The Inversion Formula

Robert A. Liebler

Colorado State University
Fort Collins, Colorado 80523

A version of the discrete Fourier transform that is valid in noncommutative groups is presented together with examples and an application to the study of difference sets in groups of order $4p^2$.

Apology and Introduction

Efforts to apply algebraic methods to combinatorial problems have from the outset faced a paradox. While a central theme of any algebraic structure theory is to enumerate intrinsic properties of the objects of the relevant category, one loses the way back to the original combinatorial problem unless additional data is tracked throughout. Thus, for example, the coding theorist using linear algebra who fails to keep track of the basis of message bits has no future even though a central theme of linear algebra is that all bases of a vector space are equivalent.

A most important part of algebraic combinatorics concerns the transfer of information between a "combinatorially relevant" coordinate system and a "algebraically expedient" coordinate system. This situation is shared by other subjects. For example, Diophantine equations are studied with rings other than the integers but special machinery is used to return to the integers.

The application of rings (or more properly finite dimensional R-algebras, for R a commutative ring) to combinatorics has been initiated a number of times. Although I. Schur introduced "Der zu einer Permutationsgruppe gehoerende Matrizenring" [18], the value of these rings in combinatorics seems to have been first clearly recognized by R. C. Bose and D. M. Mesner [2]. Since then, generalizations and variations on their theme have been called *cellular rings* by B. Weisfeiler and A. A. Lehman [20], [6], *coherent configurations* by D. G. Higman [8], and *based rings* by G. Lusztig [13].

A major challenge is to develop methods that transfer information between the combinatorial and algebraic frameworks for these rings. Progress could be useful in a number of areas including: the application of discrete Fourier transform for non-commutative groups [5], construction of generalized Hadamard matrices [3], partial addition sets [7], and of t-designs in the sense of Delsarte [4]; and even possibly the study of known P-Q schemes [1] by construction of anti-t-designs in the sense of Brouwer.

Years ago R. C. Bose argued strongly that the best place to develop new methods is in the study of explicit celebrated open problems. For at least this reason, difference sets in explicit groups interest me. Thus the word apology is used here

JCMCC 13 (1993), pp. 143-160

in the slightly archaic sense: "not as an admission of guilt or regret but rather a desire to make clear the grounds for some course, belief or position" [19].

Section 2 begins with background material from group representation theory and presents "the inversion formula". It is a formula for an element of a group ring in terms of this element's images under each of the group's irreducible representations. This formula reduces to the familiar discrete Fourier transform in case the group is abelian and thus it might be regarded as a non-commutative generalization. In this regard, the formula is perhaps not as satisfactory as eg. [15, 3.2.21] because the "Fourier coefficient" associated with a particular representation is neither unique nor an element of the underlying field. Instead, it is a certain equivalence class of elements of the group ring itself. In section 3, this nonuniqueness is exploited in the study of difference sets. Arithmetic arguments of McFarland [14] are adapted and combined with celebrated results of Segre [16,17] on arcs in Desarguesian planes and a little finite geometry to show that difference sets do not exist in certain groups of order $4p^2$ in Theorem 3.1.

This research was partially supported by National Security Agency grant MDA 904-91-H-0048 and encouragement of and helpful conversations with J. Iiams, S. Magliveras and K. W. Smith are acknowledged.

2. Group representations and the inversion formula

Let G be a finite group written multiplicatively and let R be an integral domain containing the integers $\mathbf{Z}$. The group ring RG consists of formal R-linear combinations

$$x = \sum_{g \in G} x_g g; x_g \in R$$

of elements of G with component wise addition and multiplication determined by the multiplication of G and the distributive laws.

A *representation* of G over R with representation space the R-module V is a group homomorphism

$$\varphi: G \to \text{ the units of } Hom_R(V).$$

The representation φ endows V with a (left) RG-module structure ($gv := \varphi(g)v$) and there is a one to one correspondence between G-representations over R and RG-modules. In a certain sense, the variety of RG-modules reflects the variety of ways to impose an additive structure on the multiplicative structure G and obtain a ring.

There are at least two G-representations with representation space RG that play important combinatorial roles. The *left regular representation*

$$\Lambda: G \to Hom_R(RG)(\Lambda(g)x = gx).$$

and the *right regular representation*

$$P: G \to Hom_R(RG)(P(g)x = xg^{-1}).$$

If G is not abelian then Λ and P are not equal (see example 2.5) but they are equivalent in a natural way because RG is a Frobenius algebra [15,§2.8]. It is shown in section 3 how they appear together in difference set constructions.

Of course, an "algebraically expedient basis" for the group ring RG must reflect its ring structure. Since G is finite, The Krull-Schmidt theorem implies that RG is an internal direct sum of indecomposable RG-sub bimodules. This decomposition is reflected in the expression of 1 as a sum of central primitive idempotents [15, p.19]

$$1 = \sum e_i, \text{ and so } \quad RG = \sum \oplus e_i RG e_i. \tag{2.1}$$

Associated with each e_i, is an irreducible *representation* φ_i, where $\varphi_i(g) = ge_i$. The associated RG-module is RGe_i', where and e_i' is any primitive idempotent not annihilated by e_i. Relative to any R-basis $\{b_1, \ldots, b_n\}$ of RGe_i', $\varphi_i(g)$ is realized as an invertible n by n matrix with entries in R. The *character* associated with e_i, is the function from G to R defined by $\chi_i(g) = trace(\varphi_i(g))$. The domains of both φ_i and χ_i are extended to RG by "linearity".

It is natural from an algebraic point of view to replace R with an algebraic extension of its quotient field if necessary to arrange so that each summand is as small as possible and there are as many summands as possible. Any such field K is called a *splitting field* for G. If R is a splitting field of G then the number of terms in (2.1) is the number of conjugacy classes in G [15, Th 3.1.23].

Thus, the central primitive idempotents in KG form an algebraically expedient basis in case G is abelian and K is a splitting field of characteristic zero. In this case, the discrete Fourier transform of an element δ of KG has i-th coefficient $\chi_i(\delta) \in K$, where (as above)

$$\delta e_i = \chi_i(\delta) e_i.$$

and the inversion formula reads

$$\delta = \delta 1 = \delta \sum e_i^2 = \sum \delta e_i e_i = \sum \chi_i(\delta) e_i.$$

Suppose G is not abelian. Then an arbitrary $\delta \in KG$ is no longer a K-linear combination of central primitive idempotents. However there remains the formula

$$\delta = \delta \sum e_i^2 = \sum \delta e_i e_i = \sum \varphi_i(\delta) e_i.$$

whose i-th coefficient is in the summand KGe_i, of KG and is therefore unique, by (2.1). Unfortunately, explicit computation with KGe_i is difficult, even for straightforward groups G, and for this reason, we return to KG and say $\delta_i \in KG$ is an φ_i-th *alias* of δ if $\varphi_i(\delta) = \varphi_i(\delta_i)$. Now the the (general) *inversion formula* is:

Theorem 2.2. *Let K a field of characteristic zero and take $\{e_i\}$ to be the central primitive idempotent for KG. For $\delta \in KG$, we have*

$$\delta = \sum \varphi(\delta_i) e_i,$$

where δ_i is any φ_i-th alias of δ, that is $\varphi_i(\delta) = \varphi_i(\delta_i)$.

