

**Authors' Notes, April 16, 2007.**

This section provides an introduction to group rings and defines difference sets as certain elements of an integral ring.

It includes homomorphic images.

It includes the concept of equivalence of elements of the group ring.

It now contains *some* results on idempotents.

Can we find better examples? (“Equations in a group”, section 2.6, is rather a “hodge-podge” of examples?)

It contains Lemmas 3, 4, 5 and 6.

I have added a section on March 18, 2006, giving more examples.

Warning – I am trying to reserve  $K$  for a normal subgroup (usually the kernel of a homomorphism) instead of using  $K$  for a field. I’m not sure if that notational change is complete; there may still be some places where  $K$  is a field.

Warning – I am trying to use  $R[G]$  as a group ring instead of  $RG$ . (That notational change may also be incomplete.)

The sections are

1. Motivation
2. The Group Ring  $R[G]$ .
3. Homomorphic images
4. On idempotents
5. Difference sets from the group ring point of view
6. Equations in groups

## 2 Group Rings

### 2.1 Motivation for introducing group rings

A design (or other combinatorial configuration) can often be constructed using a group  $G$  of symmetries of the design. A combinatorial configuration with a *regular* automorphism group  $G$  will be equivalent to a special subset  $D \subseteq G$  of the group of symmetries. These combinatorial configurations (such as difference sets) then require certain computations in the automorphism group; this is facilitated by using the concept of group ring.

We begin with a finite group  $G$  of order  $m$  and a ring  $R$ . (At times we will assume the ring  $R$  is the ring of integers  $\mathbb{Z}$  or some subfield  $F$  of the complex numbers  $\mathbb{C}$ .) We wish to identify special subsets of  $G$  in order to construct combinatorial structures (symmetric designs, group divisible designs, distance regular graphs) with a “nice” group of symmetries, more precisely, with a sharply transitive automorphism group.

**References** on group rings: See Milies and Sehgal [55] (which also includes a brief history of the topic on pages 125-9) or Terras, [67].

### 2.2 The group ring $R[G]$

**Definition.** Given a finite group  $G$  and ring  $R$ , the **group ring**  $R[G]$  is a set of formal sums of the form  $\sum_{g \in G} r_g g$  where  $r_g \in R$  for all  $g \in G$ . The element  $r_g \in R$  is called the **coefficient** of  $g$  in the expression

$\sum_{g \in G} r_g g$ . We make this set into a ring by defining addition and multiplication in the obvious ways. The sum of two elements  $\sum_{g \in G} a_g g$  and  $\sum_{g \in G} b_g g$  is defined to be “pointwise”, that is,

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g.$$

The product of two terms  $a_g g$  and  $a_h h$  is defined to be the term  $(a_g a_h) gh$  and we extend multiplication to the entire set  $R[G]$  using the distributive law:

$$\left( \sum_{g \in G} r_g g \right) \left( \sum_{h \in G} s_h h \right) := \sum_{g, h \in G} r_g s_h gh = \sum_{f \in G} \left( \sum_{g \in G} r_g s_{g^{-1}f} \right) f.$$

In addition, for a “scalar”  $c \in R$ , define

$$c \left( \sum_{g \in G} a_g g \right) := \sum_{g \in G} (ca_g) g.$$

The set  $R[G]$  thus becomes an algebra with addition, multiplication, and scalar multiplication. It is often convenient to think of the elements of a group ring as “polynomials” with indeterminates (“variables”) from the group  $G$  and coefficients from the ring  $R$ .

Alternatively, we may define  $R[G]$  to be the set of functions from  $G$  into  $R$  and identify the group ring element  $\sum_{g \in G} r_g g$  with the function  $r$  such that  $r(g) := r_g$ . Thus  $r_g$ , the coefficient of  $g$  in  $\sum_{g \in G} r_g g$ , is the image of  $g$  under the function  $r$ . With this “function” viewpoint, the addition of two functions  $r$  and  $s$  is pointwise and the multiplication of two functions is “convolution.” For an example of the “function” viewpoint, see the book by Terras, [67].

