

Pythagorean Triples and Units in Integral Group Rings

M. Beattie and C. Weatherby
Department of Mathematics and Computer Science
Mount Allison University
Sackville, N.B., Canada E4L 1E6 *

Abstract

In this note, we describe a simple method for finding units of group rings of the form $\mathbf{Z}[G] = \mathbf{Z}[H] \# \mathbf{Z}[C_2]$ for H an abelian group, and apply this to the case $G = D_4$, the dihedral group of order 8. Here, units may be described as integer points on hyperboloids, and, defining units u, v to be equivalent if they differ by an inner automorphism, we see that this equivalence relation partitions each hyperboloid into finitely many classes.

1 Introduction and Preliminaries

In a short note in 1990, Goodaire, Jespers and Parmenter [3] described an elementary method for finding the units in the integral group ring $\mathbf{Z}[G]$ where G is a finite group such that $G/Z(G) \cong C_2 \times C_2$ and G/G' and $Z(G)$ each have exponent 2,3,4 or 6, by finding solutions to certain Diophantine equations. In following work, Jespers and Leal described the nontrivial units in $\mathcal{U}(\mathbf{Z}[D_4])$ very concretely [6, Theorem 4.3]. In this note, we describe an equally straightforward method for finding units in $\mathbf{Z}[G]$ where G is a group such that $\mathbf{Z}[G] \cong \mathbf{Z}[H] \# \mathbf{Z}[C_2]$, H abelian. In particular, this method is useful if $G = D_n$, the dihedral group of order $2n$ and if the units of $\mathbf{Z}[C_n]$ are known. We expand upon these ideas for the case $G = D_4$, and develop an elementary geometrical interpretation of units as points with integer coefficients on a hyperboloid and relate this interpretation to the classical tree of primitive Pythagorean triples.

*The first author has support from NSERC and the second was funded by an NSERC USRA at Mount Allison University, 2003.

We write $\mathbf{Z}[G]$ for the integral group ring of a group G . We write g for both the group element $g \in G$ and for the trivial unit corresponding to g in $\mathbf{Z}[G]$. As usual, we denote the units of $\mathbf{Z}[G]$ by $\mathcal{U}(\mathbf{Z}[G])$, and we let $V = V(\mathbf{Z}[G])$ denote the group of units with augmentation 1. See [8], [10], [11] for notation and definitions.

2 The group of units of $\mathbf{Z}[H] \# \mathbf{Z}[C_2]$

Our first result follows directly from the duality results of Cohen and Montgomery [2] and is similar to the ideas for constructing units in the NSERC USRA project of P. Moore [9] in 1991. We recall the setting for the duality theorem for actions.

Let G be a finite group of order n and let G act as a group of automorphisms on a k -algebra S (k a commutative ring). Then the skew group ring $S \# k[G]$ has a natural G -grading, i.e., a $k[G]^*$ -action so that we may form $(S \# k[G]) \# k[G]^*$. We write p_g , $g \in G$, for the element of $k[G]^*$ such that $p_g(h) = \delta_{g,h}$. The p_g are a basis for $k[G]^*$. Note that the multiplicative identity in $k[G]^*$ is $\epsilon = \sum_{g \in G} p_g$.

Theorem 2.1 [2, Theorem 3.2] [1] *For S, G as above, $(S \# k[G]) \# k[G]^* \cong M_n(S)$. In fact the ring isomorphism $\phi : S \# k[G] \# k[G]^* \rightarrow M_n(S)$ is defined by $\phi(s \# h \# p_g) = ((hg)^{-1} \rightarrow s) E_{hg,g}$ where $E_{a,b}$ is the matrix with a 1 in the a^{th} row and b^{th} column, and zeroes elsewhere.*

Now let H be an abelian group with a C_2 -action and let $G = H * C_2$ so that $\mathbf{Z}[G] \cong \mathbf{Z}[H] \# \mathbf{Z}[C_2]$ and we can describe $\mathcal{U}(\mathbf{Z}[G])$ as a group of matrices with entries from $\mathbf{Z}[H]$. We let x be the generator for C_2 and for $\alpha \in \mathbf{Z}(H)$ we write $\bar{\alpha}$ for x acting on α , i.e., $\bar{\alpha} = x\alpha x$. Note that $\mathbf{Z}[H] \# \mathbf{Z}[C_2] \# \epsilon \cong \mathbf{Z}[H] \# \mathbf{Z}[C_2]$. Also for $\alpha, \beta \in \mathbf{Z}[H]$, $\phi(\alpha + \beta x) = \begin{bmatrix} \alpha & \beta \\ \bar{\beta} & \bar{\alpha} \end{bmatrix}$.

Theorem 2.2 *Let \mathcal{D} be the image of $\mathbf{Z}[G]$ under ϕ so that the unit group of $\mathbf{Z}[G]$ is isomorphic to the group of matrices in \mathcal{D} with determinant a unit in $\mathbf{Z}[H]$, i.e., $\mathcal{U}(\mathbf{Z}[G]) = \{u = \alpha + \beta x \mid \alpha \bar{\alpha} - \beta \bar{\beta} \in \mathcal{U}(\mathbf{Z}[H])\}$. If $u = \alpha + \beta x \in \mathcal{U}(\mathbf{Z}[G])$ with $\alpha \bar{\alpha} - \beta \bar{\beta} = w \in \mathcal{U}(\mathbf{Z}[H])$ then $u^{-1} = w^{-1}(\bar{\alpha} - \beta x)$.*

Corollary 2.3 *If $u = \alpha + \beta x$ has order n or infinite order in $\mathcal{U}(\mathbf{Z}[H] \# \mathbf{Z}[C_2])$ with $\det(\phi(u)) = 1$, then u and x generate a subgroup of $\mathcal{U}(\mathbf{Z}[G])$ isomorphic to a dihedral group D_n or D_∞ if and only if $\bar{\beta} = -\beta$. If $\det(\phi(u)) = -1$, then $xux = u^{-1}$ if and only if $\alpha = 0$ and $\beta = \bar{\beta}$.*

3 Units in $\mathbf{Z}[D_4]$.

In this section, we discuss $V = V(\mathbf{Z}[D_4])$, the group of units of augmentation 1 in $\mathbf{Z}[D_4]$. The characterization of units in (4) and (5) below appears in [3], see also [8, 8.2, Exercise 4]. Let D_4 be generated by x, y with $x^2 = y^4 = e$ and $xyx = y^3$. Let $u \in \mathbf{Z}[D_4]$ with

$$u = (a + by + cy^2 + dy^3) + (e + fy + gy^2 + hy^3)x = \alpha + \beta x. \quad (1)$$