Proof: In the group algebra KG we have the equation:

$$\delta = \delta \sum e_i^2 = \sum \delta e_i e_i = \sum \varphi_i(\delta) e_i = \sum \varphi(\delta_i) e_i.$$

∎

In combinatorial applications the element δ is actually in the integer group ring $\mathbf{Z}G$ and for this reason it is desirable to use the inversion formula in $\mathbf{Q}G$. There is an explicit formula [15, Th 3.2.22] for the central primitive idempotents of a group ring over a splitting field:

$$e_i = \frac{\chi_i(1)}{|G|} \sum_{g \in G} \chi_i(g^{-1}) g, \tag{2.3}$$

that can be used to obtain the central primitive idempotents in $\mathbf{Q}G$.

Corollary 2.4. *Suppose m is the exponent of G and $\zeta \in \mathbf{C}$ a primitive m-th root of unity. Let Γ be the Galois group of $K = \mathbf{Q}[\zeta]$ over $\mathbf{Q}$. Then K is a splitting field for G. For each $\sigma \in \Gamma$, σ induces a permutation of $\{e_i\}$ (and so also $\{\varphi_i\}$ and $\{\chi_i\}$) by means of*

$$e_{\sigma(i)} = \frac{\chi_i(1)}{|G|} \sum_{g \in G} \sigma(\chi_i(g^{-1})) g.$$

The central primitive idempotent in $\mathbf{Q}G$ are indexed by the Γ-orbits $X_1, X_2, \ldots, X_m$ on $\{e_i\}$ and have the form:

$$E_j = \sum_{e_i \in X_j} e_i.$$

Proof: A celebrated theorem of Brauer [15, Th 3.4.11] asserts that the cyclotomic field K is a splitting field for G. Now K is Galois over $\mathbf{Q}$ and so the sums E_j are central idempotents in $\mathbf{Q}G$. If E_j could be written as the sum of two idempotents in the center of $\mathbf{Q}G$, then each which would split into a sum of central primitive idempotents in a Γ-orbit, contrary to the definition of E_j. ∎

Example 2.5: Consider the Quaternion group of order 8.

$$G = \langle x, y | x^4 = y^4 = 1, x^{-1}y^{-1}xy = x^2 = y^2 \rangle = \{1, x, x^2, x^3, y, xy, x^2y, x^3y\}.$$

For the elements in this order,

$$\Lambda(y) = \begin{array}{c|c} \begin{matrix} & & & 1 \\ & & 1 & \\ & 1 & & \\ 1 & & & \end{matrix} & \begin{matrix} & & & \\ & & & \\ & & & \\ & & 1 & \end{matrix} \\ \hline \begin{matrix} 1 & & & \\ & & 1 & \\ & 1 & & \\ & & & 1 \end{matrix} & \begin{matrix} & & & \\ & & & \\ & & & \\ & & & \end{matrix} \end{array} \text{ while, } P(y) = \begin{array}{c|c} \begin{matrix} & & & 1 \\ & & 1 & \\ & 1 & & \\ 1 & & & \end{matrix} & \begin{matrix} & & & \\ & & & \\ & & & \\ & & & \end{matrix} \\ \hline \begin{matrix} & & & \\ & & & \\ & & & \\ & & & \end{matrix} & \begin{matrix} & & & 1 \\ & & 1 & \\ & 1 & & \\ 1 & & & \end{matrix} \end{array}.$$

Consider the matrix:

$$M_1 = \begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & & 1 & \\ 1 & 1 & -1 & -1 & & 1 & & 1 \\ 1 & 1 & 1 & 1 & -1 & & -1 & \\ 1 & 1 & -1 & -1 & & -1 & & -1 \\ \hline 1 & -1 & 1 & -1 & 1 & & -1 & \\ 1 & -1 & -1 & 1 & & 1 & & -1 \\ 1 & -1 & 1 & -1 & -1 & & 1 & \\ 1 & -1 & -1 & 1 & & -1 & & 1 \end{array}$$

having multiples of the central primitive idempotents:

$$\{e_1, e_2, e_3, e_4\} = \{(1 \pm x)(1 + x^2)(1 \pm y)/8\}; e_5 = (1 - x^2)/2,$$

as its columns. (In columns 5 through 8 $2e_5$ is multiplied by $(1 \pm y)$, $x(1 \pm y)$, as these expressions are easy aliases for elementary diagonal matrices in the explicit representation ϕ given below.) Relative to the $\mathbf{Q}$ basis of $\mathbf{Q}G$ given by the columns of M_1, the left regular representation of $\mathbf{Q}G$ is realized explicitly as a direct sum of irreducible representations since $M_1^{-1}\Lambda(x)M_1$ and $M_1^{-1}\Lambda(y)M_1$ are:

$$\begin{array}{cccc|cccc} 1 & & & & & & & \\ & 1 & & & & & & \\ & & -1 & & & & & \\ & & & -1 & & & & \\ \hline & & & & & -1 & & \\ & & & & 1 & & & \\ & & & & & & -1 & \\ & & & & & & & 1 \end{array} \quad \text{and} \quad \begin{array}{cccc|cccc} 1 & & & & & & & \\ & -1 & & & & & & \\ & & 1 & & & & & \\ & & & -1 & & & & \\ \hline & & & & & & & 1 \\ & & & & & & 1 & \\ & & & & & -1 & & \\ & & & & -1 & & & \end{array}$$

For each $g \in G$, define $\varphi(g)$ to be the 4 by 4 matrix obtained from $M_1^{-1}\Lambda(g)M_1$ by deleting rows and colums 1 through 4. Then φ is a representation of G that turns out to be irreducible over $\mathbf{Q}$. However, G has 5 confugacy classes and so Corollary (2.4) implies that φ is reducible over $\mathbf{Q}[i]$. Indeed for M_2 having the same first four columns as M_1 but with columns 5 through 8 obtained by muliplying $2e_5$ by $(1 \pm iy)$, $x(1 \pm iy)$ (These expressions are easy aliases for elementary matrices the explicit representation given by the last 2 by 2 block of $M_2^{-1}\Lambda(g)M_2$ below.), $M_2^1\Lambda(x)M_2$ and $M_2^1\Lambda(y)M_2$ have the form:

$$\begin{array}{cccc|cccc}
1 & & & & & & & \\
 & 1 & & & & & & \\
 & & -1 & & & & & \\
 & & & -1 & & & & \\
\hline
 & & & & -1 & & & \\
 & & & & 1 & & & \\
 & & & & & -1 & & \\
 & & & & & & 1 &
\end{array}
\quad \text{and} \quad
\begin{array}{cccc|cccc}
1 & & & & & & & \\
 & -1 & & & & & & \\
 & & 1 & & & & & \\
 & & & -1 & & & & \\
\hline
 & & & & -i & & & \\
 & & & & & i & & \\
 & & & & & & i & \\
 & & & & & & & -i
\end{array}$$

Although the central primitive idempotents of $\mathbf{Q}[i]G$ have the same form as those in $\mathbf{Q}G$, the columns of M_2 give a basis of $\mathbf{Q}[i]G$ that could be organized to have four 1 by 1 blocks follwed by one 2 by 2 block and so that e_i appears as the identity on the ith blocks,

$$x = \begin{array}{cccc|cccc}
1 & & & & & & & \\
 & 1 & & & & & & \\
 & & -1 & & & & & \\
 & & & -1 & & & & \\
\hline
 & & & & -1 & & & \\
 & & & & 1 & & &
\end{array}
\quad \text{and} \quad
y = \begin{array}{cccc|cccc}
1 & & & & & & & \\
 & -1 & & & & & & \\
 & & 1 & & & & & \\
 & & & -1 & & & & \\
\hline
 & & & & -i & & & \\
 & & & & & i & &
\end{array}.$$

$\Lambda(g)$ is "multiply on the left by g" and $P(g)$ is "multiply on the right by g^{-1}."

