n-1})$$

will represent the $n \times n$ matrix that has the elements $x_0, \ldots, x_{n-1}$ on the i-th pseudo-diagonal and zeroes elsewhere. If we are talking of the 0-th pseudo-diagonal, we then mean the main diagonal and refer to it as

$$A = \mathrm{DIAG}(x_0, \ldots, x_{n-1})$$

2.2.3 Preliminary propositions

Throughout this section we let ω denote a primitive p-th root of unity.

Proposition 2.1. *Suppose $x_0, \ldots, x_{p-1} \in \mathbb{Z}[\omega]$ then there exists $t_i \in \mathbb{Z}[\omega]$ satisfying*

$$\sum_{i=0}^{p-1} t_i \omega^{ij} = x_j, 0 \leq j \leq p-1$$

if and only if

$$\sum_{i=0}^{p-1} x_i \omega^{ki} \in p\mathbb{Z}[\omega] \ \forall \ 0 \leq k \leq p-1$$

Proof. The system of equations is equivalent to

$$[t_0, \ldots, t_{p-1}]W = [x_0, \ldots, x_{p-1}]$$

where $W = [a_{kl}]$, with $a_{kl} = \omega^{(k-1)(l-1)}$. Now as W is a character matrix, the orthogonality relations of a primitive root of unity tell us that

$$W^{-1} = \frac{1}{p}[a_{kl}^{-1}]$$

.

Our system is equivalent to

$$[t_0, \ldots, t_{p-1}] = [x_0, \ldots, x_{p-1}]W^{-1}.$$

Therefore, there exists a solution if and only if we have

$$\frac{1}{p}\sum_{i=0}^{p-1}\omega^{ik}x_i \in \mathbb{Z}[\omega]$$

for all $0 \leq k \leq p-1$. This, of course, is the same as saying

$$\sum_{i=0}^{p-1}\omega^{ik}x_i \in p\mathbb{Z}[\omega]\forall\ 0 \leq k \leq p-1$$

. □

Proposition 2.2. *Let A and B be $p\times\ p$ matrices over $\mathbb{Q}[\omega]$, with $A = \mathrm{DIAG}(1, \omega, \omega^2, \ldots, \omega^{p-1})$ and B as the matrix with ones on pseudo-diagonal number one, (where numbering of pseudo-diagonals start at zero) and zeroes elsewhere, that is $B = \mathrm{PDIAG}_1(1, 1, \ldots, 1)$.*

Then the $\mathbb{Z}[\omega]$ span of the matrices $\{A^iB^j, 0 \leq i, j \leq p-1\}$ consists of all elements of the form $M = [x_{ij}]$, where the numbering is via the pseudo-diagonals, and such that for each j, k with $0 \leq i, j \leq p-1$ we have

$$\sum_{i=0}^{p-1} x_{ji}\omega^{ki} \ \in\ p\mathbb{Z}[\omega]$$

.

Proof. We see that for a fixed j, the matrices $\{A^iB^j, 0 \leq i, j \leq p-1\}$, have non-zero entries only in the j-th psuedo-diagonal. The vector $(x_0, \ldots, x_{p-1})$ in $\mathbb{Z}[\omega]$ is a diagonal in the span of $\{A^iB^j\}$ if and only if there exists $t_i\ \in\ \mathbb{Z}[\omega]$ such that

$$\sum_{i=0}^{p-1} t_iA^i \ =\ \mathrm{DIAG}(x_0, \ldots, x_{p-1})$$

This, we see, means that

$$\sum_{i=0}^{p-1} t_i\omega^{ji} \ =\ x_j, 0 \leq i, j \leq p-1$$

and now applying the last proposition we now have our answer. □

Proposition 2.3. *Let $o_1 \subset\ \ o_2$ be $\mathbb{Z}$-orders in a rational algebra. Then, if an element $\alpha\ \in\ o_1$ has an inverse in o_2, then α already has an inverse in o_1.*

Proof. As groups, we have that the indices behave in the following manner:

$$(0_2\ :\ \alpha o_1)\ =\ (\alpha o_2\ :\ \alpha o_1)\ \leq\ (o_2\ :\ o_1)$$

which implies that $\alpha o_1\ = o_1$, and therefore shows us that α is a unit in o_1. □

Now we digress before continuing with our list of propositions. Let us recall our group H with the two generators a and b. Let us write $c = a^{-1}b^{-1}ab = a^{p^2}$. Then we have $H' = \langle c \rangle$ of order p. Thus $\widetilde{H} = H/\langle c \rangle = \langle \tilde{a} \rangle \times \langle \tilde{b} \rangle$. As before, ω is a primitive p-th root of unity. Then

$$\mathbb{Q}H \cong \mathbb{Q}\widetilde{H} \oplus \mathbb{Q}(\omega)_p$$

As well as this we have

$$\mathbb{Q}\widetilde{H} \cong \mathbb{Q}H/\Delta(H, \langle c \rangle) \cong \mathbb{Q}H\hat{c}$$

and

$$\mathbb{Q}(\omega)_p \cong \mathbb{Q}H/\hat{c}\mathbb{Q}H.$$

Clearly this gives us

$$\mathbb{Z}H/\Delta(H, \langle c \rangle) \cong \mathbb{Z}\widetilde{H}$$

and the mapping

$$\mathbb{Z}H \to \mathbb{Z}\widetilde{H} \oplus \mathbb{Z}[\omega]_p,$$

with the projection onto the first component. Let us proceed with the calculation of the map with respect to the second component. We easily see that

$$\tilde{c}\mathbb{Z}H + (1-c)\mathbb{Z}H = p\mathbb{Z}H + (1-c)\mathbb{Z}H$$

as c is the sum of p elements all of which are units of $\mathbb{Z}H$. (They are contained in $+H$). Also, it is obvious that

$$\tilde{c}\mathbb{Z}H \cap (1-c)\mathbb{Z}H = 0.$$

Thus, it is obvious that we have the fibre product

$$\begin{tikzcd}
\mathbb{Z}H \arrow[r] \arrow[d] & \mathbb{Z}\widetilde{H} \arrow[d] \\
\mathbb{Z}H/\tilde{c}\mathbb{Z}H \arrow[r] & \mathbb{Z}\widetilde{H}/p\mathbb{Z}\widetilde{H}
\end{tikzcd}$$

with all the maps being natural.

The $p \times p$ matrices $A = \mathrm{PDIAG}_1(1, 1, \ldots, 1, \omega)$ and $B = \mathrm{DIAG}(1, \omega, \omega^2, \ldots, \omega^{p-1})$ obviously satisfy the relations $A^p = \omega I, B^p = I, B^{-1}AB = A^{p^2+1}$.

The matrices $\{B^jA^i | 0 \leq i, j \leq p-1\}$ are linearly independant over $\mathbb{Z}[\omega]$ as is shown in the following: Assume

$$\sum_{i,j} z_{ij}B^iA^j = 0.$$

As A^j has non-zero entries only in the j-th pseudo-diagonal we have

$$\sum_i z_{ij}B^iA^j = 0 \,\forall j,\ 0 \leq j \leq p-1.$$

As A is a non-singular matrix we have that

$$\sum_i z_{ij}Bi = 0,$$

which immediately implies that $z_{ij} = 0 \; \forall 0 \leq i,j \leq p-1$.

Let $T = \mathbb{Z}H/\hat{c}\mathbb{Z}H$, and S_p be the $\mathbb{Z}[\omega]-$span of the matrices $\{B^iA^j \mid 0 \leq i,j \leq p-1\}$, from above. The claim here is that $T \cong S_p$. Consider the map

$$\phi : \mathbb{Z}H \to S_p, \qquad \phi(a) = A, \qquad \phi(b) = B.$$

As $\hat{c} = (1 + c + c^2 + ... + c^{p-1})$ is mapped by ϕ to $(1 + \omega + \omega^2 + ... + \omega^{p-1})I$, which is zero, we have the induced map $\phi_0 : T \to S_p$.

Since $\phi(a^{pk}a^ib^j) = \omega^k A^i B^j$, we have that ϕ is onto S_p. Also we see that ϕ_0 is $1 \leftrightarrow 1$, for if we tensor both T and S_p with $\mathbb{Q}$ we see that both of them have $\mathbb{Z}-$dimension of $p^n - p^{n-1}$

Proposition 2.4. *A matrix $Z \in \mathbb{Z}[\omega]$ is in S_p if and only if the matrix $X = Z'$ satisfies*

$$\sum_{i=0}^{p-1} x_{j,i}\omega^{ki} \in p\mathbb{Z}[\omega], \forall 0 \leq j,k \leq p-1, \omega^p = 1. \tag{2.1}$$

where Z' is obtained from Z by dividing all the entries below the main diagonal by ω.

Proof. We make the observation that $A^i = \mathrm{PDIAG}_i(1,1,\ldots,1,\omega,\ldots,\omega)$, where ω is repeated i times. Thus, to compute S_p it is enough to find the span of $\{B^jA^i | 0 \leq i,j \leq p-1\}$ separately for each i. Therefore, all we need do is to find all $\mathbb{Z}[\omega]$ vectors of the form $(z_{i0},\ldots,z_{ip-1})$ such that

$$\sum_{j=0}^{p-1} t_jB_j\mathrm{DIAG}(1,1,\ldots,1,\omega,\ldots,\omega) = \mathrm{DIAG}(z_{i0},\ldots,z_{ip-1})$$

which is equivalent to

$$\sum_{j=0}^{p-1} t_jB_j = \mathrm{DIAG}(z_{i0},\ldots,z_{ip-i-1},\omega^{-1}z_{ip-i},\ldots,\omega^{-1}z_{ip-1})$$

and the result therefore follows from proposition 2. □

Now let us consider a fibre product of $\mathbb{Z}H$. We have the diagram

$$\begin{tikzcd}
\mathbb{Z}H \arrow[r] \arrow[d] & \mathbb{Z}\hat{H} \arrow[d] \\
T \arrow[r, "\theta_1"] \arrow[d, "\phi_0"'] & (\mathbb{Z}/p\mathbb{Z})\hat{H} \\
S_p \arrow[ur, "\phi_1=\theta_1{\phi_0}^{-1}"'] &
\end{tikzcd}$$

with all the unablelled maps natural,and ϕ_1 defined as above. Then the diagram above is commutative.