**Definition.** Given an element  $X \in \mathbb{Z}[G]$ , we define the **support** of  $X$  to be the elements of  $G$  such that the coefficient,  $x_g$ , of  $g$  in  $X$  is nonzero.

The group ring  $R[G]$  is a free  $R$ -module with a natural basis  $G$ . If  $R$  is a field, then  $R[G]$  is a vector space over  $R$  and the elements of  $G$  form the **standard basis**  $\{g : g \in G\}$  for this vector space.

In constructing combinatorial objects with a large group of symmetries, we will be especially interested in the following rings.

1.  $\mathbb{Z}$ , the ring of integers. This ring is of interest since it is the “natural” ring for combinatorial counting.
2.  $\mathbb{Q}$ , the field of rational numbers. This field is important since it is the smallest field containing  $\mathbb{Z}$ .
3.  $\mathbb{C}$ , the field of complex numbers.
4.  $\mathbb{Z}[\zeta_t]$  and  $\mathbb{Q}(\zeta_t)$ . Here  $\zeta_t := e^{2\pi i/t}$  where  $t$  is the exponent of the group  $G$ .
5. Various subrings and quotient rings of the ring above.  $\mathbb{Q}(\zeta_t)$  is a field of dimension  $\phi(t)$  over  $\mathbb{Q}$  (here  $\phi$  is the Euler totient function) and  $\mathbb{Z}[\zeta_t]$  is not a field but a Dedekind domain (a “cyclotomic ring”).

### 2.2.1 An inner product on $R[G]$

If  $R$  is a subfield of the complex numbers  $\mathbb{C}$ , then we may define an inner product on  $R[G]$  by

$$\left\langle \sum a_g g, \sum b_g g \right\rangle := \frac{1}{|G|} \sum a_g \overline{b_g}.$$

This inner product turns the vector space  $R[G]$  into an inner product space. We will return to this concept in a later section.

### 2.2.2 Subsets as group ring elements

If  $S$  is a subset of  $G$ , then define  $\hat{S} := \sum_{s \in S} s$ . The group ring element  $\hat{S}$  is just a sum of the elements of

$S$ ; if  $S = \{s_1, s_2, \dots, s_k\}$  then  $\hat{S} = s_1 + s_2 + \dots + s_k$ . One can think of this as (almost) a notational convenience: replace commas by plus signs. For this reason, we will quickly get in the habit of lazily dropping the “hat” ( $\hat{\phantom{x}}$ ) and writing  $S$  for both a set and the sum of the elements of the set. In this way, we naturally identify subsets of  $G$  with group ring elements  $\sum a_g g$  where  $a_g \in \{0, 1\}$ .

Given a set  $S \subseteq G$ , the group ring element, the “function” viewpoint, cited above, would equate the group ring element  $\hat{S} = \sum_{s \in S}$  with the **characteristic function** from  $G$  to  $\{0, 1\}$  mapping elements of  $S$  to 1.

We write  $S^{(-1)}$  for the sum of all the elements which are inverses of the elements of  $S$ . Warning: the element  $S^{(-1)}$  is not the same as the element  $S^{-1}$ . If the element  $S$  in a group ring is invertible, its inverse  $S^{-1}$  is quite different from  $S^{(-1)}$ .

More generally, one might define  $S^{(t)}$  (note the parentheses around the  $t$ ) to be the sum of the elements  $s^t$  where  $s \in S$ .

For example, in the first section we developed the  $(7, 3, 1)$  symmetric design using the difference set  $D = \{1, 2, 4\}$  in  $\mathbb{Z}_7$ . Write the cyclic group of order seven multiplicatively as  $C_7 := \langle x : x^7 = 1 \rangle$  and so write  $D = \{x, x^2, x^4\}$ . We then view  $D$  as the group ring element  $\hat{D} = x + x^2 + x^4 \in \mathbb{Z}[C_7]$ . Thus an interesting set in the group  $C_7$  is turned into an interesting  $(0,1)$ -group ring element. This simple transformation (merely a change of viewpoint) carries considerable computational power.