The characters of G are usually presented in the character table having rows labelled by characters and colums labelled by conjugacy classes in G:

	1	x^2	x, x^3	y, y^3	xy, xy^3
χ_1	1	1	1	1	1
χ_2	1	1	−1	1	−1
χ_3	1	1	1	−1	−1
χ_4	1	1	−1	−1	1
χ_5	2	−2	0	0	0

which in turn gives the central primitive idempotents by equation (2.3). In practice, there are powerful methods for computing character tables and they are really the first step in an analysis of this type.

Example 2.6: Consider $G = \langle x | x^{2^n} = 1 \rangle$ the cyclic group of order 2^n. The character table of G is the Van derMonde matrix:

$$\lambda_j(x^k) = (\zeta^{jk});$$

where ζ is a primitive 2^n-th root of unity. The value $j = 0$ corresponds to the trivial representation and j is odd if and only if the representation is faithful. The idempotent formula (2.3) reads

$$e_{\lambda_i} = 2^{-n} \sum_{g \in G} \lambda_j(g^{-1}) g = 2^{-n} \prod_{i=0}^{n-1} [1 + \lambda_j(x^{-2^i}) x^{2^i}].$$

The faithful characters form one orbit under the Galois group $Aut_{\mathbf{Q}}\mathbf{Q}(\zeta)$, so the nontrivial central primitive idempotents in $\mathbf{Q}G$ are the remarkably simple:

$$e_k = 2^{k-n}[1 - x^{2^k}] \prod_{i=k+1}^{n-1} [1 + x^{2^i}]; k = 0, 1, \ldots, n-1.$$

This simplicity accounts for some the relative ease with which difference sets in 2-groups can be analyzed.

Example 2.7: The group

$$G = \langle x, y, z | x^3 = y^3 = z^4 = 1, yx = xy, xz = zx^{-1}, yz = zy^{-1} \rangle$$

of order 36 has 11 rational central primitive idempotents that are given in (3.4):

$$e_0 = (\sum x)(\sum y)(\sum z)/36,$$

$$e_1 = (\sum x)(\sum y)(\sum z^2)(1-z)/36,\ e_2 = (\sum x)(\sum y)(1-z^2)/18,$$

$$e_3 = (\sum x)(2-y-y^2)(1+z^2)/18,\ f_3 = (\sum x)(2-y-y^2)(1-z^2)/18,$$

$$e_4 = (2-x-x^2)(\sum y)(1+z^2)/18,\ f_4 = (2-x-x^2)(\sum y)(1-x^2)/18,$$

$$e_5 = (2-x-x^2)(\sum xy)(1+z^2)/18,\ f_5 = (2-x-x^2)(\sum xy)(1-z^2)/18,$$

$$e_6 = (2-x-x^2)(\sum x^2y)(1+z^2)/18,\ f_6 = (2-x-x^2)(\sum x^2y)(1-z^2)/18,$$

where $\sum g$ denotes the sum of the powers of $g \in G$. Kibler [11] gives the subset Δ in G having sum in $\mathbf{Z}G$:

$$\delta = (1+x)(\sum y) + (\sum x)z^2 + (\sum xy)xz + (\sum xy^2)z^3,$$

as a difference set, and so $\varphi(\delta\delta^{(-1)}) = 9$ for each nontrivial irreducible representation φ of G (see section 3). The inversion formula (2.4) requires φ-aliases for δ and these are most easily computed using explict representations for φ of the form given in Lemma 3.2. For example, the explicit representation associated with f_6 is:

$$\rho_6(x^i y^j) = \begin{pmatrix} \omega^{2i-j} & 0 \\ 0 & \omega^{j-2i} \end{pmatrix}, \rho_6(z) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ where } \omega \neq 1 = \omega^3.$$

so

$$\rho_6(\delta) = \rho_6(1+x)\rho_6(\sum y) + \rho_6(\sum x)\rho_6(z^2) + \rho_6(\sum Xy)\rho_6(xz) + \rho_6(\sum xy^2)\rho_6(z^3) = 3\rho_6(z^3),$$

since $\rho_6(\sum x^i y^j) = \begin{pmatrix} 1+\omega+\omega^2 & 0 \\ 0 & 1+\omega+\omega^2 \end{pmatrix} = 0$, for $\{0\} \neq \{i,j\} \neq \{1,2\}$ and $\rho_6(\sum xy^2) = 3$. The inversion formula can be written down as:

$$\delta = 3\left(5e_0 + e_1 + e_2 + e_3 - x^2 e_4 + xe_5 + e_6 + z^2 f_3 + x^2 z^2 f_4 + xzf_5 + z^3 f_6\right).$$

In the next section it is shown that much of the nature of these aliases is already apparent from the difference set equation. The simple nature of each alias is exploited in a geometric argument that shows this example to be truly exceptional.

3. Difference sets and the inversion formula

A subset Δ of the group G is a *difference set* (with parameters $v = |G|, k = |\Delta|, \lambda$) if for each $g \in G, g \neq 1$, there exist exactly λ solutions to

$$xy^{-1} = g, x, y \in \Delta.$$

The set Δ is a difference set in G exactly if

$$\delta\delta^{-1} = (k-\lambda)1 + \lambda \sum G \text{ in } \mathbf{Z}G,$$

where:

$$\delta = \sum_{g\in\Delta} g,\ \delta^{(-1)} = \sum_{g\in\Delta} g^{-1},\ \sum G = \sum_{g\in G} g,$$

and 1 is the identity element of G. The parameter $n = k - \lambda$ is called the *order* of Δ.

Each difference set Δ in G gives rise to a symmetric design that admits G as a sharply transitive group of automorphisms. This design has points and blocks labelled by elements of G and incidence xIy if and only if $y^{-1}x \in \Delta$. Here

$$gxIgy \text{ if and only if } (gy)^{-1}gx \in \Delta \text{ if and only if } y^{-1}g^{-1}gx = y^{-1}x \in \Delta,$$

so G acts on points and on blocks by the *left* regular representation. The incidence matrix of the design is $P(\delta)$, the *right* regular representation of G.