Consider ϕ_1. If $M \in S_p$ we wish to write M as $\sum \alpha_{ij}B^iA^j, \alpha_{ij} \in \mathbb{Z}[\omega], 0 \leq i,j \leq p-1$. Let M' be obtained from M by dividing all the elements below the main diagonal by ω.

Then the j-th pseudo-diagonal $x_{j,0}, \dots, x_{j,p-1}$ of M' is the same as the main diagonal of $\sum \alpha_{ij} B^i A^j$.

We then have

$$[\alpha_{0,j}, \dots, \alpha_{p-1,j}]W = [x_{j,0}, \dots, x_{j,p-1}]$$

where $W = [\omega^{ij}], 0 \leq i, j \leq p-1$. Therefore,

$$\alpha_{i,j} = \frac{1}{p} \sum_k \omega^{-ij} x_{i,j}.$$

Recalling that we have

$$M = \sum \alpha_{i,j} B^i A^j$$

then from the above commutative diagram we have

$$\phi_1(M) = \sum \tilde{\alpha}_{i,j} b^i a^j$$

where $\tilde{\alpha}_{i,j}$ is obtained from $\alpha_{i,j}$ by taking $\omega = 1$ and going $\mod p$.

In consideration of Proposition 3, we have the following theorem.

2.2.4 Main result for type 1 groups of order p^3

Theorem 2.5. *1.* $\mathbb{Z}H \cong \{(\alpha, M) \in \mathbb{Z}\widetilde{H} \times \mathbb{Z}[\omega]_p | M'$ *satisfies Equation 2.1 and* $\theta_2(\alpha) = \phi_1(M)\}$.

2. $\mathcal{U}\mathbb{Z}H \cong \{(\alpha, M) \in \mathcal{U}\mathbb{Z}\widetilde{H} \times \mathbb{Z}[\omega]_p | M$ *is a unit of* $\mathbb{Z}[\omega]_p, M'$ *satisfies Equation 2.1 and* $\theta_2(\alpha) = \phi_1(M)\}$.

In the theorem we have,

- M' is obtained from M by dividing every element below the main diagonal by ω where ω is a primitive p-th root of unity.
- Equation 2.1 is the one we have encountered many times already

$$\sum_{i=0}^{p-1} x_{j,i} \omega^{ki} \in p\mathbb{Z}[\omega], \ \forall 0 \leq j, k \leq p-1, \ \omega^p = 1.$$

  where $\{x_{i,j}\}$ are numbered according to the pseudo-diagonals of M'.
- $\theta_2 : \mathbb{Z}\widetilde{H} \to (\mathbb{Z}/p\mathbb{Z})\widetilde{H}$ is the natural map $\mod p$.
- $\phi_1(M) = \sum_{i,j} \tilde{\alpha}_{i,j} \tilde{b}^i \tilde{a}^j$ where $\alpha_{i,j} = \frac{1}{p} \sum_k \omega^{-ik} x_{jk} \in \mathbb{Z}[\omega]$ and $\tilde{\alpha}_{i,j}$ is obtained from $\alpha_{i,j}$ by putting $\omega = 1$ and going $\mod p$.

2.2.5 Groups of type 2 of order p^3

We now consider our second group of order 3 which we refer to as G. Recall

$$G = \langle a, b, c | (a, b) = a^{-1}b^{-1}ab = c, ca = ac, cb = bc, a^p = e = b^p = c^p \rangle \tag{2.2}$$

We note that the factor commutator group, $\widetilde{G} = G/\langle c \rangle$ is elementary abelian of order $p^2, \widetilde{G} = \langle \tilde{a} \rangle \times \langle \tilde{b} \rangle$. This gives us the decomposition

$$\mathbb{Q} \cong \mathbb{Q}\widetilde{G} \oplus \mathbb{Q}(\omega)_p.$$

In fact, we have

$$\mathbb{Q}\widetilde{G} \cong \mathbb{Q}G/\Delta(G, \langle c \rangle) \cong \mathbb{Q}G\tilde{c} \text{ and} \mathbb{Q}(\omega)_p \cong \mathbb{Q}G/\tilde{c}\mathbb{Q}G.$$

Clearly this gives us

$$\mathbb{Z}G/\Delta(G, \langle c \rangle) \cong \mathbb{Z}\widetilde{G} \text{ and the mapping} \mathbb{Z}G \to \mathbb{Z}\widetilde{G} \oplus \mathbb{Z}[\omega]_p$$

with the mapping being projection onto the first component. Our next step will be, as before, to compute the the projection into the second component. We consider the fibre product diagram

$$\begin{tikzcd}
\mathbb{Z}G \arrow[r] \arrow[d] & \mathbb{Z}\widetilde{G} \arrow[d] \\
\mathbb{Z}G/\hat{c}\mathbb{Z}G \arrow[r, "\theta_1"'] & (\mathbb{Z}/p\mathbb{Z})\widetilde{G}
\end{tikzcd}$$

where all the maps are the natural projections excepting the map θ_1 which is

$$\theta_1 : \mathbb{Z}G/\hat{c}\mathbb{Z}G \to (\mathbb{Z}/p\mathbb{Z})\widetilde{G} \text{ with}$$
$$\theta_1(\sum zc^i a^j b^k) = \sum \tilde{z}\tilde{a}^j \tilde{b}^k, \ z \in \mathbb{Z}.$$

2.2.6 Twisting of Group Rings

In order to continue, we need to introduce the notion of *twisted* group rings at this point. A twisted group ring is constructed in the same manner as an ordinary group ring except that the definition of multiplication differs. In the twisted group ring, there is a twisting factor that is used to commute elements.

Let us take the twisted group ring of a ring R and a group G. This is then written as $R \circ G$. The twisting may (and quite often is) be multiplication by a particular element of R. Therefore, if $a, b \in G, r \in R$, we may define the multiplication of a and b in the twisted group ring as $ab = rba$.

Using the notation we have just introduced, it is easy to see that $\mathbb{Z}G/\hat{c}\mathbb{Z}G$ is isomorphic as a ring to the twisted group ring $\mathbb{Z}[\omega] \circ \widetilde{G}$ with $\tilde{b}\tilde{a} = \omega\tilde{a}\tilde{b}$. After this identification, we see that the map θ_1 may be written as

$$\theta_1(\sum \alpha\tilde{a}^i\tilde{b}^j) = \sum \tilde{\alpha}\tilde{a}^i\tilde{b}^j, \alpha \in \mathbb{Z}[\omega].$$

where we get $\tilde{\alpha}$ from α by substituting $\omega = 1$ and going $\mod p$.

Let us now define the map ϕ_0 from $\mathbb{Z}[\omega] \circ \widetilde{G}$ to $\mathbb{Z}[\omega]_p$ by

$$\tilde{a} \to A = \mathrm{DIAG}(l, \omega, \dots, \omega^{p-1}), \tilde{b} \to B = \mathrm{PDIAG}_1(l, \dots, 1).$$

We note that $BA = \omega AB$ and that $A^p = I = B^p$.

We claim that $\{A^i B^j\}$ is a linearly independent set over $\mathbb{Z}[\omega]$ for $0 \leq i, j \leq p-1$. This can easily be seen as follows. Let $\alpha_{i,j}$ be in $\mathbb{Z}[\omega]$ for $0 \leq i, j \leq p-1$. Then we see that

$$\sum_i \sum_j \alpha_{i,j} A^i B^j = 0 \Longrightarrow \sum_i \alpha_{i,j} A^i B^j = 0,$$

as B^j has non-zero entries only in the j-th diagonal. Since B is non-singular, we may remove the B^j from the above result, which implies that $\alpha_{i,j} = 0$ for all $0 \leq i, j \leq p-1$. Therefore, we now have that if $S_p = \mathrm{span}\{A^i B^j, 0 \leq i, j \leq p-1\}$, then

$$\mathbb{Z}G/\hat{c}\mathbb{Z}G \cong \mathbb{Z}[\omega] \circ \widetilde{G} \cong S_p.$$

From proposition 2 it follows that

$$S_p = \{M \in \mathbb{Z}[\omega]_p \mid M \text{satisfies} \sum_{i=0}^{p-1} x_j, i\omega^{ki} \in p\mathbb{Z}[\omega] \ \forall\, 0 \leq i, j \leq p - l\}.$$

Let us consider the following fibre product diagram and extension to S_p.

$$\begin{tikzcd}
\mathbb{Z}G \arrow[r] \arrow[d] & \mathbb{Z}\widetilde{G} \arrow[d] \\
\mathbb{Z}[\omega] \circ \widetilde{G} \cong \mathbb{Z}G/\hat{c}\mathbb{Z}G \arrow[r, "\theta_1"'] \arrow[d, "\phi_0"'] & (\mathbb{Z}/p\mathbb{Z})\widetilde{G} \\
S_p \arrow[ur, "\phi_1"'] &
\end{tikzcd}$$

In the above, the map from S_p to $(\mathbb{Z}/p\mathbb{Z})\widetilde{G}$ is denoted by ϕ_1 and the map from $\mathbb{Z}G/\hat{c}\mathbb{Z}G$ to S_p is denoted by ϕ_0. Obviously, as before in a similar diagram, we define ϕ_1 to be the map $\theta_1 \phi_0^{-1}$.