### 2.2.3 Equivalence of group ring elements

**Definition.** Two elements  $X, Y \in \mathbb{Z}[G]$  are said to be translation equivalent if there is a group element  $g$  such that  $X = gY$ .  $X$  and  $Y$  are **automorphism equivalent** if there is a group automorphism  $\phi \in \text{Aut}(G)$  such that  $X = \phi(Y)$ . More generally, two elements  $X$  and  $Y$  are said to be **equivalent** if there is a group element  $g$  and automorphism  $\phi$  such that  $X = g\phi(Y)$ .

This generalizes the concept of equivalence from an earlier section.

## 2.3 Homomorphic Images of $G$ .

If  $G$  is a finite group and  $f : G \rightarrow H$  is a group homomorphism, then  $f$  extends by linearity to an algebra homomorphism  $\hat{f} : R[G] \rightarrow R[H]$ . Given an element  $X \in R[G]$ ,

$$X = \sum_{g \in G} x_g g,$$

then

$$\hat{f}(X) := \sum_{g \in G} x_g f(g).$$

**Definition.** Let  $H$  be a subgroup of  $G$  of index  $l$  in  $G$ . A set  $\{t_1, t_2, \dots, t_l\}$  is a complete set of distinct left cosets representatives if  $t_i H = t_j H \implies t_i = t_j$ . We will also call such a set a **left transversal** of  $H$  in  $G$ . We will generally assume  $t_1 = 1_G$ .

If  $H$  is a subgroup of  $G$  and  $B$  is an  $R$ -basis for  $R[H]$  then given any left transversal  $T$  of  $H$  in  $G$ , the set  $TB = \{tb : t \in T, b \in B\}$  is an  $R$ -basis for  $R[G]$ .

Suppose  $K$  is a normal subgroup of  $G$  and  $T = \{t_1, t_2, \dots, t_l\}$  is a transversal of  $K$  in  $G$ . The natural map  $f : G \rightarrow G/K$  extends to a homomorphism  $\hat{f} : \mathbb{Z}[G] \rightarrow \mathbb{Z}[G/K]$ ; given  $X = \sum_{g \in G} x_g g \in R[G]$ , we

have

$$\hat{f}(X) = \sum_{i=1}^j \left( \sum_{k \in K} x_{t_i k} \right) t_i K.$$

If  $X$  is a subset of  $G$  then the image of the group ring element  $X$  under this natural map is described by the intersection numbers of  $X$  and cosets of  $K$  in  $G$ :

$$\hat{f}(X) = \sum_{i=1}^j |X \cap t_i K| t_i K.$$

Suppose  $f : G \rightarrow H$  is a surjective group homomorphism with kernel  $K$  and suppose  $T = \{t_1, t_2, \dots, t_l\}$  is a transversal of  $K$  in  $G$ . By the fundamental homomorphism theorem of groups,  $G/K \cong H$  and so

$$\hat{f}(X) = \sum_{i=1}^j |X \cap t_i K| f(t_i).$$

We use this later so we distinguish this result as a lemma.

*FactorGroupImage*

**Lemma 3** *Let  $f : G \rightarrow H$  be a surjective group homomorphism. Let  $K$  be the kernel of  $f$  in  $G$  and let  $T$  be a transversal of  $K$  in  $G$ . The group homomorphism  $f$  extends naturally to a group ring homomorphism  $\hat{f} : R[G] \rightarrow R[H]$ . If  $X \subseteq G$  then*

$$\hat{f}(X) = \sum_{i=1}^j |X \cap t_i K| \hat{f}(t_i).$$

### 2.3.1 The canonical lift of a homomorphic image

Suppose  $f : G \rightarrow H$  is a group homomorphism with kernel  $K$ . Suppose that  $T \subseteq G$  is a transversal of  $K$  in  $G$ . The map  $\hat{f} : T \rightarrow H$  defined by  $\hat{f}(t_i) = f(t_i)$  is a bijection from  $T$  onto  $H$ . Order the elements of  $H$  such that  $h_i := f(t_i)$ . Let  $X = \sum_{h \in H} x_h h \in \mathbb{Z}[H]$  be an element of the group ring of  $H$ . The element

$$\hat{X} = \sum_{h \in H} x_h \hat{f}^{-1}(h) = \sum_{i=1}^l x_{h_i} t_i$$

is an element of  $\mathbb{Z}[G]$  which is mapped to  $X$  by  $f$ . It is the **canonical lift** of  $X$  (with respect to the homomorphism  $f$  and the transversal  $T$ .)