Let $R = \mathbf{Q}[\zeta]$ be a splitting field for G as in Corollary (2.4) and suppose that Δ is a difference set in G and let $e_0, e_1, \ldots, e_t$ be the central primitive idempotents of RG labelled so that $e_0 = (\sum G)/|G|$ is the idempotent associated with the trivial representation. Further, as is always possible, take φ_i to be an explicit unitary matrix representation. Then the difference set equation

$$\delta\delta^{(-1)} = n1 + \lambda \sum G$$

implies

$$\varphi_i(\delta)\overline{\varphi_i(\delta)}^t = e_i\delta\delta^{(-1)}e_i = \begin{cases} ke_0 & \text{if } i = 0 \\ ne_i & \text{otherwise.} \end{cases}$$

The choice of $R = \mathbf{Q}[\zeta]$ comes heavily into play in most cases where one can proceed. On the basis of only the above information, one can actually solve for $\varphi_i(\delta)$ and thereby obtain rather elementary aliases for δ as in Lemma 3.3.

In order to illustrate this method, consider groups of order $4p^2$, p an odd prime. A theorem of Menon implies that Δ is of Hadamard type and has parameters $k = 2p^2 - p, \lambda = p^2 - p$ and order $n = p^2$. Kibler [11] has settled the case $p = 3$ by computer. A beautiful theorem of McFarland [14] asserts that $p = 3$ when G is abelian. Iiams [9] has shown that $p = 3$ if a Sylow 2-subgroup is not cyclic. One of the seven remaining cases is settled in the main theorem of this section:

Theorem 3.1. *If p is an odd prime and the group*

$$G = \langle x, y, z | x^p = y^p = z^4 = 1, yx = xy, z^{-1}xz = x^{-1}z^{-1}yz = y^{-1} \rangle.$$

possesses a difference set then $p = 3$. (cf. example 2.7)

Notation of numbered results will be cummulative in this section.

Lemma 3.2. *Set $H = \langle x, y \rangle$ and let ζ a primitive p-th root of unity. Let H^* denote the character group $Hom(H, \mathbf{C}^*)$ of H. Then $K = \mathbf{Q}[\zeta, i]$, is a splitting field for G and the irreducible representations for KG are defined by:*

$$\varphi_j(x) = \varphi_j(y) = 1, \varphi_j(z) = i^j; j = 0, 1, 2, 3;$$

$$\varphi_\lambda(x) = \begin{pmatrix} \lambda(x) & 0 \\ 0 & \overline{\lambda(x)} \end{pmatrix}, \varphi_\lambda(y) = \begin{pmatrix} \lambda(y) & 0 \\ 0 & \overline{\lambda(y)} \end{pmatrix}, \varphi_\lambda(z)) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$\rho_\lambda(x) = \begin{pmatrix} \lambda(x) & 0 \\ 0 & \overline{\lambda(x)} \end{pmatrix}, \rho_\lambda(y) = \begin{pmatrix} \lambda(y) & 0 \\ 0 & \overline{\lambda(y)} \end{pmatrix}, \rho_\lambda(z) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix};$$

$$\lambda \in H^* - \{1\}.$$

Proof: Each of the indicated functions defines a unitary representation of G and is irreducible. Two of the indicated functions could be equivalent only if their

restrictions to the cyclic subgroups generated by x, y and z are equivalent. The only possibilities are $\varphi_\lambda \cong \varphi_{\overline{\lambda}}$ and $\rho_\lambda \cong \rho_{\overline{\lambda}}$. Taking this into account we have identified a subspace of KG of dimension $4+2^2(p^2-1)/2+2^2(p^2-1)/2 = |G|$. The result follows. ∎

Call a system of distinct representatives for the $Aut_{\mathbf{Q}}\mathbf{Q}[\zeta]$-orbits on the nontrivial characters of H a *cyclic basis* for H^* **[14, p6]**.

Lemma 3.3. *Suppose $\delta \in \mathbf{Z}G$ satisfies $\varphi(\delta\delta^{(-1)}) = p^2 I$ for all of the nontrivial φ in (3.2). If $p \equiv 1 \pmod 4$, let $a, b \in \mathbf{Z}$ such that $a^2 + b^2 = p$. Then δ has a φ-alias of the form $g\delta' g'$, where $g, g' \in G$ and δ' equals:*

i) p,
ii) $(a \pm bz)g(a \pm bz)$ *where* $g \in G$ *and* $\varphi = \varphi_1, \varphi_3$ *or* $\rho_\lambda \lambda \in \Lambda$,
iii) $-p$ *if* $\varphi = \varphi_\lambda$ *for some* $\lambda \in \Lambda$,
iv) $(a \pm bz)\sum_{j=0}^{p-2} z^{2j} h^{tj}$ *where* $h \in H, t \in \mathbf{Z}$ *and* $\varphi = \rho_\lambda, \lambda \in \Delta$, *or*
v) $(a \pm bz)\sum_{j=0}^{p-2} z^{j} h^{tj}$ *where* $h \in H, t \in \mathbf{Z}$ *and* $\varphi = \rho_\lambda, \lambda \in \Lambda$.

In particular, only cases i) and iii) occur when $p \equiv 3 \pmod 4$.

The proof of this crucial lemma is postponed.

Since the φ-aliases for $\delta \in \mathbf{Z}G$ provided by Lemma 3.3 are in $\mathbf{Z}G$, Corollary (2.4) applies. Call a system of distinct representatives for the $Aut_{\mathbf{Q}}\mathbf{Q}[\zeta]$-orbits on the nontrivial characters of H a *cyclic basis* for H^* **[14, p6]**. By Corollary 2.4, the central primitive idempotents in $\mathbf{Q}G$ are,

$$E_0 = e_{\varphi_0} = \frac{1}{4p^2}\sum H(1+z^2)(1+z),$$

$$E_1 = e_{\varphi_2} = \frac{1}{4p^2}\sum H(1+z^2)(1-z),$$

$$E_2 = e_{\varphi_1} + e_{\varphi_3} = \frac{1}{2p^2}\sum H(1-z^2),$$

$$E_\varphi = \sum_{k=1}^{\frac{p-1}{2}} e_{\varphi^k} = \frac{1+z^2}{2p^2}[p\sum(ker\varphi) - \sum H]; \varphi \in \Lambda,$$

$$F_\rho = \sum_{k=1}^{\frac{p-1}{2}} e_{\rho^k} = \frac{1-z^2}{2p^2}[p\sum(ker\rho) - \sum H]; \rho \in \Lambda, \tag{3.4}$$

where Λ is a cyclic basis for the characters of H. The inversion formula given in Theorem (2.2) over $\mathbf{Q}$ for δ now reads:

$$\delta = (2p^2 - p)E_0 \pm p\,E_1 + \delta_2 E_2 + \sum_{\varphi \in \Lambda} \delta_\varphi E_\varphi + \gamma_\varphi F_\varphi,$$

where $\delta_2, \delta_\varphi, \gamma_\varphi$ are the appropriate aliases for δ determined in Lemma 3.3. Thus

$$2p^2\delta - \left(\frac{2p^2-p}{2}(1+z) \pm \frac{p}{2}(1-z)\right)\sum H(1+z^2) - \delta_2 \sum H(1-Z^2)$$
$$= \sum_{\varphi\in\Lambda}[\delta_\varphi(1+z^2)+\gamma_\varphi(1-z^2)][p\sum(ker\varphi) - \sum H].$$