As before, given M in S_p we wish to find $\phi_0^{-1}(M) \in \mathbb{Z}[\omega] \circ \widetilde{G}$. Let $M = \{x^{j,i}\}$ be numbered by the pseudo-diagonals. We wish to find $a_i, j \in \mathbb{Z}[\omega]$ suc that $\sum_{i,j} a_{i,j} A^i B^j = M$. It is necessary to find $a_{i,j}$ such that

$$\sum_i a_{i,j} A^i = \mathrm{DIAG}(x_{j,0}, \dots, x_{j,p-1}), \ 0 \leq j \leq p-1.$$

Again as before we get this is equivalent to the matrix equation

$$[a_{0,j}, \dots, a_{p-1,j}]W = [x_{j,0}, \dots, x_{j,p-1}]$$

where $W = [w_{i,j}]$ is numbered by columns and rows starting at zero and $w_{i,j} = \omega^{ij}$. Again, by following the previous procedure, we see that

$$a_{i,j} = (\frac{1}{p})\sum_{k=0}^{p-1}\omega^{-ki}x_{j,k}.$$

From the above we have that

$$\phi_0^{-1}(M) = \sum_{i,j} a_{i,j}\tilde{a}^i\tilde{b}^j \quad \text{and} \quad \phi_1(M) = \sum_{i,j}\tilde{a}_{i,j}\tilde{a}^i\tilde{b}^j$$

where $\tilde{a}_{i,j}$ is obtained from $a_{i,j}$ by substituting $\omega = 1$ and going $\mod p$.

The above constitutes the first part of the next theorem. The second part follows directly from proposition 3 as S_p is an order in $\mathbb{Z}[\omega]_p$.

2.2.7 Main result for type 2 groups of order p^3

Theorem 2.6.

1. *$\mathbb{Z}G \cong \{(\alpha, M) \in \mathbb{Z}\widetilde{G} \times \mathbb{Z}[\omega]_p | M'$ satisfies condition 2.1 and $\theta_2(\alpha) = \phi_1(M)\}$.*
2. *$\mathcal{U}\mathbb{Z}G \cong \{(\alpha, M) \in \mathcal{U}\mathbb{Z}\widetilde{G} \times \mathbb{Z}[\omega]_p | M$ is a unit of $\mathbb{Z}[\omega]_p, M$ satisfies 2.1 and $\theta_2(\alpha) = \phi_1(M)\}$.*

In the theorem we have,

1. $\theta_2 : \mathbb{Z}\widetilde{G} \to (\mathbb{Z}/p\mathbb{Z})\widetilde{G}$ is the natural map mod p;
2. The condition 2.1 is the one we have encountered many times

$$\sum_{i=0}^{p-1} x_{j,i}\omega^{ki} \in p\mathbb{Z}[\omega],\ \forall 0 \le j, k \le p-1,\ \omega^p = 1.$$

   where $\{x_{j,i}\}$ are numbered according to the pseudo-diagonals of M.
3. $\phi_1(M) = \sum_{i,j}\tilde{a}_{i,j}\tilde{a}^i\tilde{b}^j$ where $a_{i,j} = \frac{1}{p}\sum_k \omega^{-ki}x_{j,k} \in \mathbb{Z}[\omega]$ and $\tilde{a}_{i,j}$is obtained from $a_{i,j}$by putting $\omega = 1$ and going $\mod p$.

2.2.8 Concluding remarks on groups of order p^3

This concludes our section on groups of order p^3. It should be noted that there are striking similarities in the derivations for both types of groups. However, the proofs do need to be presented separately due to the underlying differences. In a paper by Dr. S. Sehgal and Dr. Jürgen Ritter, [5] the method presented here for type 1 groups of order p^3 is extended to similar type groups of order p^n.

At the end of this paper, I will present examples of the methods shown in this section, using groups of order 27.

2.3 Third method - Groups of order pq

2.3.1 Generalities

In this section, we shall study the unit group of groups of order pq, where p and q are primes $p \equiv 1(\mod q)$. We shall restrict our attention to the non-abelian group of this order. In order to refresh your memory, we have

$$G = \langle a, b \mid a^p = b^q, bab^{-1} = a^j \not\equiv 1 \mod p,\ j^q \equiv 1 \mod p\rangle. \tag{2.3}$$

In this case, we will need to consider the set of normalized units of $\mathbb{Z}G$ given by the map:

$$\sigma : \mathcal{U}\mathbb{Z}G \to \mathcal{U}\mathbb{Z}[b]$$

where

$$\sigma(a) = 1,\ \sigma(b) = b.$$

The kernel of this homomorphism is obviously those elements of $\mathcal{U}\mathbb{Z}G$ for which the coefficient of a^k is 1 and the power of b is 0. Let us denote the kernel by $\mathcal{N}$. This set shall be the group of *normalized* units of $\mathbb{Z}G$. We note that any unit of $\mathbb{Z}G$ can be written as the product of a normalized unit and a unit of $\mathbb{Z}[b]$.

Now since the units of $\mathbb{Z}[b]$ are known to us and we have the equation

$$ba = a^j b$$

we only need to determine the set of normalized units.

Let ω be a primitive p-th root of unity. Then the field $k = \mathbb{Q}(\omega)$ is a cyclic extension of $\mathbb{Q}$ of order $p - 1$. Let k_0 be the fixed field of the automorphism $t : \omega \to \omega^j$. Then k_0 is of degree $(p-1)/q$ over $\mathbb{Q}$. For any element α of k let

$$\alpha^t, \alpha^{(2)t}, \ldots, \alpha^{(q-1)t}$$

be the succesive applications of the automorphism t.

Let R and R_0 denote the rings of integers of k and k_0, respectively. We note that R is a free R_0-module with the basis

$$1, \chi, \chi^2, \ldots, \chi^{q-1}$$

where

$$\chi = \omega - 1$$

is the prime in R over the rational prime p. The corresponding prime in R_0 is

$$X_0 = (\omega - 1)(\omega^2 - 1), \ldots, (\omega^q - 1).$$

As $(\omega^i - 1)/(\omega - 1)$ is a unit, we have that $\chi_0 = \chi^q$ as ideals.

Recalling from number theory that in the above situation we have that

$$\mathbb{Z}/p\mathbb{Z} \cong R_0/\chi_0 R_0 \cong R/\chi R.$$

Therefore, in particular, we have that each element of R modulo χ is congruent to a rational integer.

At this point, we present a lemma.

Lemma 2.7. *Suppose $\alpha \in R$, with $\alpha \equiv s \pmod{x}$, with $s \in \mathbb{Z}$. Then α can be written uniquely as*

$$\alpha = a_0 + a_1\omega + \cdots + a_{p-1}\omega^{p-1}$$

with $\sum a_i = s$, and the $a_i \in \mathbb{Z}$.

Proof. Write

$$\alpha = c0 + c_1\omega + c_2\omega^2 + \cdots + c_{p-1}\omega^{p-1}$$

where the c_i are rational integers. Since $a \equiv S \pmod{\chi}$, we therefore have

$$c0 + c_1 + c_2 + \cdots + c_{p-1} \equiv S \pmod{p}. \tag{2.4}$$

In full generality the first equation may be rewritten as

$$\alpha = (c_0 + m) + (c_1 + m)\omega + (c_2 + m)\omega^2 + \cdots + (c_{p-1} + m)\omega^{p-1}$$

where m is a rational integer. The sum of the new coefficients is s if and only if

$$c0 + c_1 + c_2 + \cdots + c_{p-1} + pm = s.$$

Considering 2.4 above, the relation gives us a unique value for m such that the equality does hold. □

2.3.2 The unit group as matrices over R

.

Recall that it is obvious that $\mathbb{Z}G \cong \mathbb{Z}[a,b]$ and, therefore, an element x of $\mathbb{Z}G$ can be written as

$$x(a,b) = x_0(a) + x_1(a)b + \cdots + x_{q-1}(a)b^{q-1}$$

where $x_i(a)$ is an element of $\mathbb{Z}[a]$. Therefore, if $x, y, z \in \mathbb{Z}G$, written as above, and $z = x \cdot y$, then we would have (upon recalling the definition of multiplication in a group ring) the equations

$$\begin{aligned}
z_0(a) = &\quad x_0(a)y_0(a) + x_1(a)y_{q-1}(a^j) + \cdots + x_{q-1}(a)y_1(a^{j^{q-1}}) \\
z1(a) = &\quad x_0(a)y_1(a) + x_1(a)y_0(a^j) + \cdots + x_{q-1}(a)y_2(a^{j^{q-1}}) \\
\vdots & \\
z_{q-1}(a) = &\quad x_0(a)y_{q-1}(a) + x_1(a)y_{q-2}(a^j) + \cdots + x_{q-1}(a)y_0(a^{j^{q-1}})
\end{aligned}$$

Recalling that$\mathbb{Z}[a] \cong \mathbb{Z}[X]/X^{p-1}$ we can therefore associate to an element $x(a,b) \in \mathbb{Z}G$ the elements

$$\alpha_0 = x_0(\omega), \alpha_1 = x_1(\omega), \ldots, \alpha_{q-1} = x_{q-1}(\omega),$$

with $\alpha_i \in R$.

Consider the matrix

$$A = \begin{bmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_{q-1} \\ \alpha^t_{q-1} & \alpha^t_0 & \cdots & \alpha^t_{q-2} \\ & & \vdots & \\ \alpha_1^{(q-1)t} & \alpha_2^{(q-1)t} & \cdots & \alpha_0^{(q-1)t} \end{bmatrix}$$

with entries in R. We shall call matrices with this form matrices of type 1.

From our previous calculations, we see that the obvious map $x(a,b) \to A$ is a homomorphism from $\mathbb{Z}G$ into the matrices of type 1.