## 2.4 On idempotents

An idempotent is an element  $e$  of a ring  $R$  such that  $e^2 = e$ .

In the rational group ring  $\mathbb{Q}[G]$ , any subgroup  $H$  gives, in a natural way, an idempotent  $e = \frac{H}{|H|}$ . (The group ring *element*  $H$  has the property that  $H^2 = |H|H$ , where  $|H|$  is the size of the set  $H$ , and so  $(\frac{H}{|H|})^2 = \frac{H}{|H|}$ .)

In the next section, we will discuss idempotents in some detail, after the introduction of characters. At this stage, it is appropriate to mention a few properties of idempotents.

*IdempotentBasics*

**Lemma 4** *Suppose  $R$  is a ring with unity 1 and  $e \neq 1$  is an idempotent. Then*

1.  $1 - e$  is an idempotent and  $e(1 - e) = 0$ .
2.  $R = Re \oplus R(1 - e)$
3. If  $a$  is a fixed element of  $R$  and  $x_0 \in R$  such that  $x_0 e = a$ , then the set of solutions to the equation  $x e = a$  is exactly the set  $x_0 + R(1 - e)$ .

**Proof** Part (a) is merely a calculation.  $((1-e)^2 = 1-2e+e^2 = 1-e$ . Similarly  $(1-e)e = e-e^2 = e-e = 0$ .)

To prove part (b), note that given any ring element  $r$ , we have  $r = re + r(1-e)$  by the distributive law and so  $R \subseteq Re + R(1-e) \subseteq R$ . Thus  $R = Re + R(1-e)$ . Now, suppose  $x \in Re \cap R(1-e)$ . Then  $x = ae = b(1-e)$  for some ring elements  $a, b \in R$ . Multiplication by  $e$  on the right then gives  $xe = ae^2 = ae = x$  and  $xe = b(1-e)e = 0$ . Thus  $x = 0$  and so  $Re \cap R(1-e) = \{0\}$ .

To prove part c we first note that any element of the set  $x_0 + R(1-e)$  will be a solution to  $xe = a$  since  $x_0$  is a solution and  $(1-e)e = 0$ . On the other hand, if  $x$  is a solution to  $xe = a$  then  $(x-x_0)e = 0$  and so  $x-x_0 \in R(1-e)$ . Therefore  $x \in x_0 + R(1-e)$ .

Following Milies-Sehgal ([55], section 3.3, pp. 134 ff), we write  $\Delta_R(G, H) := R[G](1-e)$  where  $e = \frac{H}{|H|}$ .  $\Delta_R(G, H)$  is called the **augmentation ideal** of  $H$  in  $G$ . As ideals of the ring  $R[G]$ , we note that  $R[G]e = \langle H \rangle$ ,  $\Delta_R(G, H) = R[G](1-e) = \langle \{1-h : 1 \neq h \in H\} \rangle$  and so

$$R[G] = \langle H \rangle \oplus \langle \{1-h : 1 \neq h \in H\} \rangle = \langle H \rangle \oplus \Delta_R(G, H).$$

We explicitly describe a special case of this result, for later reference.

*AugmentationCyclic*

**Lemma 5** *Let  $G$  be a group,  $x \in G$ . Let  $R$  be some subfield of the complex numbers. Write  $\langle x \rangle$  for the sum of elements of the cyclic subgroup generated by  $x$ . Write  $R[G]\langle x \rangle$  and  $R[G](1-x)$  for the cyclic submodules generated by the elements  $\langle x \rangle$  and  $1-x$ , respectively. Then*

$$R[G] = R[G]\langle x \rangle \oplus R[G](1-x)$$

The  $R[G]$ -ideal  $R[G](1-x)$  is the augmentation ideal  $\Delta_R(G, \langle x \rangle)$ . If  $G$  has order  $m$  while  $x$  has order  $n$ , then the dimensions of  $R[G]\langle x \rangle$  and  $R[G](1-x)$  as  $R$ -vector spaces are  $m/n$  and  $(m/n)(n-1)$ , respectively.