In order to postpone consideration of the more complicated aliases appearing in Lemma 3.3, multiply this equation by $(1+z^2)$ to obtain:

$$p^2\delta(1+z^2) - \left(\frac{2p^2-p}{2}(1+z) \pm \frac{p}{2}(1-z)\right)\sum H(1+z^2)$$
$$= \sum_{\varphi\in\Lambda}\delta_\varphi[p\sum(ker\varphi) - \sum H](1+z^2).$$

By Lemma 3.3, there exist $\epsilon \in \{0,1\}$, $\epsilon_\varphi \in \{-1,1\}$ and $d_\varphi \in G$; $\varphi \in \Lambda$ such that $\delta_\varphi = p\epsilon_\varphi d_\varphi$ and

$$p\delta(1+z^2) - p\sum G + z^\epsilon \sum H(1+z^2) = \sum_{\varphi\in\Lambda}\epsilon_\varphi d_\varphi[p\sum(ker\varphi - \sum H](1+z^2).$$

Thus

$$\delta(1+z^2) - \sum G = \sum_{\varphi\in\Lambda}\epsilon_\varphi d_\varphi \sum(ker\varphi)(1+z^2) - \frac{z^\epsilon + d_0 + d_1 z}{p}\sum H(1+z^2), \tag{3.5}$$

where

$$d_i = |\{\varphi\in\Lambda \mid \epsilon_\varphi = 1, d_\varphi \in z^i H\cdot z^2\rangle\}|$$
$$- |\{\varphi\in\Lambda \mid \epsilon_\varphi = -1, d_\varphi \in z^i H\cdot\langle z^2\rangle\}|.$$

Now $d_0 + d_1$ has absolute value less than or equal to $p+1$ and is even since

$$p+1 = |\Lambda| \equiv d_0 + d_1 \pmod 2$$

so $\{d_0, d_1\} = \{-1, \pm p\}$ or $\{0, \pm p - 1\}$.

Now view $G/\langle z^2\rangle = H\langle z^2\rangle/\langle z^2\rangle \cup zH\langle z^2\rangle/\langle z^2\rangle$ as the union of two Desarguesian affine planes of order p (lines are cosets of subgroups of the elementary abelian group $H\langle z^2\rangle/\langle z^2\rangle$). The parallel classes in both planes are indexed by $\varphi \in \Lambda$ and each term $d_\varphi\sum(ker\varphi)(1+z^2)$ is the set of points on a line in the parallel class indexed by φ in one of the planes. We have shown that one $H\langle z^2\rangle$-coset, say $\Pi = \pi H \cup \pi z^2 H$, $\pi \in G$ contains at least $p-1$ of these lines, say $\ell \in L$, and the associated ϵ_φ are all equal, say to γ.

Lemma 3.6. *The support S of $\delta(1-z^2)$ in πH is either a conic Ω with one point at infinity or the disjoint union of Ω and an affine tangent line ℓ.*

Proof: The restriction of equation (3.5) to elements of G in Π gives the multiset equation

$$\delta(1+z^2)\cap\Pi = (1-\gamma)\Pi + \gamma\sum(\ell\in L).$$

Since each point of Π is counted 0, 1 or 2 times on the left, no three of these lines are on the same point. Together with the line at infinity, the lines in L form a "line arc" and therefore $|L|\le p$. Since $|L|\ge p-1$, theorems of Segre [16,17] imply that they are tangents to a conic having exactly one point at infinity. The lines tangent to such a conic cover the $p(p-1)/2$ affine exterior points twice, the p affine absolute points Ω once and the $p(p-1)/2$ affine interior points zero times. The support of $\delta(1-z^2)$ is exactly the set of points covered once and so is Ω in case $|L|=p$, $\Omega+(\ell\cap\Omega)$ in case $|L|=p-1$ and ℓ is the affine tangent to Ω not in L. ∎

Set $\epsilon = p-|L|$ and take $\lambda\in\Lambda$ be chosen so that $ker\ \lambda$ is not in the parallel class of the ideal point of Ω and is not parallel to the tangent ℓ to Ω not in L in case $\epsilon=1$. Then, in the notation of (3.2) $\rho_\lambda(\delta) = \begin{pmatrix} c & -d \\ \overline{d} & \overline{c}\end{pmatrix}$ and one of c, d equals

$$\sum_{g\in S}\pm\lambda(g) = \sum m_j\zeta^j,$$

where $m_j = |\Delta\cap g ker\lambda| - 1|\Delta\cap g z ker\lambda|$, for appropriate $g\in\Pi$. Observe that

0) $\sum m_j = |\Delta\cap\pi H| - |\Delta\cap\pi z^2 H|$;
1) $m_j = \pm\epsilon$ for at least $(p-1)/2$ values of j; (3.7)
2) $m_j\equiv\epsilon+1 \pmod 2$ exactly once in which case $|m_j|\le 2$; and
3) $|m_j|\le 2+|\epsilon|$.

because there are $(p-1)/2$ passing lines to, one tangent line to and $(p-1)/2$ secant lines to Ω in the parallel class of λ. In addition note that the p-tuple $(m_0,\dots,m_{p-1})$ is unique modulo $(1,\dots,1)$ as $\sum\zeta^j = 0$ is the only relation among the coefficients since $[\mathbf{Q}(\zeta):\mathbf{Q}] = p-1$.

Proof of Theorem 3.1: Compare (3.7) with those appearing in the Lemma 3.3.

An alias of type i) has at most one nonzero term in the expansion of c, d and this term equals p. This fits only if $\epsilon=1$ and $p=3$.

An alias of type v) has one zero coefficent and half of the remaining coefficients $\pm a$ and half $\pm b$. Since a and b have opposite parity, this doesn't fit.

An alias of type ii) has $\{c,d\}$ of the form $\{ab(\zeta^k\pm\overline{\zeta}^k), a^2\zeta^k\pm b^2\overline{\zeta}^k\}$, so all but two of the terms m_j must be equal $(=\pm\epsilon)$. Exactly one of a, b is odd, call it a. If $k\neq 0$ then Π is associated with a term of the form $a^2\zeta^k\pm b^2\overline{\zeta}^k$ and $a=1$, by (3.7.2). Now the other $m_j\neq\pm\epsilon$ has absolute value ≤ 3 and the form

$\pm\epsilon \pm b^2$ where b is even. This occurs only if $\epsilon = 1, p = 5$ and the multiset of m_j's is $\pm\{1,1,1,2,-3\}$. If $k = 0$ only the term of (3.7.2) survives. Since it differs from the rest by at most 3, this occurs only if $\epsilon = 1, p = 5$ and the multiset of m_j's is $\pm\{1,1,1,-2,1\}$. In each of these cases, (3.7.0) implies that $\Delta \cap \pi H$ and $\Delta \cap \pi z^2 H$ have a difference of 2. This is incompatible with each of the possible φ_1-aliases of δ listed in Lemma 3.3.

An alias of type iv) has one zero term and all of the rest of the same parity half each equalling say $\pm a$ (a may in principle be odd or even at this point).