Let us consider what happens when A is invertible in R. Denoting the first row of A^{-1} by $\beta_0, \ldots, \beta_{q-1}$ and we would then have the system of equations

$$\begin{aligned} \beta_0\alpha_0 + \beta_1\alpha^t_{q-1} + \cdots + \beta_{q-1}\alpha_1^{(q-1)t} &= & 1 \\ \beta_0\alpha_1 + \beta_1\alpha^t_0 + \cdots + \beta_{q-1}\alpha_2^{(q-1)t} &= & 0 \\ &\vdots& \\ \beta_0\alpha_{q-1} + \beta_1\alpha^t_{q-2} + \cdots + \beta_{q-1}\alpha_0^{(q-1)t} &= & 0 \end{aligned}$$

If we apply the automorphism $t : \omega \to \omega^j$ to these relations successively we see that

$$A^{-1} = \begin{bmatrix} \beta_0 & \beta_1 & \cdots & \beta_{q-1} \\ \beta^t_{q-1} & \beta^t_0 & \cdots & \beta^t_{q-2} \\ & & \vdots & \\ \beta_1^{(q-1)t} & \beta_2^{(q-1)t} & \cdots & \beta_0^{(q-1)t} \end{bmatrix}$$

is once again of the same type. Therefore, our conclusion is that the invertible matrices of the type 1 form a group.

Let us restrict the homomorphism from $\mathbb{Z}G$ to type 1 matrices down to $\mathcal{N}$, the group of normalized units of $\mathbb{Z}G$. Let us further restrict it to matrices of type 1 that satisfy the following conditions:

$$\alpha_0 \equiv 1, \alpha_1 \equiv 0, \cdots, \alpha_{q-1} \equiv 0 \pmod{\chi} \text{or} A \equiv I \pmod{\chi} \tag{2.5}$$

$$\det A \text{ is a unit in } R_0. \tag{2.6}$$

We conjecture that the homomorphism is actually an isomorphism. First, we show that it is one-to-one. Let $x(a,b)$ be in $\mathcal{N}$, with $x(a,b)$ being mapped to the identity. Then

$$x_0(\omega) = 1, x_1(\omega) = 0, \cdots, x_{q-1}(\omega) = 0.$$

Since $x(a,b)$ is a normalized unit we also have

$$x_0(1) = 1, x_1(1) = 0, \cdots, x_{q-1}(1) = 0$$

which means that

$$x_0(a) = 1, x1(a) = 0, \cdots, x_{q-1}(a) = 0.$$

That shows that the map is one-to-one.

Now we turn our attention to the matter of onto. Let A be invertible of type 1 and satisfy conditions 2.5 and 2.6. Let B be the inverse of A. Let

$$\alpha_0 = x_0(\omega), \alpha_1 = x1(\omega), \cdots, \alpha_{q-1} = x_{q-1}(\omega).$$

where the $x_i(X)$ are polynomials with rational integer coefficients of degree $\leq p-1$, the sum of the coefficients of $x_i = 1$ or $= 0$, corresponding to $i = 0$, or $i = 1, 2, \cdots, q-1$. Form the element

$$x(a,b) = x_0(a) + x1(a)b + \cdots + x_{q-1}(a)b^{q-1}$$

and the corresponding element for B

$$y(a,b) = y_0(a) + y_1(a)b + \cdots + y_{q-1}(a)b^{q-1}$$

which is derived in a similiar manner.

Since $AB = I$ we have

$$\sum_{l+m \equiv i \pmod{p}} x_l(\omega)y_m(\omega) = 1 \text{ or } 0$$

according as to $i = 0$ or $i = 1, 2, 3, \cdots, q-1$. We also see that

$$\sum_{l+m \equiv i \pmod{p}} x_l(1)y_m(1) = 1 \text{ or } 0$$

according as to $i = 0$ or $i = 1, 2, 3, \cdots, q-1$. Therefore, $x(a,b)y(a,b) = 1$. In the same manner as above we see that $y(a,b)x(a,b) = 1$.

Therefore, we have proven that the group $\mathcal{N}$ of normalized units of $\mathbb{Z}G$ is isomorphic to the type 1 matrices in R that satisfy conditions 2.5 and 2.6.

2.3.3 The unit group as matrices over R_0

In this section, we continue from where we left off at the end of the last section and extend our description of $\mathcal{N}$.

Let us put

$$\begin{aligned} \delta = & \quad (X - \chi^t)(X - \chi^{2t}) \cdots (X - \chi^{(q-1)t}) \\ = & \quad X^{q-1} + \delta_1 X^{q-2} + \cdots + \delta_{q-1}. \end{aligned}$$

Also let

$$\delta = \delta\chi.$$

Since we obviously have $X - \chi \equiv X \pmod{\chi}$, we have that

$$N_{k/k_0}(X - \chi) \equiv X \pmod{\chi_0},$$

and, therefore, if we compare coefficients we will have

$$\delta_i \equiv \chi^i \pmod{\chi_0}. \tag{2.7}$$

If one lets $\delta_0 = 1$ then let

$$P = \begin{bmatrix} 1 & \chi^1 & \cdots & \chi^{q-1} \\ 1 & \chi^t & \cdots & (\chi^t)^{q-2} \\ & & \vdots & \\ 1 & \chi^{(q-1)t} & \cdots & (\chi^{(q-1)t})^{q-1} \end{bmatrix}$$

With some work, we can see that P^{-1} is $[p_{i,j}], 1 \leq i, j \leq q$ where the numbering is by rows and columns and $p_{i,j} = (\delta_{q-i}/\delta)^{(i-1)t}$, where a^{0t} is, of course, just a.

Let $E = \mathrm{PDIAG}_1(1, 1, \cdots, 1)$ be a $q \times q$ matrix. It is quite obvious that $E^{-1} = \mathrm{PDIAG}_{q-1}(1, 1, \cdots, 1) = E^{q-1}$. For a matrix M with entries in k, we shall denote by M' the matrix obtained from M by applying the automorphism t to the entries of M. In consideration of this, it is obvious that $P' = EP$, and $(P^{-1})' = P^{-1}E^{-1}$. Therefore if A has its entries in k, then $P^{-1}AP$ has entries in k_0 if and only if $A' = EAE^{-1}$.

This is equivalent to the matrix A being a type 1 matrix from the previous section. That is

$$A = \begin{bmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_{q-1} \\ \alpha^t_{q-1} & \alpha^t_0 & \cdots & \alpha^t_{q-2} \\ & & \vdots & \\ \alpha_1^{(q-1)t} & \alpha_2^{(q-1)t} & \cdots & \alpha_0^{(q-1)t} \end{bmatrix}$$

where the elements are in k.

It then follows that the map from A to $X = P^{-1}AP$ is an isomorphism of the ring of matrices A of type 1 having entries in k with the ring of $q \times q$ matrices X with entries in k_0.

Let $X = [x_{i,j}], 0 \leq i, j \leq q-1$. Suppose that X with entries in R_0 satisfies the congruence

$$X \equiv \begin{bmatrix} 1 & 0 \\ * & 1 \end{bmatrix} \pmod{\chi_0 (= \chi^{q-1})}. \tag{2.8}$$

Then the entries in the first row of the corresponding matrix $A = PXP^{-1}$ are

$$\begin{aligned} \alpha_0 &= \frac{1}{\delta}\left(x_0(\chi)(\delta_{q-1}) + x_1(\chi)(\delta_{q-2}) + \cdots + x_{q-1}(\chi)(\delta_0)\right) = \frac{\beta_0}{\delta} \\ \alpha_1 &= \frac{1}{\delta^t}\left(x_0(\chi)(\delta_{q-1})^t + x_1(\chi)(\delta_{q-2})^t + \cdots + x_{q-1}(\chi)(\delta_0)^t\right) = \frac{\beta_1}{\delta^t} \\ &\vdots \\ \alpha_{q-1} &= \frac{1}{\delta^{(q-1)t}}\left(x_0(\chi)(\delta_{q-1})^{(q-1)t} + \cdots + x_{q-1}(\chi)(\delta_0)^{(q-1)t}\right) = \frac{\beta_{q-1}}{\delta^{(q-1)t}} \end{aligned}$$

where for $0 \leq i \leq q-1$,

$$x_i(\chi) = x_{0,i} + x_{1,i}\chi + \cdots + x_{q-1,1}\chi^{q-1} \equiv \chi^i \pmod{\chi^{i+1}},$$

This implies, if we consider the congruences involving the δ_i's and the congruences that one can derive by successive applications of the automorphism t to them we have

$$\beta_0 \equiv q\chi^{q-1} \pmod{\chi}$$

and

$$\beta_i \equiv (\chi^{it})^{q-1} + \chi(\chi^{it})^{q-2} + \cdots + \chi^{q-2}(\chi^{it})^{q-1} + \chi^{q-1} \pmod{\chi}$$

Since δ and its conjugates via the isomorphism t are all associates of χ^{q-1} this means that the α_i are all elements of R. As well, $\pmod{\chi}$ we will have the following hold true:

$$\begin{aligned} \frac{\delta}{\chi^{q-1}} = & \quad \left(1 = (\chi^t/\chi)\right)\left(1 = (\chi^{2t}/\chi)\right)\cdots\left(1 = (\chi^{(q-1)t}/\chi)\right) \\ \equiv & \quad (j-1)(j^2-1)\cdots(j^{q-1}-1) \\ \equiv & \quad q \end{aligned}$$

Therefore, we have that

$$\alpha_0 = \frac{\beta_0}{\delta_0} \equiv 1 \pmod{\chi}.$$

Since

$$(\frac{\chi^t}{\chi})^q - 1 = \left(\frac{\omega^j - 1}{\omega - 1}\right)^q - 1 \equiv j^q - 1 \equiv 0 \pmod{\chi},$$

therefore, $(\chi^t)^q - \chi^q \equiv 0 \pmod{\chi^{q+1}}$, and therefore, noticing that $\chi^t - \chi$ is an associate of χ, we have

$$\beta_1 \equiv \left(\frac{(\chi^t)^q - \chi^q}{\chi^t - \chi}\right) \equiv 0 \pmod{\chi^q}$$

giving us the relation

$$\alpha_1 = \frac{\beta_1}{\delta^t} \equiv 0 \pmod{\chi}.$$

Similarly, we can continue to show that $\alpha_i \equiv 0 \pmod{\chi}$ for $2 \leq i \leq q-1$.