Since $\{e, y^2\} = Z(D_4)$, the centre of D_4 , there is a ring homomorphism $\lambda: \mathbf{Z}[D_4] \rightarrow \mathbf{Z}[D_4]/\mathbf{Z}[Z(D_4)] \cong \mathbf{Z}[C_2 \times C_2]$ given by $\lambda(u) = (a + c) + (b + d)Y + (e + g)X + (f + h)XY$ where X, Y are the images of x, y in the factor group $D_4/Z(D_4) \cong C_2 \times C_2$. Since $\mathbf{Z}[C_2 \times C_2]$ has only trivial units [4], we then have four possible cases for units with augmentation 1, namely one of $a + c, b + d, e + g, f + h$ is 1 and the remaining 3 sums are 0. We denote the subsets of these units in V by V_i with $1 \leq i \leq 4$ respectively. Note that $y^2V_i = V_i$ for all i , and also

$$V_2 = yV_1 = V_1y; \quad V_3 = xV_1 = V_1x; \quad V_4 = yxV_1 = V_1yx. \quad (2)$$

Thus these sets are in bijective correspondence. Therefore, up to multiplication with a trivial unit, we may assume that elements of V lie in V_1 , i.e.,

$$a + c = 1, \quad b + d = e + g = f + h = 0. \quad (3)$$

For $u \in V$, it follows directly from (3) that

$$u \in V_1 \text{ iff } u = 1 + \gamma(1 - y^2) \text{ where } \gamma = -c + by + ex + fyx. \quad (4)$$

Now let $u = \alpha + \beta x \in V_1$. By the results of Section 2, $\alpha\bar{\alpha} - \beta\bar{\beta}$ is a unit in $\mathbf{Z}[C_4]$ fixed by the action of x . Since $\mathbf{Z}[C_4]$ has only trivial units [4], $\alpha\bar{\alpha} - \beta\bar{\beta} = \pm 1$ or $\pm y^2$.

By (4), $\alpha\bar{\alpha} - \beta\bar{\beta} = (1 + 2\delta) - (2\delta)y^2$ where $\delta = b^2 + c^2 - e^2 - f^2 - c$. Since δ is an integer, we must have that $\delta = 0$, that is, $\alpha\bar{\alpha} - \beta\bar{\beta} = \det(\phi(u)) = 1$, and

$$e^2 + f^2 - b^2 = c(c - 1) = -ac. \quad (5)$$

Remark 3.1 Note that $\phi(y) = \begin{bmatrix} y & 0 \\ 0 & y^3 \end{bmatrix}$ and $\phi(x) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Thus for $u \in V_1 \cup V_2$, $\det(\phi(u)) = 1$ and $V_1 \cup V_2$ is a normal subgroup of V of index 2. Similarly, $\det(\phi(u))$ for u in V_3 or V_4 is -1.

Since $-ac \geq 0$, (5) shows that all units in V_1 lie on a surface $X^2 + Y^2 - Z^2 = -ac$ which is a hyperboloid of one sheet if $ac \neq 0$ and a cone if $ac = 0$. Let H_k denote the set of integer points on the hyperboloid $X^2 + Y^2 = Z^2 + k$.

Let \mathcal{H}_n denote the units with $c = n$ on $H_{n(n-1)}$. A point (e, f, b) in \mathcal{H}_c is identified with the unit $u = 1 + \gamma(1 - y^2)$ with $\gamma = -c + by + ex + fyx$ as in (4). Given any value of c , \mathcal{H}_c is nonempty. Since $c(1 - c) = 2mn$ for integers m, n , then, $b = m + n, e = m, f = n$ satisfies (5).

Then we may identify V_1 with $\cup_{c \in \mathbf{Z}} \mathcal{H}_c$, i.e. V_1 is identified with the set of two copies of each hyperboloid $H_{n(n-1)}$. One copy of $H_{n(n-1)}$ corresponds to the units with $c = n$ and the other to the units with $c = 1 - n$.

The following proposition gives the multiplication for units in V_1 .

Proposition 3.2 *Let $u = (e, f, b) \in \mathcal{H}_c$ and $v = (e', f', b') \in \mathcal{H}_{c'}$. Then $uv = (e'', f'', b'') \in \mathcal{H}_{c''}$ where*

$$\begin{aligned} c'' &= c + c' + 2bb' - 2cc' - 2ee' - 2ff' \\ &= (b + b')^2 + (c - c')^2 - (e + e')^2 - (f + f')^2; \\ b'' &= (1 - 2c')b + (1 - 2c)b' + 2fe' - 2ef'; \\ e'' &= (1 - 2c')e + (1 - 2c)e' + 2b'f - 2bf'; \\ f'' &= (1 - 2c')f + (1 - 2c)f' + 2be' - 2eb'. \end{aligned}$$

Proof. The proof is by direct computation, using (5) in order to see the second formula for c'' . ■

The multiplication formula in Proposition 3.2 may be interpreted as

$$\begin{bmatrix} e'' \\ f'' \\ b'' \end{bmatrix} = (1 - 2c') \begin{bmatrix} e \\ f \\ b \end{bmatrix} + (1 - 2c) \begin{bmatrix} e' \\ f' \\ b' \end{bmatrix} + 2 \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix} \left(\begin{bmatrix} e \\ f \\ b \end{bmatrix} \times \begin{bmatrix} e' \\ f' \\ b' \end{bmatrix} \right).$$

Thus $u, v \in V_1$ commute if and only if they represent parallel vectors in \mathbf{Z}^3 .

Corollary 3.3 *V_1 is a normal subgroup of V and V/V_1 is isomorphic to the Klein 4-group.*

Proof. Proposition 3.2 shows that V_1 is a subgroup and the rest of the statement follows from (2). ■

Let $\mathcal{H} = \cup_{n \in \mathbf{Z}} \mathcal{H}_{2n}$, i.e., \mathcal{H} is the set of units in V_1 with c even and can be identified with the set of integer points on the hyperboloids $H_{2n(2n-1)}$, $n \in \mathbf{Z}$.

Corollary 3.4 \mathcal{H} , the set of units with c even, is a subgroup of V_1 , and $V_1 \cong \mathcal{H} \times Z(V_1)$, where $Z(V_1) = \{1, y^2\}$.