Augmentation ideals are covered in section 3.3, pages 134-138, of Milies and Sehgal's book, [55].

If  $R$  is some subfield of the complex numbers, and  $H$  is a subgroup of  $G$  then  $e = \frac{H}{|H|}$  is an idempotent. Can we further identify the elements of  $R[G](1-e)$  in this case? We are particularly interested in the integral group ring  $\mathbb{Z}[G]$ .

#### 2.4.1 Integral bases for $\mathbb{Z}[G]$

A basis  $B = \{\beta_1, \beta_2, \dots, \beta_{|G|}\}$  for  $\mathbb{Q}[G]$  is an **integral basis** if  $\mathbb{Z}[G]$  is exactly the set

$$\mathbb{Z}[G] = \left\{ \sum_{\beta \in B} a_\beta \beta : a_\beta \in \mathbb{Z} \right\}.$$

The **standard basis**,  $\{g : g \in G\}$  is (by definition) an integral basis for  $\mathbb{Z}[G]$ .

Suppose  $H$  is a subgroup of  $G$  with transversal  $T$ . Recall that if  $B$  is a basis of  $K[H]$ , then the set  $TB := \{t\beta : t \in T, \beta \in B\}$  is a basis for  $K[G]$ . Furthermore, if  $B$  is an integral basis for  $\mathbb{Z}[H]$  then  $TB$  is an integral basis for  $\mathbb{Z}[G]$ .

In addition to the standard integral basis, we wish to consider two other bases here, one of which is an integral basis and one which is not.

Given subgroup  $H$  of  $G$ , set

$$B_1 := \{1\} \cup \{h-1 : 1 \neq h \in H\}$$

and

$$B_2 := \left\{ \frac{H}{|H|} \right\} \cup \{1-h : 1 \neq h \in H\}.$$

The set  $B_1$  is an integral basis for  $\mathbb{Z}[H]$  for we have

$$\sum_{h \in H} a_h h = \sum_{1 \neq h \in H} a_h (h-1) + \left( \sum_{h \in H} a_h \right) 1_H.$$

Conversely, given

$$X = \sum_{1 \neq h \in H} b_h(h-1) + (b_1)1_H$$

we may collect terms and write this as

$$X = \sum_{1 \neq h \in H} b_h h + (b_1 - \sum_{1 \neq h \in H} b_h)1_H.$$

If the coordinates of  $X$  with respect to one basis are integers then the coordinates of  $X$  with respect to the other basis are integers.

If  $\mathbb{Z}[H]$  has a natural inner product defined by the standard basis (so that, as in section 2.2,  $\langle \sum a_h h, \sum b_h h \rangle = \sum a_h \overline{b_h}$ ) then the set  $\{h-1 : 1 \neq h \in H\}$  is a basis for  $\langle H \rangle^\perp$ .

The set  $B_2$  is *not* an integral basis for  $\mathbb{Z}[H]$ , but significant in later analysis. Note that

$$\sum_{1 \neq h \in H} (1-h) = |H| - H.$$

Suppose an element  $X \in \mathbb{Z}[H]$  is written as a linear combination of elements from basis  $B_1$ :

$$X = a_1 1 + \sum_{1 \neq h \in H} a_h (1-h).$$

Rewrite this as follows:

$$\begin{aligned} X &= a_1 \left( \frac{H}{|H|} \right) + a_1 \left( \frac{|H| - H}{|H|} \right) + \sum_{1 \neq h \in H} a_h (1-h) \\ &= a_1 \left( \frac{H}{|H|} \right) + \frac{a_1}{|H|} \left( \sum_{1 \neq h \in H} (1-h) \right) + \sum_{1 \neq h \in H} a_h (1-h) \\ &= a_1 \left( \frac{H}{|H|} \right) + \sum_{1 \neq h \in H} \left( a_h + \frac{a_1}{|H|} \right) (1-h). \end{aligned}$$

Thus an element  $X$  of the group ring  $\mathbb{Q}[H]$  is an element of the integral group ring  $\mathbb{Z}[H]$  only if, when written as a linear combination of  $\frac{H}{|H|}$  and  $(1-h)$ , the coefficients of  $(1-h)$  have form  $a_h + \frac{a_1}{|H|}$  where the numerator  $a_1$  in the fraction is the coefficient of  $\frac{H}{|H|}$ .