Now let us do the converse. Suppose we have a matrix A of type 1 with entries in R that satisfy the conditions

$$\alpha_i \equiv 0 \text{ or } 1 \pmod{\chi}$$

depending as $i = 0$ or $i = 1, 2, \cdots, q-1$. Let $X = P^{-1}AP$. Number the matrix X as above, $X = [x_{i,j}]$ for $0 \leq i, j \leq q-1$, the numbering according to columns and rows. In consideration of the above, we note that

$$\begin{aligned}
x_{i,j} = & \sum_{u,v} \left((\frac{\delta_{q-i-1}}{\delta})^{(u)t} (\alpha_{q-u+v})^{(u)t} (\chi^j)^{(v)t} \right) \\
= & \sum_{u} \left(\sum_{v} (\frac{\delta_{q-i-1}}{\delta})(\alpha_{q-u+v})(\chi^j)^{(v-u)t} \right)^{(u)t} \\
= & \sum_{u} \left(\sum_{v} (\frac{\delta_{q-i-1}}{\delta})(\alpha_{v})(\chi^j)^{(v)t} \right)^{(u)t} \\
= & \operatorname{Tr} \left((\frac{\delta_{q-i-1}}{\delta})(\sum_{v} \alpha_v (\chi^j)^{(v)t}) \right),
\end{aligned}$$

where Tr is the trace of k over k_0. Since δ is the different of the extension k over k_0, we have that $x_{i,j}$ is in R_0. As well, in view of the congruences involving the δ_i and the α_i, we would have that if $j \geq i$,

$$\begin{aligned}
x_{i,j} = & \operatorname{Tr} \left(\left(\frac{\chi^{q-i-1}}{\delta} \right) \sum_{v} \alpha_v (\chi^j)^{(v)t} \right) \\
= & \operatorname{Tr} \left(\frac{\chi_{q-i-1}}{\delta} \alpha_0 \chi^j \right) \\
= & \operatorname{Tr} \left(\frac{\chi_{q-1+j-i}}{\delta} \right) \\
\equiv & \ 1 \text{ or } 0 \pmod{\chi_0}
\end{aligned}$$

according to whether $i = j$ or $i < j$. This means that the matrix X has entries in R_0 satisfying the conditions in equivalence 2.8. Therefore, we have proven the following theorem.

Theorem 2.8. *The group of normalized units $\mathcal{N}$ of $\mathbb{Z}G$ is isomorphic to the group of $q \times q$ matrices X in R_0 that are invertible in R_0 and satisfying the congruences*

$$X \equiv \begin{bmatrix} 1 & 0 \\ * & 1 \end{bmatrix} \pmod{\chi_0 (= \chi^{q-1})}.$$

This concludes our section on the groups of order pq. The rest of the thesis deals with concrete examples.

Chapter 3

Applications of Representation Method.

In this section, we shall use the first method described in this paper to describe the unit groups of S_3, D_4, D_6, and, as well, as give a brief expository account of the method findings for A_4.

3.1 The Unit Group of $\mathbb{Z}S_3$.

The first thing we do is consider a map deduced from a representation of S_3 given by

$$\begin{aligned} \theta(12) &= & \begin{pmatrix} 1 & -1 & \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} \end{pmatrix} \\ \theta(123) &= & \begin{pmatrix} 1 & 1 & \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \end{pmatrix} \end{aligned}$$

As one can see from the above this gives rise to a map

$$\theta : \mathbb{Q}\ S_3 \to \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}_2.$$

We define the map by linear extension using the convention that cycles multiply from the right to the left (for example $(12)(123) = (23)$). Since we have defined θ by linear extension we see that this map is a homomorphism.

Let $B_1 = \{e, (12), (23), (13), (123), (132)\}$ be a basis of $\mathbb{Q}S_3$ and let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_6)$ be an element of $\mathbb{Q}S_3$ with respect to the basis B_1. Similarly let B_2 be the canonical basis for $\mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}_2$ with $X = (x_1, x_2, \cdots, x_6)$ being an element of that space with respect to B_2.

Then we may consider $x = \theta\alpha = \alpha A$ where

$$A = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & -1 & 1 & -1 & 0 & -1 \\ 1 & -1 & -1 & 0 & -1 & 1 \\ 1 & -1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & -1 & 1 & -1 \\ 1 & 1 & -1 & 1 & -1 & 0 \end{bmatrix}$$

and upon further calculation we see that

$$A^{-1} = \frac{1}{6}\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & -1 & 1 & 1 \\ 2 & 2 & -2 & 0 & -2 & 0 \\ 0 & 0 & -2 & 2 & -2 & 2 \\ 0 & -2 & 0 & 2 & 2 & -2 \\ 2 & -2 & 2 & 0 & 0 & 2 \end{bmatrix}$$

As A is invertible, it is readily seen that θ is an isomorphism. Moreover from the elements of A it is readily seen that

$$\theta\mathbb{Z}S_3 \subset \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}_2.$$

Furthermore, if we consider A^{-1}, then for $x_i \in \mathbb{Z}S_3$, we have

$$\theta^{-1}x \in \mathbb{Z}S_3 \iff$$

$$\begin{array}{ccccccll} x_1 & +x_2 & +2x_3 & & & +2x_6 & \equiv 0 & \pmod 6 \\ x_1 & -x_2 & +2x_3 & & -2x_5 & -2x_6 & \equiv 0 & \pmod 6 \\ x_1 & -x_2 & -2x_3 & -2x_4 & & +2x_6 & \equiv 0 & \pmod 6 \\ x_1 & -x_2 & & +2x_4 & +2x_5 & & \equiv 0 & \pmod 6 \\ x_1 & +x_2 & -2x_3 & -2x_4 & +2x_5 & & \equiv 0 & \pmod 6 \\ x_1 & +x_2 & & +2x_4 & -2x_5 & -2x_6 & \equiv 0 & \pmod 6 \end{array}$$

After simple row reduction we see that this reduces to the following set of three equations.

$$\begin{array}{ccccccll} x_1 & +x_2 & & +2x_4 & +4x_5 & +4x_6 & \equiv 0 & \pmod 6 \\ & 4x_2 & & & +4x_5 & +2x_6 & \equiv 0 & \pmod 6 \\ & & 4x_3 & +2x_4 & +4x_5 & +2x_6 & \equiv 0 & \pmod 6 \end{array}$$

The second and third reduce respectively to:

$$\begin{array}{cccccl} x_2 & & \equiv & x_6 & -x_5 & \pmod 3 \\ x_4 & +x_5 & \equiv & x_3 & +x_5 & \pmod 3 \end{array}$$

Inspection of the first equation shows us that

$$x_1 + x_2 \equiv 0 \pmod 2$$

If we also consider our first equation as an equation modulo 3 and combine it with the result of the second equation we get

$$x_1 \equiv x_4 + x_6 \pmod 3.$$

Therefore, the final result is as follows:

$$\begin{array}{cccccl} x_1 & +x_2 & \equiv & 0 & & \pmod 2 \\ & x_2 & \equiv & x_6- & x_5 & \pmod 3 \\ x_1 & & \equiv & x_3+ & x_5 & \pmod 3 \\ & & \equiv & x_4+ & x_6 & \pmod 3 \end{array}$$

Keeping all this in mind, we next consider the projection operator $\phi : \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}_2 \to \mathbb{Q}_2$. Then we can see that

$$\phi\theta\mathbb{Z}S_3 = \left\{ \begin{pmatrix} x_3 & x_4 \\ x_5 & x_6 \end{pmatrix} | x_3 + x_5 \equiv x_4 + x_6 \pmod 6 \right\}$$

Let us call this space $\mathbf{Y}$.

Let $X = (x1, \cdots, x6) \in \theta\mathbb{Z}S_3$, with $x_6 \equiv x_3 + x_5 - x_4 \pmod 3$. Let $\delta = x_3x_6 - x_4x_5$. Consider

$$(x_3 - x_4)(x_3 + x_5) = x_3(x_3 + x_5 - x_4) - x_4x_5 \equiv x_3x_6 - x_4x_5 \pmod 3 \equiv \delta \pmod 3$$

In consideration of our row reduced equations it follows that X^{-1} exists and is in $\theta\mathbb{Z}S_3 \iff x_3x_6 - x_4x_5 = \delta = \pm 1, x_1 = 1, x_2 = \delta x_1$.

We see by composition of maps, that $\phi\theta$ is a homomorphism of $\mathbb{Z}S_3$ into $\mathbf{Y}$, and therefore induces a homomorphisim of the unit group of $\mathbb{Z}S_3$ into the unit group of $\mathbf{Y}$. We will now show that this induced homomorphism is one to one and onto, proving that it is an isomorphism.