Corollary 3.5 For $u = (e, f, b) \in \mathcal{H}_c$, $u^{-1} = (-e, -f, -b) \in \mathcal{H}_c$, so \mathcal{H}_c is closed under taking inverses.

Now we show that if u is a nontrivial unit in V_1 , then the subgroup generated by u is isomorphic to \mathbf{Z} and consists of points with integer coordinates on a line through the origin. If $u \in \mathcal{H}_0$, then this line lies on the cone; otherwise the subgroup will lie on a line intersecting infinitely many hyperboloids.

Theorem 3.6 Let $u = (e, f, b) \in \mathcal{H}_c$ and let $u^n = (e_n, f_n, b_n) \in \mathcal{H}_{c_n}$. For n a positive integer, $(e_n, f_n, b_n) = \alpha_n(e, f, b)$ for some integer α_n with $\alpha_1 = 1, \alpha_2 = 2(1 - 2c)$, etc. Furthermore the sequence $|\alpha_1|, |\alpha_2|, \dots$ is strictly increasing. For n a positive integer, $c_n = \beta_n c$ for some integer β_n where $\beta_1 = 1, \beta_2 = 4a$, etc. If $ac \neq 0$, then the sequence $|\beta_1|, |\beta_2|, \dots$ is strictly increasing. If $c = 0$, then $c_n = 0$ for all n . If $a = 0, c = 1$, then $c_n = 0$ if n is even, and $c_n = 1$ if n is odd.

Proof. We show first that $(e_n, f_n, b_n) = \alpha_n(e, f, b)$ and $c_n = \beta_n c$ for integers α_n, β_n . The proof is by induction on n . If $n = 2$, then by Proposition 3.2, $\alpha_2 = 2(a - c) = 2(1 - 2c)$. Now suppose that for $n = k - 1$, $(e_{k-1}, f_{k-1}, b_{k-1}) = \alpha_{k-1}(e, f, b)$. Then again, by Proposition 3.2, $(e_k, f_k, b_k) = ((1 - 2c_{k-1}) + (1 - 2c)\alpha_{k-1})(e, f, b)$. Similarly, since $c_2 = 4ac$, again using induction on n , we suppose $c_{k-1} = \beta_{k-1}c$. Then $c_k = c + \beta_{k-1}(1 - 2c)c + 2\alpha_{k-1}ac$ so that $\beta_k = 1 + \beta_{k-1}(1 - 2c) + 2a\alpha_{k-1}$.

Now suppose that $ac \neq 0$, so that $|a - c| > 1$. Note that we have shown that

$$\alpha_n = 1 - 2\beta_{n-1}c + (1 - 2c)\alpha_{n-1}; \quad (6)$$

$$\beta_n = 1 + \beta_{n-1}(1 - 2c) + 2a\alpha_{n-1}. \quad (7)$$

Next we claim that for $n \geq 2$, α_n and β_n have the same sign and $|\alpha_n| > |\alpha_{n-1}|, |\beta_n| > |\beta_{n-1}|$. We note that $\alpha_1 = 1, \beta_1 = 1, \alpha_2 = 2(a - c), \beta_2 = 4a$ and proceed by induction. Suppose that α_{k-1} and β_{k-1} have the same sign. Since $-2c, a - c$ and $2a$ all have the same sign, then the summands $-2c\beta_{k-1}, (a - c)\alpha_{k-1}, (a - c)\beta_{k-1}, 2a\alpha_{k-1}$ in (6), (7) have the same sign. If these are positive, then clearly α_k, β_k are positive and greater than $|\alpha_{k-1}|, |\beta_{k-1}|$. If the summands all are negative then since $|2c\beta_{k-1}| > 1$ and $|2a\alpha_{k-1}| > 1$, we still have that $|\alpha_k|, |\beta_k|$ are greater than $|\alpha_{k-1}|, |\beta_{k-1}|$ respectively.

Now let $ac = 0$. If $c = 0$, then the multiplication formula in Proposition 3.2 immediately yields that $\alpha_n = n, c_n = 0$ for all n . If $c = 1$, then again

by Proposition 3.2 and a simple induction argument, the sequence of α_n is $1, -2, 3, -4, \dots$ and the sequence of integers c_n is $1, 0, 1, 0, 1, \dots$ ■

Corollary 3.7 *The only units of finite order in V_1 are the trivial units 1 and y^2 . Any unit of finite order in V_2, V_3, V_4 has order 2 or 4.*

The next theorem describes the units of finite order in V_2, V_3 and V_4 in an elementary way. See also [7].

Theorem 3.8 (i) *The set $V_2 = yV_1$ has no units of order 2, but has nontrivial units of order 4. A unit $u \in V_2, u = y^3 + \gamma(1 - y^2)$ with $\gamma = a + by + ex + fyx$ is of order 4 if and only if $a = 0$ and (e, f) is an integer point on the circle $X^2 + Y^2 = b(b - 1)$.*

(ii). *The sets V_3 and V_4 have no units of order 4, but have nontrivial units of order 2. For $u = y^2x + \gamma(1 - y^2)$ in V_3 , γ as above, then u has order 2 if and only if $a = 0$, and (b, f) is a point on the hyperbola $X^2 - Y^2 = e^2 - e$. For $u = y^3x + \gamma(1 - y^2)$ in V_4 , γ as above, then u has order 2 if and only if $a = 0$, and (b, e) is a point on $X^2 - Y^2 = f^2 - f$.*

Proof. (i) Let $u = \alpha + \beta x \in V_2$ as in (1). Suppose first that $u^2 = 1$. Theorem 2.2 implies that $\alpha = \bar{\alpha}, \beta = -\beta$. Thus $b = d$, contradicting $b + d = 1$. Now let $u^2 = y^2 = u^{-2}$. This implies that $\alpha^2 = \bar{\alpha}^2$, and so that either $b = d$, a contradiction, or $a = c = 0$. Straightforward computation shows that if $a = c = 0$, $u^2 = y^2$ if and only if $e^2 + f^2 = b^2 - b$.