In case $\epsilon = 1$, the m_j value of ± 1 occurs at least $1 + (p-1)/2$ times by Lemma 3.6 (disjoint union) and (3.7.1). It follows that the multiset of m_j's is $\{\pm 1, \ldots, \pm 1, 0, \pm 1, \ldots, \pm 1\}$ with half of the terms positive and half negative. By (3.7.0), $\varphi_1(\delta)$ has an alias of type (3.3i) and there are integers n_j and $x \in G - \Pi$ such that

$$\sum_{g \in T} \pm\lambda(g) = \sum h_j \zeta^j = \pm p\lambda(x)$$

where T is the support of $\delta(1 - z^2)$ on $G - \Pi$. This means that

$$\pm p = \pm[\,|x ker\lambda \cap \Delta| - |xz^2 ker\lambda \cap \Delta|\,] - t$$

where t arises from the relation $\sum \zeta^j = 0$ and the intersections of Δ with the other lines parallel to $ker\ \lambda$ as in (3.7). By equation (3.5), T is the set of points off the disjoint union of a line parallel to ℓ and a line in the parallel class determined by the ideal point of Ω. The lines parallel to $ker\ \lambda$ intersect T in sets of odd cardinality, namely $p - 2$ or p and it follows that both t and $|T \cap x ker\lambda| = |x ker\lambda \cap \Delta| + |xz^2 ker\lambda \cap \Delta|$ are odd. Now the last displayed equation implies that p is even, which is a contradiction.

In case $\epsilon = 0$, a is forced to equal 1 and the multiset of m_j's is $\pm\{0, \ldots, 0, 1, 2, \ldots, 2\}$. This forces Ω entirely into one of the H-cosets associated with Π and therefore (3.7.0) provides complete information about $\Delta \cap \pi H$ and $\Delta \cap \pi z^2 H$. The difference of the cardinalities of these intersections is p and so each of the sets $\Delta \cap \pi H$ and $\Delta \cap \pi z^2 H$ contains the exterior points of Ω but one of them also containing the points of Ω. This implies that $\varphi_1(\delta)$ has an alias of type i) in Lemma 3.3 and therefore each of the H-cosets in $G - \Pi$ contains $p(p-1)/2$ elements of Δ.

Now turn to ρ_μ, where $ker\ \mu$ is in the parallel class labelled by the ideal point of Ω. Since all elements of Ω are in the same coset and each line in this parallel class has exactly one point in Ω, the associated entry of $\rho_\mu(\delta)$ is $\pm\sum \zeta^k = 0$. This implies that $\rho_\mu(\delta)$ has an alias of type i) in Lemma 3.3 and the term in $\rho_\mu(\delta)$ associated with $(G - \Pi)$ has the form $\pm p\zeta^t = \sum n_j \zeta^j$ where each n_j has the form $|\Delta \cap g ker\lambda| - |\Delta \cap z^2 g ker\lambda|$ for some g. By equation (3.5), the support of Δ on $(G - \Pi)$ is the complement of a line in the parallel class of λ, so one of the $n_j = 0$ and the others are all odd. It follows that the other coefficients n_j are

constant ($= \pm p$), since $[\mathbf{Q}[\zeta]:\mathbf{Q}] = p-1$. This shows that $\Delta \cap (G-\Pi)$ is a union of cosets of $ker\mu$. Now the entries of $\rho_\lambda(\delta)$ associated with $(G-\Pi)$ are zero, contrary to case iv). ∎

The proof of Theorem (3.1) has been reduced to the

Proof of 3.3: Since $\varphi_2(\delta)$ is an integer of absolute value p and $\varphi_2(z) = -1$, i) holds in this case. In case φ equals φ_1 or φ_3 $\varphi(\delta)$ is a Gaussian integer of modulus p and so i) or ii) holds.

The matrix $\varphi_\lambda(\delta)$ has the form $\varphi_\lambda(\delta) = \begin{pmatrix} a & b \\ \overline{b} & \overline{a} \end{pmatrix}$ where

$$a = \sum_{h\in H}\lambda(\delta_h h) + \sum_{h\in H}\lambda(\delta_{hz^2}h), b = \sum_{h\in H}\lambda(\delta_{hz}h) + \sum_{h\in H}\lambda(\delta_{hz^3}h) \in \mathbf{Z}[\zeta].$$

Compare the (1,2) entries in the difference set equation $\varphi(\delta\delta^{(-1)}) = p^2 I$ to see that $2ab = 0$. Suppose $b = 0$ and recall [15, p 15] that $\pi = (1-\zeta)$ is a prime ideal in $\mathbf{Z}[\zeta]$ that is invariant under conjugation and $(p) = \pi^{p-1}$. The equation $a\overline{a} = p^2$ now implies that $(a) = \pi^{p-1} = (p)$, and so a/p is a unit of modulus 1 in $\mathbf{Z}[\zeta]$. If φ is twisted by $\sigma \in Aut_{\mathbf{Z}}\mathbf{Z}[\zeta]$, then the above argument leads to $\sigma(a/p)$ is also a unit of modulus 1. A theorem of Kronecker [14, p 15 l-1] (that an algebraic integer all of whose algebraic conjugates have modulus 1 must be a root of unity) implies that $a/p = \pm\zeta^k$ for some k. Thus either case i) or iii) occurs.

All that remains are the representations ρ_λ. Since $\rho_\lambda(\delta) = \begin{pmatrix} c & -d \\ d & \overline{c} \end{pmatrix}$ where

$$c = \sum_{h\in H}\lambda(\delta_h h) - \sum_{h\in H}\lambda(\delta_{hz^2}h), d = \sum_{h\in H}\lambda)\delta_{hz}h) - \sum_{h\in h}\lambda(\delta_{hz^3}h) \in \mathbf{Z}[\zeta],$$

we study the ring of matrices $\mathcal{R}$ of the form $m(:\ z,y) = \begin{pmatrix} x & -y \\ \overline{y} & \overline{x} \end{pmatrix}$ where $x, y \in \mathbf{Z}[\zeta]$. It is convenient to identify $\mathbf{Z}[\zeta]$ with the subring $\{m(x,0)\}$ of $\mathcal{R}$. Observe that each nontrivial element of $\mathcal{R}$ has positive determinant and so $\mathcal{D} = \mathcal{R}\otimes_{\mathbf{Z}[\zeta]}\mathbf{Q}[\zeta]$ is a division ring. Note also that the cyclic group $Aut_{\mathbf{Z}}\mathbf{Z}[\zeta]$ acts naturally on $\mathcal{R}$ and and that $\sigma(\rho_\lambda(\delta)) = \rho_{\sigma(\lambda)}(\delta)$ for each $\sigma \in Aut_{\mathbf{Z}}\mathbf{Z}[\zeta]$. Finally, the map $\tau: \mathcal{R} \to \mathcal{R}$ defined by $\tau(m(x,y)) = m(\overline{x}, -y)$ takes a matrix to its conjugate transpose and induces an anti-automorphism of $\mathcal{R}$ that commutes with $Aut_{\mathbf{Z}}\mathbf{Z}[\zeta]$.

The ring $\mathcal{R}$ has an additional remarkable property of which we make repeated use.