Let

$$Z = \begin{pmatrix} x_3 & x_4 \\ x_5 & x_6 \end{pmatrix} \in \mathcal{U}(\mathbf{Y}).$$

Also let $\delta = x_3x_6 - x_4x_5 = \pm 1$ and if $x_1, x_2 \in \{-1, 0, 1\}$ are defined by the congruences

$$\begin{aligned} x_2 &\equiv x_6 - x_5 \pmod 3 \text{ and} \\ x_1 &\equiv x_3 + x_5 \pmod 3 \end{aligned}$$

then neither x_1 nor x_2 is zero and all the above conditions are satisified. Therefore $\alpha = \theta^{-1}X$ is a unit in $\mathbb{Z}S_3$ with $\phi\theta\alpha = U$. Therefore, by the above we have that $\phi\theta$ is one to one and onto, therefore we have

Theorem 3.1. *The unit group of $\mathbb{Z}S_3$ is isomorphic to:*

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{U}(\mathbb{Z}_2) | a + c \equiv b + d \pmod 3 \right\}$$

3.2 The units of $\mathbb{Z}D_4$

In this section, we will determine the group of units of $\mathbb{Z}D_4$, where D_4 is the dihedral group of order 8. This group is determined by the generators a, b together with the relations

$$a^4 = b^2 = baba = 1.$$

Before proceeding with the construction, we give a few definitions. The homomorphism $\xi : \mathbb{Z}G \to \mathbb{Z}$ with $\xi(g) = 1$ for all $g \in G$ is called the *augmentation function.* Denote by $V(\mathbb{Z}G)$ the normal subgroup of the units $u \in \mathbb{Z}G$ such that $\xi(u) = 1$. If u is in $V(\mathbb{Z}G)$, it is called a *normalized unit*. Finally an automorphism θ of $\mathbb{Z}G$ is said to be normalized if $\xi\theta(g) = 1$ for all $g \in G$.

Now, as before, we determine our map from $\mathbb{Q}D_4$ to a direct sum of matrix rings over $\mathbb{Q}$. In this case, the map will be

$$\theta : \mathbb{Q}D_4 \to \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}_2$$

given by

$$\begin{aligned} \theta(a) &= \left(1, 1, -1, -1, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right) \quad \text{and} \\ \theta(b) &= \left(1, -1, 1, -1, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) \end{aligned}$$

In the same manner as before, consider D_4 as the basis of $\mathbb{Q}D_4$ and use the canonical basis for the right hand side of the above mapping. Then the map θ can be represented by A where A is the following matrix.

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & -1 & -1 & 0 & -1 & 1 & 0 \\ 1 & 1 & 1 & 1 & -1 & 0 & 0 & -1 \\ 1 & 1 & -1 & -1 & 0 & 1 & -1 & 0 \\ 1 & -1 & 1 & -1 & 0 & 1 & 0 & \\ 1 & -1 & -1 & 1 & -1 & 0 & 0 & 1 \\ 1 & -1 & 1 & -1 & 0 & -1 & -1 & 0 \\ 1 & -1 & -1 & 1 & 1 & 0 & 0 & -1 \end{bmatrix}$$

Continuing our calculations we find that A^{-1} is $\frac{1}{8}$ times the following matrix.

$$A^{-1} = \frac{1}{8}\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 2 & 0 & -2 & 0 & 0 & 2 & 0 & 2 \\ 0 & -2 & 0 & 2 & 2 & 0 & -2 & 0 \\ 0 & 2 & 0 & -2 & 2 & 0 & -2 & 0 \\ 2 & 0 & -2 & 0 & 0 & 2 & 0 & -2 \end{bmatrix}$$

In the same manner as before, we see that if

$$X = \left(x_1, x_2, x_3, x_4, \begin{pmatrix} x_5 & x_6 \\ x7 & x_8 \end{pmatrix}\right)$$

with $X \in \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}_2$ then X belongs to$\theta(\mathbb{Z}D_4)$ iff

$$x_1+ \quad x_2+ \quad x_3+ \quad x_4+ \quad 2x_5 \qquad + \quad 2x8 \quad \equiv 0 \pmod 8$$

$$\bullet$$

$$\bullet$$

$$\bullet$$

$$x_1- \quad x_2- \quad x_3+ \quad x_4+ \quad 2x_5 \qquad - \quad 2x_8 \quad \equiv 0 \pmod 8$$

Applying row reduction in the same manner as the last example we get

$$\begin{array}{rcccccccccl}
i) & x_1+ & x_2+ & x_3+ & x_4+2 & x_5 & & + & 2x_8 & \equiv 0 & \pmod 8 \\
ii) & & x_2+ & x_3 & & & & + & 2x_8 & = 0 & \pmod 4 \\
iii) & & & x_3- & x_4- & x_5- & x_6- & x_7+ & x_8 & \equiv 0 & \pmod 4 \\
iv) & & & & x_4+ & x_5 & + & x_7 & & \equiv 0 & \pmod 2 \\
v) & & & & & x_5 & & + & x_8 & \equiv 0 & \pmod 2 \\
vi) & & & & & & x_6+ & x_7 & & \equiv 0 & \pmod 2
\end{array}$$

In addition, if X is to belong to $\theta(\mathcal{U}\mathbb{Z}D_4)$, then $x_i = \pm 1$ for $i = 1, 2, 3, 4$ and we must have $x_5 x_8 - x_6 x_7 = \pm 1$.

Consider $\mathcal{X} \in GL(2, \mathbb{Z})$, with

$$\mathcal{X} = \begin{pmatrix} x_5 & x_6 \\ x_7 & x_8 \end{pmatrix}$$

which satisfy equations $v)$ and $vi)$ above. Then there exists $x_i, i = 1, 2, 3, 4$ with $X = (x_1, x_2, x_3, x_4, \mathcal{X} \in \mathcal{U}\mathbb{Z}D_4) \iff$ one of $a)$, $b)$ or $c)$ below hold.

$$\begin{array}{rlll}
a) & x_8 \equiv 1 \pmod 2; & x_5 + x_6 + x_7 - x_8 \equiv 0 \pmod 4; & x_5 + x_8 \equiv 2 \pmod 4 \\
b) & x_8 \equiv 1 \pmod 2; & x_5 + x_6 + x_7 - x_8 \equiv 2 \pmod 4; & x_5 + x_8 \equiv 0 \pmod 4 \\
c) & x_8 \equiv 0 \pmod 2; & x_5 + x_8 \equiv 0 \pmod 4; &
\end{array}$$

Let us do the calculations that show this. Consider: if X is in $\theta(\mathcal{U}D_4)$, then, as noted before, we must have x_1, x_2, x_3 and $x_4 = \pm 1$. Let $\delta = \pm 1$. Then there are only certain combinations of the above that satisfy equations $i)$ through $vi)$. In particular, it should be noted that either all of x_1 to x_4 are either of the same sign or there are two of one sign and two of the other. To see this, consider equations $i)$ and $v)$. If three of x_1 to x_4 were positive 1 and the fourth negative 1, then we would have that $x_5 + x_8 \equiv 1 \pmod 4$. This is an obvious contradiction to equation $v)$.

Therefore, let us consider the cases separately. If $x_1 = x_2 = x_3 = x_4 = \delta$, then equation $i)$ implies that

$$\begin{aligned} 2x_5 + 2x_8 &\equiv 4 \pmod 8 \text{ which implies that} \\ x_6 + x_8 &\equiv 0 \pmod 4. \end{aligned}$$

Equation $iii)$ tells us that

$$\begin{aligned} -x_5 - x_6 - x_7 + x_8 &\equiv 0 \pmod 4 \text{ which implies that} \\ x_5 + x_6 + x_7 - x_8 &\equiv 0 \pmod 4. \end{aligned}$$

Finally, equation $ii)$ gives us that

$$x_8 \equiv 1 \pmod 2.$$

It can be readily seen that the above is condition $a)$.

Let us now consider $x_1 = x_2 = -x_3 = -x_4 = \delta$. Here we see that equation $i)$ implies

$$x_5 + x_8 \equiv 0 \pmod 4.$$

Equation *ii*) implies

$$x_8 \equiv 0 \pmod 2.$$

We see that we now have condition *c*). In addition, however, we can see that equation *iii*) implies that

$$x_5 + x_6 + x_7 - x_8 \equiv 0 \pmod 4.$$

Now suppose that $x_1 = -x_2 = x_3 = -x_4 = \delta$. Then, we will have equation *i*) implying

$$x_5 + x_8 \equiv 0 \pmod 4.$$

Equation *ii*) gives us

$$x_8 \equiv 0 \pmod 2.$$

Again, we have condition c). This time, though, Equation *iii*) shows us

$$x_5 + x_6 + x_6 - x_8 \equiv 2 \pmod 4.$$

The last combination to consider is $x_1 = -x_2 = -x_3 = x_4 = \delta$. In this case we get equation *i*)showing that

$$x_5 + x_8 \equiv 0 \pmod 4.$$

Equation *ii*) implies that

$$x_8 \equiv 1 \pmod 2.$$

Equation *iii*) implies that

$$x_5 + x_6 + x_7 - x_8 \equiv 2 \pmod 4.$$

This finally is condition b).

To show the other direction of the if and only if above is quite simple given the above calculations. What one needs to do is to simply choose the particular x_i $(i = 1, 2, 3, 4)$ as given above. These will then satisfy all the equations.

Let us denote by Ω those matrices of $GL(2, \mathbb{Z})$ that satisfy equations *v*) and *vi*) above and any one of a), b) or c). It is obvious by the linearity of the constraints that Ω is a subgroup of $GL(2, \mathbb{Z})$. For any element $X \in \Omega$ we can see by the above computations that there are exactly two elements of $\theta\mathcal{U}\mathbb{Z}D_4$ with X as the last member.

Let $\delta = \pm 1$ as above.

If a) holds, then $\mathcal{X} = (\delta, \delta, \delta, \delta, X) \in \theta\mathcal{U}\mathbb{Z}D_4$.

If b) holds, then $\mathcal{X} = (\delta, -\delta, -\delta, \delta, X) \in \theta\mathcal{U}\mathbb{Z}D_4$.