(ii) Now let $u = \alpha + \beta x \in V_3$ as in (1). Suppose first that $u^2 = y^2$. For $u \in V_3$, $\det(\phi(u)) = -1$, so that $u^{-1} = -\bar{\alpha} + \beta x$. Then $u^2 = u^{-2}$ implies as above that either $b = d = 0$ or $a = c = 0$. If $a = c = 0$, again as above, $e^2 + f^2 = b(b - 1)$. But the left side of this equation is odd, the right side is even, so this is impossible. A similar contradiction arises if $b = d = 0$. Now suppose that $u = u^{-1}$. Then $\alpha = -\bar{\alpha}$, or equivalently $a = 0$, and $\alpha\bar{\alpha} = \beta\bar{\beta} + 1$, or equivalently $b^2 = f^2 + e^2 - e$.

The argument for V_4 is similar. ■

Remark 3.9 *A subgroup of $V(\mathbf{Z}[D_4])$ isomorphic to the Klein 4-group K must be generated by y^2 and a unit of order 2 in V_3 or V_4 . For suppose u, v generate a copy of K with $u \in V_3$ and $v \in V_4$. Then $uv \in V_2$ which has no units of order 2. Thus u, v both lie in V_3 or V_4 , and $uv = y^2$.*

4 Integer points on a hyperboloid

We now describe a method for finding integer points on H_k for various k based on “growing the tree of primitive Pythagorean triples from $(3,4,5)$ ”.

A point $P = (a, b, c) \in H_0$ satisfies $x^2 + y^2 = z^2$. If a, b, c are positive, then (a, b, c) is called a Pythagorean triple. Every Pythagorean triple is a multiple of a primitive Pythagorean triple, i.e. one in which $\gcd(P) = \gcd(a, b, c) = 1$. In order to construct all primitive Pythagorean triples, it suffices to find all primitive Pythagorean triples (a, b, c) with a, c odd and b even, since all others are obtained by switching a, b . The “tree” of such triples with a, b, c positive grown from the “seed” $(3, 4, 5)$ is well known; we review its construction.

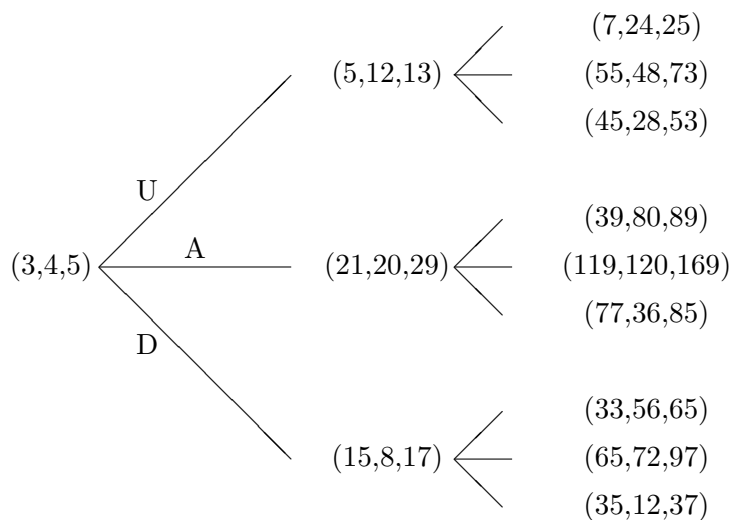
Let $I_i, i = 1, 2, 3$, and $I_{1,2}$ be the matrices representing reflections in the planes $X = 0, Y = 0, Z = 0$ and $X = Y$ respectively.

Let U, A, D be the transformations with matrices

$$A = \begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{bmatrix}, \quad U = AI_2, \quad D = AI_1, \quad I_3AI_3 = A^{-1}, \quad I_{1,2}AI_{1,2} = A. \quad (8)$$

The reflections $I_i, I_{1,2}$ and A preserve $x^2 + y^2 - z^2$, and so map H_k to H_k . As well, they preserve the parity of each of x, y, z and $\gcd(x, y, z)$.

The tree of primitive Pythagorean triples (a, b, c) with a, c odd and b even is constructed by applying U, A, D to the triple $(3,4,5)$, then to $U(3,4,5) = (5, 12, 13)$, etc, so that each branching of the tree has 3 limbs. The first few branches of the tree are given below:



Theorem 4.1 [5] *Every primitive Pythagorean triple with a odd and b even, appears exactly once in this tree.*

We construct the integer points on H_k , $k \neq 0$, in a similar manner. Let \mathcal{G} be a group of linear transformations on \mathbf{Z}^3 which maps H_k to itself. We define an equivalence relation $\sim_{\mathcal{G}}$ on H_k by $P \sim_{\mathcal{G}} Q$ if and only if $Q = T(P)$ for some $T \in \mathcal{G}$. Denote the equivalence class of P by $[P]_{\mathcal{G}}$.

Now define groups of transformations on H_k as follows:

- (i) Let \mathcal{R} be generated by $I_{1,2}, I_i, i = 1, 2, 3$. $\mathcal{R} \cong D_4 \times C_2$.
- (ii) Let \mathcal{R}' be generated by I_3 and $I_{1,2}$. $\mathcal{R}' \cong C_2 \times C_2$.
- (iii) Let \mathcal{A}' be generated by the U, A, D or equivalently by A, I_1, I_2 .
- (iv) Let \mathcal{A} be generated by \mathcal{A}' and \mathcal{R}' .

Since $A(1, 0, 1) = (3, 4, 5)$, Theorem 4.1 yields the following.

Theorem 4.2 $H_0 = \bigcup_{n \geq 0} [n(1, 0, 1)]_{\mathcal{A}}$.

Lemma 4.3 $Q \in [P]_{\mathcal{A}}$ if and only if $Q = TR(P)$ for some $R \in \mathcal{R}', T \in \mathcal{A}'$.