If m in $\mathcal{R}$ has determinant 1, then $m = \rho_\lambda(g)$ for some $g \in G$. (3.8)

Indeed, $m(x,y)$ has determinant $(x\overline{x} + y\overline{y}) = 1$ and has entries that are algebraic integers. For any automorphism σ of $\mathbf{Q}[\zeta]$, $\sigma(y)\sigma(\overline{y}) = \sigma(y)\overline{\sigma(y)}$ is a non-negative real number, so every algebraic conjugate of x has modulus less

than or equal to 1. If even one of these conjugates has modulus strictly less than one, then the norm of x is (equal to the product of all algebraic conjugates of x and equal to the constant term in the minimal polynomial of x) an integer of absolute value less than 1; that is x has norm zero. It follows that either x or y equals zero and all algebraic conjugates of the other have modulus 1. The above mentioned theorem of Kronecker implies that the nonzero term, say x is, root of unity, say μ, $\mu^n = 1$. Since $2 \geq [\mathbf{Q}[\mu,\zeta]:\mathbf{Q}[\zeta]] = \varphi(n/gcd(n,p))$, [10, 13.2] (here φ denotes the Euler φ-function), it follows that x has order dividing $2p$. The result now follows by inspection.

Let $\pi = (1-\zeta)\mathcal{R}$. Then π is an ideal in $\mathcal{R}$ that is τ-invariant, since

$$(1-\zeta)m(x,y) = m(x,-\zeta y)(1-\zeta), \overline{(1-\zeta)}^{\tau} = \bar{\zeta}(1-\zeta).$$

The ideal π is also $Aut_{\mathbf{Z}}\mathbf{Z}[\zeta]$-invariant and $\pi^{p-1} = (p)$, since $(1-\zeta)$ has these properties in $\mathbf{Z}[\zeta]$. Consequently, $\mathcal{R}/(p^2)$ has (Jacobson) radical containing π. The ring $\mathcal{R}/\pi$ is the finite ring $\mathbf{Z}/(p)[i]$ where $i^2 = -1$ and τ induces complex conjugation. Since $\mathcal{R}/\pi$ is of dimension 2 over $GF(p)$, any proper nontrivial ideal $\mathcal{I}/\pi$ in $\mathcal{R}/\pi$ has dimension 1 over $GF(p)$. If $0 \neq m(x,y)\pi/\pi \in \mathcal{I}/\pi$, then $m(x,y)$ has rank 1 (mod p) and

$$\det(m(x,y)) = x^2 + y^2 \equiv 0 \pmod{p}.$$

Thus, if $p \equiv 3 \pmod 4$, then $\mathbf{Z}/(p)[i]$ is the Galois field $GF(p^2)$ and π is prime. If $p \equiv 1 \pmod 4$, then $\mathbf{Z}/(p)[i] \cong GF(p) \oplus GF(p)$ and $\pi = \pi_1\pi_2$, where

$$\pi_1 = (1-\zeta, m(a,b)), \pi_2 = (1-\zeta, m(a,-b)) = \tau(\pi_1),$$

and a, b are integers such that $a^2 + b^2 = p$. In general, the radical of $\mathcal{R}/(p^2)$ is $\pi/(p^2)$. Such an $\mathcal{R}$-module is called *uniserial* [14,p.42]. When $p \equiv 1 \pmod 4$, the $\mathcal{R}/(p^2)$-ideals form a poset that is the product of two totally ordered chains and each ideal has the form $\pi_1^i\pi_2^j/(p^2)$, because $\mathcal{R}/\pi$ is $\mathcal{R}$-isomorphic to $\pi_1^i\pi_2^j/\pi_1^{i+1}\pi_2^{j+1}$ and so has only two proper nontrivial submodules. Thus $Aut_{\mathbf{Z}}\mathbf{Z}[\zeta]$ acts trivially on the set of $\mathcal{R}/(p^2)$-ideals.

Let $d = \rho_\lambda(\delta)$ and take σ to be a generator of $Aut_{\mathbf{Z}}\mathbf{Z}[\zeta]$. By the difference set equation $d\tau(d) = p^2$, the ideal (d) contains (p^2). The preceding paragraph implies $(d) = (\sigma(d))$. Thus, there exist $m, n \in \mathcal{R}$ such that $\sigma(d) = m\,d\,n$. If possible, take n, m so that $\det m = 1 = \det n$. Observe that $n\tau(n) = \det n \in \mathbf{Z}(\mathcal{D})$, since it is a scalar matrix. The difference set equation for $\sigma(d)$ and d gives:

$$\begin{aligned} p^2 &= \sigma(d)\tau\sigma(d) = (m\,d\,n)\tau(m\,d\,n) = m\,d[n\,\tau(n)]\tau(m\,d) \\ &= m[n\,\tau(n)][d\,\tau(d)]\tau(m) = m\,n\,\tau(n)p^2\tau(m) = p^2(m\,n)\tau(m\,n). \end{aligned}$$

This shows that $1 = \det mn$ and so both $\det mI_2 = m\tau(m)$ and $\det nI_2 = n\tau(n)$ are units in $Z(\mathcal{D})$. Thus, in fact, $\det m = 1 = \det n$ is a possible choice and (3.8) implies

$$\sigma(\rho_\lambda(\delta)) = \rho_\lambda(g'\delta g''), \text{ for some } g', g'' \in G.$$

If $p \equiv 3 \pmod 4$, then $\mathcal{R}/p^2$ is uniserial so each of its ideals is τ invariant too. It follows from the difference set equation that $\rho_\lambda(\delta) \in \pi^{p-1} = (p)$ and so $\rho_\lambda(\delta) = p\,m$ where $1 = \sigma^i(m)\tau\sigma^j(m)$ for all j. By (3.8), $m = \rho_\lambda(g)$ for some $g \in G$ and i) holds in this case.

Suppose that $p \equiv 1 \pmod 4$ and write

$$g' = z'h', g'' = h''z'', \text{ for } z', z'' \in \langle z \rangle \text{ and } h', h'' \in H/\ker \rho_\lambda.$$

Define σ as an automorphism of $H/\ker \rho_\lambda$ by $\rho_\lambda(h^\sigma) = \sigma(\rho_\lambda(h))$, and note that as such σ commutes with (conjugation by) z', z''. Also, z' induces an automorphism of H of order at most 2 and σ generates $Aut_{\mathbf{Z}}\mathbf{Z}[\zeta]$ and so it has order $p-1$. Since $p > 3$, $\sigma z' \neq 1 \neq z''\sigma$ in $Aut(H/\ker\rho_\lambda)$. Replace δ with $h'^{(1-\sigma z')^{-1}}\delta h''^{(1-z''\sigma)^{-1}}$. Then

$$\begin{aligned}\sigma(\rho_\lambda(\delta)) &= h'^{(1-\sigma z')^{-1}\sigma} z'h'\delta h''z''h''^{(1-z''\sigma)^{-1}\sigma} \\ &= z'h'^{(1-\sigma z')^{-1}\sigma z'+1}\delta h''^{(1-z''\sigma)^{-1}\sigma z''+1}z'' \\ &= z'h'^{(1-\sigma z')^{-1}}\delta h''^{(1-z''\sigma)^{-1}}z'' = z'\delta' z''\end{aligned}$$