If c) holds, there are two cases to consider. If we have the first, which is

$$x_5 + x_6 + x_7 - x_8 \equiv 0 \pmod 4.$$

holding, then

$$\mathcal{X} = (\delta, \delta, -\delta, -\delta, X) \in \theta\mathcal{U}\mathbb{Z}D_4.$$

Otherwise, we have

$$x_5 + x_6 + x_7 - x_8 \equiv 2 \pmod 4.$$

holding which gives us

$$\mathcal{X} = (\delta, -\delta, \delta, -\delta, X) \in \theta\mathcal{U}\mathbb{Z}D_4.$$

Now, we are in a position to describe the unit group of $\mathbb{Z}D_4$. If we choose $\alpha \in \mathcal{U}\mathbb{Z}D_4$ such that $\theta(\alpha) = (x_1, x_2, x_3, x_4, X)$, then we can observe that $\xi(\alpha) = x_1$. From this and the preceding information it is easy to see that since for any element X in Ω there are exactly two elements in $\theta\mathcal{U}\mathbb{Z}D_4$, we have the following theorem.

Theorem 3.2.

$$\theta\mathcal{U}\mathbb{Z}D_4 \cong \{\pm 1\} \times \Omega.$$

3.3 Units of $\mathbb{Z}D_6$.

In this section, we will show how a minor extension to the method can be used to describe groups of higher orders. At this point, we will determine the unit group of $\mathbb{Z}D_6$where $D_6$is the dihedral group of order 12 given by the generators a, b together with the relations

$$a^2 = b^6 = ab^2ab^2 = e$$

Now if we applied the method of this section blindly we would be dealing with matrices of order 12. This, to say the least, is inelegant. In addition to this the description of $\mathcal{U}\mathbb{Z}D_6$ would include a direct product of two matrix groups. This does not give us a very satisfying description, as determining properties of this type of product is not very easy.

Instead, what we do in this section is to consider $D_6 \cong C_2 \times S_3$ where C_2 is the cyclic group of order 2,$= +1, -1$ under multiplication. $S_3$is, as before, the symmetric group on 3 elements. Keeping this in mind, we have $\mathbb{Z}D_6 \cong (\mathbb{Z}C_2)S_3$, where $\mathbb{Z}C_2$ is the group ring of the group C_2 over the ring $\mathbb{Z}$, and the whole thing is the group ring of the group S_3 over the ring $\mathbb{Z}C_2$. The isomorphism of the above group rings is a well known theorem (See Sehgal[6]).

At this point, let us denote $\mathbb{Q}C_2$ by $\mathcal{R}$. Then what we intend to do is to apply the method used previously, replacing $\mathbb{Q}$ by $\mathcal{R}$ and $\mathbb{Z}$ by $\mathbb{Z}C_2$. This brings us to the point where we may now define the map θ as

$$\theta \mathcal{R}S_3 \to \mathcal{R} \oplus \mathcal{R} \oplus \mathcal{R}$$

where the mapping is defined by

$$\theta(1\ 2) = \qquad \begin{pmatrix} 1 & -1 & \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} \end{pmatrix}$$

and

$$\theta(1\ 2\ 3) = \qquad \begin{pmatrix} 1 & 1 & \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \end{pmatrix}$$

At this point, one must keep in mind that the elements of the above vectors are in $\mathcal{R}$ not in $\mathbb{Q}$ as before.

Now, let us consider the two modules that we have. The first $\mathcal{R}S_3$ is obviously a free module over $\mathcal{R}$ with basis the elements of S_3. The second is again a free module over $\mathcal{R}$ being a direct sum of matrix rings over $\mathcal{R}$. We will use the standard basis for this module.

Considering this, we may look at θ as a module homomorphism between two free modules. We may therefore represent it as a matrix A, in this case, a 6×6 matrix. Obviously this matrix is going to have the same entries as the one we obtained when looking at $\mathbb{Z}S_3$, with the distinction that these elements will be in $\mathcal{R}$ and not just in $\mathbb{Q}$. For the sake of convenience I will rewrite A and A^{-1}.

$$A = \qquad \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & -1 & 1 & -1 & 0 & -1 \\ 1 & -1 & -1 & 0 & -1 & 1 \\ 1 & -1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & -1 & 1 & -1 \\ 1 & 1 & -1 & 1 & -1 & 0 \end{bmatrix}$$

and

$$A^{-1} = \qquad \frac{1}{6}\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & -1 & 1 & 1 \\ 2 & 2 & -2 & 0 & -2 & 0 \\ 0 & 0 & -2 & 2 & -2 & 2 \\ 0 & -2 & 0 & 2 & 2 & -2 \\ 2 & -2 & 2 & 0 & 0 & 2 \end{bmatrix}$$

As before, since A is invertible we see that θ is an isomorphism. Also, as before, we are led to a set of six congruences that describe when an element of $(\mathbb{Z}C_2) \oplus (\mathbb{Z}C_2) \oplus (\mathbb{Z}C_2)_2$ mapped by θ^{-1}

is in $(\mathbb{Z}C_2)S_3$. It is not neccessary to re-write the original equations. The result after row reduction are the equations:

$$\begin{aligned} x_1 + x_2 &\equiv 0 \pmod 2 \\ x_2 &\equiv x_6 - x_5 \pmod 3 \\ x_1 \equiv x_3 + x_5 &\equiv x_4 + x_6 \pmod 3 \end{aligned}$$

At the risk of being repititious, we note that the above congruences are in $\mathbb{Z}C_2$. Namely that we are considering modulo the ideals generated by 2 or 3 in $\mathbb{Z}C_2$in the above equations.

Let ϕ denote the projection map of $\mathcal{R} \oplus \mathcal{R} \oplus \mathcal{R}_2$ onto $\mathcal{R}_2$. Then we have that

$$\phi\theta((\mathbb{Z}C_2)S_3) = \begin{pmatrix} x_3 & x_4 \\ x_5 & x_6 \end{pmatrix} : x_3 + x_5 \equiv x_5 + x_6 \pmod 3$$

Let us call the above set $\mathcal{Y}$.

Let us now pause for a moment to consider some of the properties of $\mathbb{Z}C_2$, where e is the identity of C_2 and η is the other element with $\eta^2 = e$. The units of the group ring $\mathbb{Z}C_2$ are easy to determine as they are only $\pm C_2$. Therefore, for a matrix to be in the units of $(intctwo)_2$ the determinant must be one of $\pm e$ or $\pm\eta$.

Let us continue. If $X = (x_1, \cdots, x_6)$ is in $\theta(\mathbb{Z}C_2)S_3$, then, if we let δ represent any one of $\pm e, \pm\eta$, then as was calculated before, we have that X^{-1} exists and is in $\theta(\mathbb{Z}C_2)S_3$ if and only if

$$x_3x_6 - x_4x_5 = \delta, x_1 = \delta, \qquad x_2 = \pm\delta.$$

The mapping $\phi\theta$ is a ring homomorphism of $(\mathbb{Z}C_2)S_3$ into $\mathcal{Y}$ and thus induces a homorphism from $\mathcal{U}(\mathbb{Z}C_2)S_3 \to \mathcal{U}\mathcal{Y}$. I conjecture that this is an isomorphism onto. To see this let

$$\mu = \begin{pmatrix} x_3 & x_4 \\ x_5 & x_6 \end{pmatrix} \in \mathcal{U}\mathcal{Y}.$$

Then $\delta = x_3x_6 - x_4x_5 = \pm e$ or $\pm\eta$ and if we choose x_1, x_2 which are in $\{e, 0, -e, \eta, -\eta\}$ to satisfy

$$\begin{aligned} x_2 &\equiv x_6 - x_5 \pmod 3 \\ x_1 &\equiv x_3 + x_5 \pmod 3, \end{aligned}$$

it follows from this that neither x_1 nor x_2 is 0 and that the above conditions are all satisfied. Thus $\alpha = \theta^{-1}X$ is a unit in $(\mathbb{Z}C_2)S_3$ with $\phi\theta\alpha = \mu$. Furthermore, we can see that from the preceding conditions that $\phi\theta$ is one-to-one.

Therefore, remembering that $\mathbb{Z}D_6 \cong (\mathbb{Z}C_2)S_3$ and that $\mathcal{U}\mathbb{Z}D_6 \cong \mathcal{U}(\mathbb{Z}C_2)S_3$ we have the following theorem.

Theorem 3.3.

$$\mathcal{U}\mathbb{Z}D_6 \cong \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{U}\mathbb{Z}C_2 : a + c \equiv b + d \pmod 3 \right\}.$$

3.4 The Unit Group of $\mathbb{Z}A_4$,(expository)

In this section, we will present the charachterization of $\mathcal{U}\mathbb{Z}A_4$ as presented by Allen and Hobby[1]. We will not include the proofs, as it is felt that nothing new is to be gained from rehashing the method.

As is known A_4 has 4 irreducible representations, call them $\theta_i, i = 1, 2, 3, 4$. Also A_4 is generated by the two elements $a = (12)(34)$ and $b = (123)$. The representations $\theta_i, i = 1, 2, 3$ are easily described as follows. $\theta_i(a) = 1$ and $\theta_i(b) = \omega^{i-1}$. The fourth, θ_4 is given as follows

$$\theta_4(a) = \begin{bmatrix} -1 & 0 & 1 \\ -1 & 0 & 1 \\ -1 & 1 & 0 \end{bmatrix} \text{ and}$$

$$\theta_4(b) = \begin{bmatrix} -1 & 1 & 0 \\ -1 & 0 & 0 \\ -1 & 0 & 1 \end{bmatrix}$$

Let $\theta : \mathbb{Q}A_4 \to \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}_3$ be defined by $\theta(r) = (\theta_1(r), \theta_2(r), \theta_3(r), \theta_4(r))$. Then we may use this map as in the preceding sections to determine the unit group. The characterization arrived at by Allen and Hobby is as follows.