Proof. This follows directly from the commutation relations in (8). ■

Let $(x, y, z) \in H_k$ with k not a square and $x = 2m + 1$ odd. Then $0 \neq t = z - y$. Letting $s = z + y$, we have $ts = x^2 - k$. We identify points with x odd in H_k with the set of pairs $\mathcal{P}_k = \{(m, t) | m \in \mathbf{Z}, t \text{ divides } (2m + 1)^2 - k\}$ via

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 2m + 1 \\ \frac{(2m+1)^2 - k - t^2}{2t} \\ \frac{(2m+1)^2 - k + t^2}{2t} \end{bmatrix} = \begin{bmatrix} 2m + 1 \\ \frac{s-t}{2} \\ \frac{s+t}{2} \end{bmatrix}.$$

Now identify points $(x, y, z) \in H_k$ with $x = 2m$ even, k not a square, in a similar way with the set of pairs $\mathcal{Q}_k = \{(m, t) | m \in \mathbf{Z}, t \text{ divides } (2m)^2 - k\}$ via

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 2m \\ \frac{(2m)^2 - k - t^2}{2t} \\ \frac{(2m)^2 - k + t^2}{2t} \end{bmatrix} = \begin{bmatrix} 2m \\ \frac{s-t}{2} \\ \frac{s+t}{2} \end{bmatrix}.$$

The linear transformations U, A, D on H_k define maps (which we also denote U, A, D) on \mathcal{P}_k and \mathcal{Q}_k , by

$$U(m, t) = (m + t, t) \text{ and } A(m, t) = (m + s, s) \text{ for } (m, t) \in \mathcal{P}_k \text{ or } \mathcal{Q}_k;$$

$$D(m, t) = (s - m - 1, s) \text{ for } (m, t) \in \mathcal{P}_k;$$

$$D(m, t) = (s - m, s) \text{ for } (m, t) \in \mathcal{Q}_k.$$

Remark 4.4 Note that if $(m, t) \in \mathcal{P}_k$ or \mathcal{Q}_k corresponds to $(x, y, z) \in H_k$, then (m, s) corresponds to $(x, -y, z)$, $(m, -t)$ corresponds to $(x, -y, -z)$.

Remark 4.5 Note that if k is a square, say $k = K^2$, then any point $(\pm K, y, y)$ lies on H_k so that the bijective correspondence between H_k and $\mathcal{P}_k \cup \mathcal{Q}_k$ fails.

Lemma 4.6 Let $P = (x, y, z) \in H_k$.

(i) If $k \equiv 0 \pmod{4}$, then either x, y, z are all even (and thus $\gcd(P) \geq 2$), or z is odd, and x, y have different parity.

(ii) If $k \equiv 1 \pmod{4}$, then either x, y, z are all odd, or z is even and x, y have different parity.

(iii) If $k \equiv 2 \pmod{4}$, then z must be even and x, y both odd.

(iv) If $k \equiv 3 \pmod{4}$, then z must be odd and x, y both even.

Proof. Note that $(2m + 1)^2 \equiv 1 \pmod{4}$ and $(2m)^2 \equiv 0 \pmod{4}$. ■

Corollary 4.7 (i) If $\mathcal{P}_k \neq \emptyset$, then for any $m \in \mathbf{Z}$, there exists t such that $(m, t) \in \mathcal{P}_k$.

(ii) If $\mathcal{Q}_k \neq \emptyset$, then for any $m \in \mathbf{Z}$, there exists t such that $(m, t) \in \mathcal{Q}_k$.

Proof. (i) Let $\mathcal{P}_k \neq \emptyset$, $m \in \mathbf{Z}$, $x = 2m + 1$. If k is even, then $st = x^2 - k$ is odd, so that we may let $t = 1$, $s = x^2 - k$ to obtain values of y, z . If k is odd, then by Lemma 4.6, $k \equiv 1 \pmod{4}$ so that 4 divides $z^2 - y^2$ and we may choose $t = 2$ and s even.

The proof of (ii) is similar and uses the fact that here we cannot have $k \equiv 2 \pmod{4}$. ■

Theorem 4.8 Let k be a positive integer which is not a square. Let S_k be the set of points on H_k with $0 \leq x^2 \leq M_k$ where

$$M_k = \begin{cases} \max\{k - 4, 1\} & \text{if } k \equiv 1 \pmod{4} \\ \max\{k - 21, 1\} & \text{if } k \equiv 2 \pmod{4} \\ \max\{k - 15, 1\} & \text{if } k \equiv 3 \pmod{4} \\ \max\{k - 15, 1\} & \text{if } k \equiv 0 \pmod{4} \text{ and } x \text{ is odd.} \end{cases}$$

Then every point P in H_k with $\gcd(P) = 1$ is equivalent mod \mathcal{A} to a point in S_k .

Proof. By Corollary 4.7, if $\mathcal{P}_k(\mathcal{Q}_k)$ is nonzero so is $\mathcal{P}_k \cap S_k$ ($\mathcal{Q}_k \cap S_k$). Now let $P = (x, y, z) \in H_k$ with P corresponding to $(m, t) \in \mathcal{P}_k$, $\gcd(P) = 1$, and $x^2 > k$ so that s, t have the same sign. Since $I_1 \in \mathcal{A}$, we assume that $m > 0$. Now if $0 < |t| \leq m$, then apply a reflection if necessary so that t is negative, and then $U(m, t) = (m - |t|, t)$ and $0 \leq m - |t| < m$. If $0 < |s| \leq m$, then we apply I_2 to swap t and s and argue as above.

Assume s, t are positive. Suppose $0 < m < t$ and $0 < m < s$. If $t \geq 2m + 1$ and $s \geq 2m + 1$, then $st \geq (2m + 1)^2$. But $st = (2m + 1)^2 - k$, which is a contradiction. Say $s \leq 2m$, so that $0 < m < s \leq 2m$. If $m = 1$, then $s = 2$ and $D(m, t) = (0, 2)$. If $m > 1$, then $m < m + 1 < 2m$ and $|s - (m + 1)| < m$. So again $D(m, t)$ is a point $P' = (x', y', z')$ with $|x'| < |x|$.

The argument for a point $Q = (x, y, z)$ corresponding to $(m, t) \in \mathcal{Q}_k$ with $m > 0$ and $x^2 > k$ is similar. If $0 < t \leq m$ or $0 < s \leq m$, the argument is the same. If $t > m$ and $s > m$, then if both $s, t \geq 2m$, we have that $st \geq 4m^2$, contradicting $st = 4m^2 - k$. Say $m < s < 2m$. Then $m > 1$ and $|s - m| < m$. Then $D(m, t) = (s - m, s)$ has x coordinate smaller in absolute value.

Now let $x^2 < k$. If $x^2 = k - p$ where p is 1 or a prime, then $st = -p$ so that either $|t|$ or $|s|$ is 1. We may assume that $t = -1$ and then $U(m, t) = (m - 1, t)$ and $0 \leq m - 1 < m$. Thus if $x^2 > k - 4$, there is a transformation T in \mathcal{A} such that $T(P)$ has x coordinate with smaller absolute value.