Since z^2 is in the center of G, we have

$$\begin{pmatrix}\sigma(c) & \sigma(-d)\\ \sigma(\bar d) & \sigma(\bar c)\end{pmatrix} = \sigma(\rho_\lambda(\delta)) = \pm\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}^e\begin{pmatrix}c & -d\\ \bar d & \bar c\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}^{e'}$$

where $e, e' \in \{0,1\}$. Now $m(c,d)$ satisfies the difference set equation if and only if $m(c,-d)$, $m(c,\bar d)$ and $m(d,c)$ do too, so there are really only four cases that need be considered:

$$\begin{aligned}&\sigma\colon c \to c; d \to d\\ &\sigma\colon c \to -c; d \to -d\\ &\sigma\colon c \to \bar c \to c; d \to -\bar d \to d\\ &\sigma\colon c \to d \to -c \to -d \to c\end{aligned}$$

The set $\{\zeta^{\sigma^j} | j = 0, \ldots p-2\}$ is a basis for $\mathbf{Z}[\zeta]$ over $\mathbf{Z}$. Write

$$c = \sum \gamma_j\zeta^{\sigma^j}, d = \sum \delta_j\zeta^{\sigma^j} \text{ for unique } \gamma_j, \delta_j \in \mathbf{Z}; j \in \mathbf{Z}/(p-1).$$

In the first case, $c, d \in \mathbf{Z}$, and ii) holds since $\mathcal{R} \cap \mathbf{Z} \cong \mathbf{Z}[i]$, the Gaussian integers.

In case $\sigma: c \to -c$, $\gamma_{j+1} = -\gamma_j$ and so:

$$c = \gamma_0 \sum (-1)^j \zeta^{\sigma^j} = -\gamma_0 \sqrt{p},$$

by a theorem of Gauss [**10, p 75**]. Consequently, the second case leads to iv).

In case $\sigma: c \to \bar{c} \to c; d \to -d \to d$, observe that $\bar{c} = \sum \gamma_j \zeta^{\sigma^{j+q}}$, where $q = (p-1)/2$ and conclude that $\gamma_{j+1} = \gamma_{j+q}; \delta_{j+1} = -\delta_{j+q}$. Therefore

$$c = \gamma_0 \sum \zeta^{\sigma^j} = -\gamma_0, d = \delta_0 \sum (-1)^j \zeta^{\sigma^j} = \delta_0 \sqrt{p}, \gamma_0, \delta_0 \in \mathbf{Z};$$

The only solution of the difference set equation of this type has $\delta_0 = 0$, and appears in i).

The final case $\sigma: c \to d \to -c \to -d \to c$ leads to $\gamma_j = \delta_{j+2} = -\delta_{j+3}$. Then

$$2(c + id) = c + i\sigma(c) - \sigma^2(c) - i\sigma^3(c) = \sum (\gamma_j + i\gamma_{j-1} - \gamma_{j-2} - i\gamma_{j-3}) \zeta^{\sigma^j}.$$

Because the $(j+1)$-st term in this sum is obtained from the j-th by multiplication by i, so:

$$2(c + id) = (\gamma_3 + i\gamma_2 - \gamma_1 - i\gamma_0) \sum i^j \zeta^{\sigma^j} = 2(\gamma_0 + i\gamma_1) \sum i_j \zeta^{\sigma^j}.$$

The sum $\alpha + i\beta = \sum i^j \zeta^{\sigma^j}$ a generalized Gauss sum, and has modulus $\sqrt{p}$ [**10, Ch 8**]. Since $p \equiv 1 \pmod 4$, -1 is a square in $\mathbf{Z}/(p)$, and so $\alpha, \beta \in \mathcal{R} \cap \mathbf{Q}[\zeta]$. Therefore

$$c = \gamma_0 \alpha - \gamma_1 \beta, d = \gamma_1 \alpha + \gamma_0 \beta \in \mathcal{R} \cap \mathbf{Q}[\zeta].$$

By the difference set equation,

$$p^2 = c\bar{c} + d\bar{d} = (c + id)\overline{(c + di)} = (\gamma_0 + i\gamma_1)\overline{(\gamma_0 + i\gamma_1)} p.$$

Thus $\gamma_0 + i\gamma_1$ is a Gaussian integer of modulus p. This is case v) of the Lemma.

References

1. E. Bannai and T. Ito, "Algebraic Combinatorics I: Association schemes", Benjamin/Cummings, 1984.
2. R.C. Bose and D.M. Mesner, *On linear associative algebras corresponding to association schemes of partially balanced designs*, Ann Math Stat **30** (1959), 21–38.

3. W. de Launey, *Generalized Hadamard matrices whose rows and columns form a group*, in "Combinatorial Mathematics X", Lecture notes in Mathematics 1036, Springer, New York, 1983, pp. 154–176.
4. P. Delsarte, *Hahn Polynomials, Discrete Harmonics and t-designs*, SIAM Appl. Math. **34** (1978), 157–166.
5. P. Diaconis, *Group Representation Theory in Probability and Statistics*, Inst of Math Statisitics, Howard California (1988).
6. I.A. Faradzev, A.A. Ivanov and M.H. Klim, *Galois correspondence between permutation groups and cellular rings (association schemes)*, Graphs and Combinatorics **6** (1990), 303–332.
7. D. Ghinelli and S. Loewe, *On multipliers of partial addition sets*, Geometria Dedicata **40** (1991), 55–58.
8. D.G. Higman, *Invariant theory, coherent configurations and generalized polygons*, Math. Cent Tract **57** (1974), 27–43.
9. J. Iiams. (to appear).
10. K.Ireland and M. Rosen, "A Classical Introduction to Modern Number Theory", Springer, New York, 1990.
11. R.E. Kibler, *A summary of noncyclic difference sets, $k < 20$*, J. Comb. Theory A **25** (1978), 62–67.
12. R.A. Liebler and K.W. Smith, *On difference sets in certain 2-groups*, in "Coding Theory, Design Theory and Graph Theory", Wiley, 1992, pp. 191–206.
13. G. Lusztig, *Leading coefficients of character values of Hecke algebras in Proceedings of Symposia in Pure Math*, American Math. Soc. **47** (1987), 235–262.
14. R.L. McFarland, *Difference sets in abelian groups of order $4p^2$*, Mitt. Math. Sem. Giessen **192** (1989), 1–70.
15. H. Nagao and Y. Tsushima, "Representations of Finite Groups", Academic Press, 1991.
16. B. Segre, *Curvi Rationali Normali e K-archi negli spazi finite*, Ann Mat. Pura. Appl. **39** (1955), 357–379.
17. B. Segre, *Ovals in a finite projective plane*, Can. J. Math. **7** (1955), 414–416.
18. I. Schur, *Zur Theorie der einfach transitiven permutations Gruppen*, Gesammelte Abhandlung III, Springer (1973), 266–298.
19. Webster's ninth new collegiate dictionary (1983), Merriam-Webster, Springfield, Mass.
20. B.J. Weisfeiler and A.A. Lehman, *The reduction of a graph to its canonical form and the arising algebra*, NTI ser 2 **9** (1968), 12–16.