Theorem 3.4.

$$\mathcal{U}\mathbb{Z}A_4 \cong \{\pm 1\} \times \{X \in SL(3, \mathbb{Z})\}$$

where X satisfies the below conditions 1), 2) and 3)

- *Every column sum of X is congruent to* $1 \pmod 4$.
- *No row contains all odd elements.*
- *One pseudo-trace is congruent to* $-1 \pmod 4$ *while the other two are congruent to* $0 \pmod 4$.

There are three pseudo-traces on a three by three matrix, they are the sums of the elements on the pseudo-diagonals that have been discussed previously.

Chapter 4

Groups of order 27

In this section, we will use the method presented earlier in the paper to determine the unit group of the integral group rings of the two non-commutative groups of order 27.

The structures of these two groups are:

$$G = \langle a, b | (a, b) = c, ca = ac, cb = bc, a3 = b^3 = c^3 = 1\rangle, \text{ and}$$
$$H = \langle a, b | a^9 = b^3 = 1, b^{-1}ab = a^4\rangle.$$

As is true in general, we have that $\widetilde{G} = \langle\tilde{a}\rangle \times \langle\tilde{b}\rangle$, and $\widetilde{H} = \langle\tilde{a}\rangle \times \langle\tilde{b}\rangle$ are both elementary abelian 3-groups. Also, it is well known that $\mathcal{U}\mathbb{Z}\tilde{G} = \pm\tilde{G}$ and $\mathcal{U}intgr\tilde{H} = \pm\tilde{H}$. The object of this section is to give a concrete description of both $\mathcal{U}\mathbb{Z}G$ and $\mathcal{U}\mathbb{Z}H$.

4.1 First group of order 27.

Let us consider G first. Referring back to our general proof we would let $A = \mathrm{DIAG}(1, \omega, \omega^2)$ and $B = \mathrm{PDIAG}_1$. Our fibre product diagram would become

$$\begin{tikzcd}
\mathbb{Z}G \arrow[r] \arrow[d] & \mathbb{Z}\tilde{G} \arrow[d] \\
\mathbb{Z}[\omega]^\circ\tilde{G} \cong \mathbb{Z}G/\tilde{c}\mathbb{Z}G \arrow[r] \arrow[d, "\phi_0"'] & (\mathbb{Z}/3\mathbb{Z})\tilde{G} \\
S_p \arrow[ur, "\phi_1"] &
\end{tikzcd}$$

The maps ϕ_0 and ϕ_1 are defined in the same way as they were in general.

Specializing the condition (*) from the general theorem we see that the matrix

$$M = \begin{bmatrix} x_{0,0} & x_{1,0} & x_{2,0} \\ x_{2,1} & x_{0,1} & x_{1,1} \\ x_{1,2} & x_{2,2} & x_{0,2} \end{bmatrix} \in \mathbb{Z}[\omega]_3$$

belongs to our S_p if and only if for each $i, 0 \leq i \leq 2$, the conditions

$$\begin{aligned} x_{i,0} + x_{i,1} + x_{i,2} \in & \quad 3\mathbb{Z}[\omega] \\ x_{i,0} + x_{i,1}\omega + x_{i,0}\omega^2 \in & \quad 3\mathbb{Z}[\omega] \\ x_{i,0} + x_{i,1}\omega^2 + x_{i,2}\omega \in & \quad 3\mathbb{Z}[\omega] \end{aligned}$$

hold. To find $\phi_1(M)$, we need $a_{i,j} \in \mathbb{Z}[\omega]$ such that $M = \sum a_{i,j} A^i B^j$. This will give us the matrix equations

$$\begin{bmatrix} a_{0,j} \\ a_{1,j} \\ a_{2,j} \end{bmatrix} = \frac{1}{3} \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega^2 & \omega \\ 1 & \omega & \omega^2 \end{bmatrix} \begin{bmatrix} x_{j,0} \\ x_{j,1} \\ x_{j,2} \end{bmatrix}$$

and this is equivalent to

$$\begin{aligned} a_{0,j} &= \frac{1}{3}(x_{j,0} + x_{j,1} + x_{j,2}) \\ a_{1,j} &= \frac{1}{3}(x_{j,0} + \omega^2 x_{j,1} + \omega x_{j,2}) \\ a_{2,j} &= \frac{1}{3}(x_{j,0} + \omega x_{j,1} + \omega^2 x_{j,2}) \end{aligned} \tag{4.1}$$

From our previous work we know that $\phi_1(M) = \sum \tilde{a}_{i,j} \tilde{a}^i \tilde{b}^j$. Also, we know that the units of $\mathbb{Z}G$ are pairs (α, M), with $\alpha \in \mathcal{U}\mathbb{Z}\tilde{G}$ and M in S_p with $\phi_1(M) = \phi_2(\alpha)$. However, since we know that $\mathcal{U}\mathbb{Z}\tilde{G} = \pm\tilde{G}$, we need matrices M such that

$$\phi_1(M) = \sum \tilde{a}_{i,j} \tilde{a}^i \tilde{b}^j = \theta_2(\pm a^m b^n)$$

for some m, n. If we put $\pi = \omega - 1$ we then get

- For two values of i and all j, $a_{i,j} \equiv 0 \pmod{\pi}$.
- Considering the third value for i, either

$$\begin{aligned} a_{i,0} &= \pm 1, & a_{i,1} &\equiv a_{i,2} \equiv 0 \pmod{\pi} \text{ or} \\ a_{i,1} &= \pm 1, & a_{i,0} &\equiv a_{i,2} \equiv 0 \pmod{\pi} \text{ or} \\ a_{i,2} &= \pm 1, & a_{i,1} &\equiv a_{i,1} \equiv 0 \pmod{\pi} \end{aligned}$$

This proves the following theorem.

Theorem 4.1.

$\mathcal{U}\mathbb{Z}G \cong \{M \in \mathcal{U}\mathbb{Z}[\omega]_3 | M$ satisfies 1. and 2. above where the $a_{i,j}$ are given by equation 4.1$\}$

From the above it is clear that the matrices in $\mathcal{U}\mathbb{Z}[\omega]_3$ which are congruent to $I \pmod{\pi^3}$ are contained in $\mathcal{U}\mathbb{Z}G$ and therefore, $\mathcal{U}\mathbb{Z}G$ is a congruence subgroup in $SL(3, \mathbb{Z}[\omega])$.

4.2 Second group of order 27.

Now, let us describe $\mathcal{U}\mathbb{Z}H$ If we have a matrix

$$X = Z' = \begin{bmatrix} x_{0,0} & x_{1,0} & x_{2,0} \\ x_{2,1} & x_{0,1} & x_{1,1} \\ x_{1,2} & x_{2,2} & x_{0,2} \end{bmatrix}$$

satisfying (*) then the corresponding matrix in S_p is

$$Z = \begin{bmatrix} x_{0,0} & x_{1,0} & x_{2,0} \\ \omega x_{2,1} & x_{0,1} & x_{1,1} \\ \omega x_{1,2} & \omega x_{2,2} & x_{0,2} \end{bmatrix}$$

If we write $A = \sum a_{i,j} B^i A^j$, then $\phi_1(Z) = \pm h, h \in H$ if and only if the matrix X satisfies 1. and 2. from above. Then we have the the following theorem.

Theorem 4.2.

$\mathcal{U}\mathbb{Z}H \cong \left\{ Z \in \mathcal{U}\mathbb{Z}[\omega]_3 | Z' \text{ satisfies 1. and 2. above where the } a_{i,j} \text{ are given by equation 4.1} \right\}$

Appendix A

Definitions

Definition A.1. *G is an* abelian group *when all elementsts of G commute.*

Definition A.2. *G is* Hamiltonian *when it is non-abelian and where each subgroup is normal. All such groups are of the form $G = Q_8 \times E \times D$ where Q_8 is the quaternion group of order 8, D is a torsion group and E is a direct sum of a finite number of copies of the cyclic group C_2. A Hamiltonian 2-group is a group of the form $Q_8 \times E$ where $E^2 = 1$).*

Definition A.3. *N is a* normal *subgroup of G when it is invariant under conjugation. That is $\forall g \in G, n \in N, g^{-1}ng \in N$.*

Definition A.4. *A non-abelian group of size 8 denoted as Q_8 with the elements $\{1, -1, i, -i, j, -j, k, -k\}$ where $i^2 = j^2 = k^2 = ijk = -1$ and $(-1)x = x(-1) = -x \; \forall x \in Q_8$. This is a Hamiltonian group and is included in all Hamiltonian groups.*

Definition A.5. *G is a* torsion group *when it is an abelian group and every element of G has finite order. This is sometimes referred to as* periodic.

Bibliography

[1] P. J. Allen and C. Hobby. A characterization of units in $\mathbb{Z}[A_4]$. *Journal of Algebra*, 66:534–543, 1980.

[2] I. Hughes and K. R. Pearson. The group of units of the integral group ring $\mathbb{Z}S_3$. *Canadian Mathematics Bulletin*, 15:529–534, 1972.

[3] I. S. Luthar. Units in integral group rings. *to appear*, 1981.

[4] C. Polcino-Milies. The units of the integral group ring $\mathbb{Z}D_4$. *Bol. Soc. Brasil. Mat*, 4:85–92, 1972.

[5] J. Ritter and S.K. Sehgal. Integral group rings of some p-groups. *to appear*, 1981.

[6] Sudarshan K. Sehgal. *Topics in Group Rings*. Marcell Dekker, Inc., 270 Madison Avenue, New York, 1978. ISBN 0-8247-6755-1.