If $k \equiv 2 \pmod{4}$ then by Lemma 4.6, z is even, and x, y are both odd, so that $x^2 - k \equiv 3 \pmod{4}$ and thus $x^2 - k \in \{-1, -5, -9, \dots\}$. Suppose $x^2 - k = -9$. If $|t| = 1$ we argue as above to reduce to a point with smaller absolute x value. If $|t| = |s| = 3$, then 3 divides y, z . But for $t = 3$, $|m - t| < |m|$ for $m \geq 2$. If $m = 1$, then $x = 3$, contradicting $\gcd(P) = 1$. Since 5, 13, 17 are prime, this proves that if $x^2 > k - 21$, there is a transformation T in \mathcal{A} such that $T(P)$ has x coordinate with smaller absolute value.

If $k \equiv 3 \pmod{4}$, by Lemma 4.6, z is odd and x, y are both even. Then $x^2 - k \in \{-3, -7, -11, -15, \dots\}$ and the result follows since 3, 7, 11 are prime. Similarly if $k \equiv 0 \pmod{4}$, x odd, y even and z odd, then $x^2 - k \in \{-3, -7, -11, -15, \dots\}$. ■

Corollary 4.9 *For k not a square, H_k is partitioned into finitely many equivalence classes by $\sim_{\mathcal{A}}$.*

Proof. Given k , for any value of x^2 there are only finitely many solutions s, t to $st = x^2 - k$. Thus by Theorem 4.8, there are only finitely many equivalence classes of points with \gcd of 1. If $\gcd(P) = d > 1$, then $(1/d)P \in H_{k/d^2}$, and since k is only divisible by a finite number of squares, we are done. ■

If k is not too large, Theorem 4.8 is useful in determining the equivalence classes of points mod \mathcal{A} on a hyperboloid H_k .

Example 4.10 First we look at some examples where k is square-free. These examples follow from Lemma 4.6 and Theorem 4.8.

- (i) Let $k = 2$. For $(x, y, z) \in H_2$, x, y are both odd. S_2 is the set of points (x, y, z) with $|x| = |y| = 1$. Thus $H_2 = [(1, 1, 0)]_{\mathcal{A}}$.
- (ii) Let $k = 3$, then x, y are both even. The set S_3 consists of the points in H_3 with $x = 0$. Thus $H_3 = [(0, 2, 1)]_{\mathcal{A}}$.
- (iii) For $k = 5$, S_5 is the set of points with $x^2 \leq 1$. If x is odd, then $x = 1$, and $|y| = 2, |z| = 0$. If x is even, apply $I_{1,2}$. Thus $H_5 = [(1, 2, 0)]_{\mathcal{A}}$.
- (iv) If $k = 6$, then we have x, y odd so S_6 is the set of points with $|x| = 1$. Then $|y| = 3, |z| = 2$. Thus $H_6 = [(1, 3, 2)]_{\mathcal{A}}$.
- (v) If $k = 14$, then $H_{14} = [(1, 7, 6)]_{\mathcal{A}}$.
- (vi) If $k = 30$, then S_k is the set of points with $|x| = 1$ or 3 . If $|x| = 3$, then we obtain the points $(3, 11, 10)$ and $(3, 5, 2)$. If $|x| = 1$, then we obtain the point $(1, 15, 14)$. Since $(1, 15, 14) = U(3, 11, 10)$, and $D(3, 5, 2) = (11, 3, 10)$ then $H_{30} = [(1, 15, 14)]_{\mathcal{A}}$.

In the next example, k is divisible by a square, so that H_k will contain points with $\gcd > 1$ and we refer back to Example 4.10.

Example 4.11 (i) Let $k = 8$ and $P \in H_8$ with $\gcd(P) = 1$. S_8 is the set of points with $x^2 = 1$, x odd. (Points with x even are obtained by applying $I_{1,2}$.) Now $|x| = 1$ implies $|y| = 4, |z| = 3$. For $P \in H_8$ with $\gcd(P) = 2$, then $P = 2P'$ for $P' \in H_2$. Thus $H_8 = [2(1, 1, 0)]_{\mathcal{A}} \cup [(1, 4, 3)]_{\mathcal{A}}$.

(ii) If $k = 12$, then again S_{12} is the set of points with $x^2 = 1$, x odd. If $|x| = 1$ then $|y| = 6, |z| = 5$. If $\gcd(P) = 2$, then $P = 2P'$ with $P' \in H_3$. Thus, $H_{12} = [2(0, 2, 1)]_{\mathcal{A}} \cup [(1, 6, 5)]_{\mathcal{A}}$.

(iii) Let $k = 18$ and then S_{18} is again the set of points with $x^2 = 1$. Then $st = -17$ and $|y| = 9, |z| = 8$. If $\gcd(P) = 3$ then $P \in [3(1, 1, 0)]_{\mathcal{A}}$. Thus $H_{18} = [(1, 9, 8)]_{\mathcal{A}} \cup [3(1, 1, 0)]_{\mathcal{A}}$.

(iv) If $k = 56$, then S_{56} is the set of x odd, $x^2 \leq 41$, i.e., $|x|$ is $1, 3$, or 5 . If $|x| = 1$, we obtain points $(1, 28, 27)$, and $(1, 8, 3)$. If $|x| = 3$, we obtain the point $(3, 24, 23) = I_1 U^2(1, 28, 27)$. If $|x| = 5$, we obtain $(5, 16, 15) = I_1 U I_1(3, 24, 23)$. If $P \in H_{56}$ has $\gcd 2$, then from Example 4.10 $P \in [2(1, 7, 6)]_{\mathcal{A}}$. Thus $H_{56} = [(1, 28, 27)]_{\mathcal{A}} \cup [(1, 8, 3)]_{\mathcal{A}} \cup [2(1, 7, 6)]_{\mathcal{A}}$. It is not clear whether or not the first two classes are the same.

5 Partitioning the units by inner automorphisms

Consider the units $u_1 = (0, 1, -1), u_2 = (1, 0, 1), u_3 = (0, -1, -1), u_4 = (-1, 0, 1)$ in \mathcal{H}_0 . Let $U_i, i = 1, \dots, 4$, be the inner automorphisms of V_1 induced by u_i , i.e., $U_i(w) = u_i w u_i^{-1}$. Using Theorem 3.2 it is easy to check that the U_i act as linear transformations on \mathbf{Z}^3 that preserve $x^2 + y^2 - z^2$. The matrices associated with these linear transformations are:

$$U_1 = I_3 U_3 I_3 = \begin{bmatrix} 1 & 4 & 4 \\ -4 & -7 & -8 \\ 4 & 8 & 9 \end{bmatrix}; \quad U_2 = I_3 U_4 I_3 = \begin{bmatrix} -7 & -4 & 8 \\ 4 & 1 & -4 \\ -8 & -4 & 9 \end{bmatrix}. \quad (9)$$

As well, we have the following commutation relations:

$$\begin{aligned} I_1 U_1 I_1 &= U_1^{-1}; & I_2 U_1 I_2 &= U_3^{-1}; & I_3 U_1 I_3 &= U_3; & I_{1,2} U_1 I_{1,2} &= U_4; \\ I_1 U_2 I_1 &= U_2^{-1}; & I_2 U_2 I_2 &= U_2^{-1}; & I_3 U_2 I_3 &= U_4 & I_{1,2} U_2 I_{1,2} &= U_3. \end{aligned} \quad (10)$$

Again, note that the U_i preserve the gcd of any triple and the parity of x, y, z . Define the following groups of transformations on the H_k .

(i) Let \mathcal{U} be generated by U_1, U_2 , the I_i and $I_{1,2}$.

(ii) Let \mathcal{U}' be generated by the $U_i, i = 1, \dots, 4$.

In [6, Theorem 4.3] it is shown that \mathcal{H} is a free group of rank 3 generated by the bicyclic units u_1, u_2, u_4 . Thus \mathcal{U}' is the group of inner automorphisms of \mathcal{H} , which is isomorphic to \mathcal{H} . In other words, each \mathcal{H}_c is an \mathcal{H} -set. From [6, Theorem 4.3] and (10), we obtain the following.

Lemma 5.1 (i) For $u, v \in \mathcal{H}_c$, $u \sim_{\mathcal{U}'} v$ if and only if there is $w \in \mathcal{H}$ such that $v = w u w^{-1}$.

(ii) $u \sim_{\mathcal{U}} v$ if and only if $u \sim_{\mathcal{U}'} R(v)$ for some $R \in \mathcal{R}$.

Lemma 5.2 The group \mathcal{U} is a subgroup of \mathcal{A} so that in \mathcal{H}_c , $[P]_{\mathcal{U}} \subseteq [P]_{\mathcal{A}}$. Furthermore, if $T, S \in \{A, U, D, A^{-1}, U^{-1}, D^{-1}\}$, then $TS \in \mathcal{U}$.

Proof. This follows directly from Lemma 4.3 and the relations

$$U_1 = (I_2 A)^2; \quad U_2 = (I_1 A^{-1})^2; \quad U_3 = (I_2 A^{-1})^2; \quad U_4 = (I_1 A)^2.$$

For example, $UD = AI_2 AI_1 = I_2 (I_2 A)^2 I_1 = I_2 U_1 I_1$ and $UD^{-1} = AI_2 I_1 A^{-1} = I_2 U_1 U_4^{-1} I_1$. ■

Theorem 5.3 Suppose $P = WR'(P)$ where W is a composition of an odd number of transformations from $\{A, U, D, A^{-1}, U^{-1}, D^{-1}\}$ and $R' \in \mathcal{R}'$. Then $[P]_{\mathcal{A}} = [P]_{\mathcal{U}}$.

Proof. Suppose $Q \in [P]_{\mathcal{A}}$. Then $Q = TR(P)$ for some $T \in \mathcal{A}'$, $R \in \mathcal{R}'$. If T can be written as the composition of an even number of transformations from $\{A, U, D, A^{-1}, U^{-1}, D^{-1}\}$, then $T \in \mathcal{U}$ and $[P]_{\mathcal{A}} = [P]_{\mathcal{U}}$. Otherwise, write $Q = TRWR'(P)$. By (8), $RW = W'R$ where W' is also the composition of an odd number of transformations from $\{A, U, D, A^{-1}, U^{-1}, D^{-1}\}$. But then $TW' \in \mathcal{U}$ and we are done. ■

Corollary 5.4 \mathcal{H}_c contains only finitely many equivalence classes mod \mathcal{U} .

Proof. $[P]_{\mathcal{A}} = [P]_{\mathcal{U}} \cup [A(P)]_{\mathcal{U}}$ where the last two classes may be equal. ■

Theorem 5.3 yields the following examples.

Example 5.5 Since $(1, 0, 1) = D(1, 0, 1)$, then $[(1, 0, 1)]_{\mathcal{A}} = [(1, 0, 1)]_{\mathcal{U}}$. Thus \mathcal{H}_0 , the set of integer points on the cone, consists of all points which can be obtained from reflections of $(n, 0, n)$, $n \geq 0$ by an inner automorphism.

Example 5.6 From Example 4.10, $H_2 = \mathcal{H}_2 = [(1, 1, 0)]_{\mathcal{A}}$. Since $u_3u_2^{-1} = (1, 1, 0) = A^{-1}UD(1, 1, 0)$, then $\mathcal{H}_2 = [(1, 1, 0)]_{\mathcal{U}}$. Thus if $u \in \mathcal{H}_2$, $u = wvw^{-1}$ for some $w \in \mathcal{H}$ and $v \in \{(1, 1, 0), (-1, 1, 0), (1, -1, 0), (-1, -1, 0)\}$.

Example 5.7 From Example 4.10, $\mathcal{H}_{-2} = H_6 = [(1, 3, 2)]_{\mathcal{A}}$. But $(1, 3, 2) = U^{-1}A^{-1}D(1, 3, 2)$ and so $\mathcal{H}_{-2} = [(1, 3, 2)]_{\mathcal{U}}$, and every unit with $c = -2$ can be obtained from a reflection of $(1, 3, 2) = (u_3u_2)^{-1}$ by an inner automorphism.

Example 5.8 Let $c = 4$. Then $\mathcal{H}_4 = H_{12} = [2(0, 2, 1)]_{\mathcal{A}} \cup [(1, 6, 5)]_{\mathcal{A}}$. Since $AI_3I_{1,2}(0, 2, 1) = (0, 2, 1)$, and $I_1AI_2(1, 6, 5) = (1, 6, 5)$, then $\mathcal{H}_4 = [(0, 4, 2)]_{\mathcal{U}} \cup [(1, 6, 5)]_{\mathcal{U}}$. Note that $(0, 4, 2) = u_4u_2$ and $(6, -1, -5) = u_3u_2^{-1}u_4$.

Example 5.9 Let $c = 6$. Then $\mathcal{H}_6 = H_{30} = [(1, 15, 14)]_{\mathcal{A}}$. But $(1, 15, 14) = I_1U(1, 15, 14)$ so $\mathcal{H}_6 = [(1, 15, 14)]_{\mathcal{U}}$.

In Example 4.11, it was not determined if $(1, 8, 3) \sim_{\mathcal{A}} (1, 28, 27)$. We show next that $[(1, 28, 27)]_{\mathcal{U}} \neq [(1, 8, 3)]_{\mathcal{U}}$. Since $U^3(7, 4, 3) = (1, 28, 27)$, $[(7, 4, 3)]_{\mathcal{U}} = [(1, 28, 27)]_{\mathcal{U}}$. Note that $[(7, 4, 3)]_{\mathcal{A}} = [(7, 4, 3)]_{\mathcal{U}}$ since $D(7, 4, 3) = (7, -4, 3)$.

Lemma 5.10 *In \mathcal{H}_8 , $[(7, 4, 3)]_{\mathcal{U}} \neq [(1, 8, 3)]_{\mathcal{U}}$.*

Proof. By Lemma 5.1, these units are equivalent if and only if $wu = R(v)w$ for some $w \in \mathcal{H}$, $R \in \mathcal{R}$. Let $w = (e, f, b) \in \mathcal{H}_c$, with c even. If $w(7, 4, 3) = (1, 8, 3)w$, by Proposition 3.2, $2f = 3e$ (so e is even) and $2c = 1 + 3e - 4b$, impossible. Thus $[(1, 8, 3)]_{\mathcal{U}} \neq [(7, 4, 3)]_{\mathcal{U}}$. If $w(-7, 4, 3) = (1, 8, 3)w$, then $f = -2e$ and $2c = 1 + 3e + 3b$. Then f is even by the first equation and since $e^2 + f^2 = b^2 + c(c - 1)$, then e, b have the same parity. But then the second equation is impossible. If $w(7, -4, 3) = (1, 8, 3)w$, then $4b + 6c - 6f = 3$, impossible. If $w(7, 4, -3) = (1, 8, 3)w$, then $2c = 1 - 4b$, impossible. Now let $w(-7, -4, 3) = (1, 8, 3)w$. This implies that $2b = -2 + 4c + 3f, 2e = -3f$ so that f is even, and as above, e, b have the same parity. Combining the two equations, we have that $b + e = -1 + 2c$ which is impossible. Let $w(-7, 4, -3) = (1, 8, 3)w$. Then $2f = 3b - 4e, 2c = 1 + 3b$. But the first equation implies that b is even, which makes the second impossible. If $w(7, -4, -3) = (1, 8, 3)w$, then $4e = -3 + 6c + 8f$ which is impossible. If $w(-7, -4, -3) = (1, 8, 3)w$, then $4e = -3 + 6c - 6f$, also impossible. ■

Note that in the above proof, it is not necessary to test $R = I_{1,2}$ since inner automorphisms preserve parity. The final example partially describes the classes in \mathcal{H}_8 . It is not clear whether or not $[(1, 8, 3)]_{\mathcal{A}} = [(1, 8, 3)]_{\mathcal{U}}$. Since $U(1, 8, 3) = (-9, 0, -5)$, this is equivalent to the question of whether or not $[(1, 8, 3)]_{\mathcal{U}} = [(-9, 0, -5)]_{\mathcal{U}}$. Unfortunately, the method of Lemma 5.10 does not yield a straightforward contradiction. In fact, it is easy to show that $(1, 8, 3)w$ cannot equal $wR(9, 0, 5)$ for $R \neq I_3$. However, the equation $(1, 8, 3)w = w(9, 0, -5)$ yields $f = 2(1 - 2c) - 4b, e = f - b$. Substituting into the equation for a hyperboloid gives

$$20b = -18c + 9 \pm \sqrt{14c^2 - 14c + 1}.$$

A computer search for integer solutions yields none but we have been unable to prove that none exist. Thus we have the following (incomplete) example.

Example 5.11 Let $c = 8$. From Example 4.11, $H_{56} = [2(1, 7, 6)]_{\mathcal{A}} \cup [(1, 28, 27)]_{\mathcal{A}} \cup [(1, 8, 3)]_{\mathcal{A}}$. Since $(1, 7, 6) = U^{-1}I_1(1, 7, 6)$, $[2(1, 7, 6)]_{\mathcal{A}} = [2(1, 7, 6)]_{\mathcal{U}}$. Thus $\mathcal{H}_8 = [2(1, 7, 6)]_{\mathcal{U}} \cup [(1, 28, 27)]_{\mathcal{U}} \cup [(1, 8, 3)]_{\mathcal{U}} \cup [(9, 0, 5)]_{\mathcal{U}}$ where it has not been determined if the last two classes are equal.

Acknowledgement: Thanks to E. Goodaire, E.Jespers, M.M.Parmenter, C.Polcino Milies for their helpful comments on the first draft of this project.

References

- [1] M. Beattie, Duality theorems for group actions and gradings, Ring Theory Proceedings Granada 1986, Lecture Notes in Mathematics 1328, Springer, New York, 1988, 28-32.
- [2] M. Cohen and S. Montgomery, Group-graded rings, smash products, and group actions, Trans. Amer. Math. Soc., **282**, (1984), 237-258.
- [3] E.G. Goodaire, E. Jespers, and M.M. Parmenter, Determining units in some integral group rings, Canad. Math. Bull., **33** (2), (1990), 242-246.
- [4] G. Higman, The units of group rings, Proc. London Math. Soc.,**46** (1940), 231-248.
- [5] A. Hall, Genealogy of Pythagorean triads, Mathematical Gazette, LIV 390 (1979), 377-379.
- [6] E. Jespers and G. Leal, Describing units of integral group rings of some 2-groups, Communications in Algebra 19(1991), no. 6, 1809-1827.
- [7] C. P. Milies, The group of units of the integral group ring $\mathbf{Z}D_4$, Bol. Soc. Brasil. Mat. **4**, (1972), 85-92.
- [8] C.P.Milies and S. Sehgal, An introduction to group rings, Kluwer 2002.
- [9] P. Moore, Units of integral group rings for finite groups, Mt. Allison U. Research Report M/CS 91-4.
- [10] D. Passman, The algebraic structure of group rings, Wiley-Interscience, New York, 1977.
- [11] S.K. Sehgal, Topics in group rings, Marcel Dekker, New York, 1978.