If  $H$  is a proper subgroup of  $G$ , we may extend the integral basis  $B_1 = \{1\} \cup \{h-1 : 1 \neq h \in H\}$  to all of  $G$  by multiplying by a transversal  $T$ . Given the basis  $TB_1$ , we use the work above to change coordinates to the basis  $TB_2$ .

This is especially useful if  $H$  is the kernel of a homomorphism. Suppose  $f$  is a homomorphism from  $G$  onto a group  $L$  with kernel  $H$  and suppose that  $T$  is a transversal of  $H$  in  $G$ . Let  $X$  be any element of  $\mathbb{Z}[G]$ . Suppose

$$X = \sum_{t \in T} t \left( a_t + \sum_{1 \neq h \in H} a_{th} (h-1) \right).$$

Then we may write  $X$  with respect to the basis  $TB_2$  as

$$X = \left( \sum_{t \in T} a_t t \right) \left( \frac{H}{|H|} \right) + \sum_{t \in T} t \left( \sum_{1 \neq h \in H} \left( a_{th} + \frac{a_t}{|H|} \right) (1-h) \right).$$

The element  $A := \sum_{t \in T} a_t t$  is the canonical lift of  $f(X)$  to  $G$  and so we write  $X$  in terms of  $A$ :

$$X = A \left( \frac{H}{|H|} \right) + \sum_{1 \neq h \in H} \frac{A}{|H|} (1-h) + \sum_{t \in T} t \left( \sum_{1 \neq h \in H} a_{th} (1-h) \right).$$

We will return to integral bases in a later section.

## 2.5 Difference sets, from the group ring point of view

**Example 4, continued.** Let  $G := \langle x, y : x^8 = y^2 = 1, xy = yx \rangle$ . Earlier we claimed that the set  $D := \{1, x, y, x^3y, x^5y, x^7y\}$  is a  $(16, 6, 2)$  difference set.

How could we find (create) such objects as difference sets? Replace the set  $D$  by the group ring element  $\hat{D} := 1 + x + y + x^3y + x^5y + x^7y$ . This element  $\hat{D}$  obeys a certain equation. If we write  $\hat{D}^{(-1)}$  for the sum of inverses of elements in the set  $D$ , that is,  $\hat{D}^{(-1)} = 1 + x^7 + y + x^5y + x^3y + xy$ , then  $\hat{D}\hat{D}^{(-1)} = 4 \cdot 1 + 2(\sum_{g \in G} g)$ . If we also use  $\hat{G}$  to represent not just the set  $G$  but the sum of members of that set, then we have  $\hat{D}\hat{D}^{(-1)} = 4 \cdot 1 + 2\hat{G}$ .

(Thus we equate an element  $S$  with the sum  $\hat{S}$  of elements of  $S$  and the sum  $\hat{S}$  with its support.)

**Definition.** (Third definition of difference set.) Let  $(G, \cdot)$  be a finite group written multiplicatively. ( $G$  need not be abelian.) Set  $v := |G|$ . A proper nonempty set  $D \subseteq G$  is a  $(v, k, \lambda)$  **difference set** if  $D$  has  $k$  elements and in the group ring  $\mathbb{Z}[G]$ ,

$$D \cdot D^{(-1)} = (k - \lambda)1_G + \lambda G.$$

As we have done in other places, we will soon drop the “hat” ( $\hat{\phantom{x}}$ ) symbol and use  $f$  interchangeably for both  $f$  and  $\hat{f}$ . We will often suppress the symbols “ $1_G$ ” and “ $\cdot$ ” and so write

$$DD^{(-1)} = (k - \lambda) + \lambda G.$$

*DSFactorImage*

**Lemma 6** Suppose that  $f : G \rightarrow H$  is a group homomorphism with kernel  $K$  and suppose  $D$  is a difference set in  $G$ . Then  $f(D)$  satisfies the equation  $f(D) \cdot f(D^{(-1)}) = (k - \lambda) \cdot 1_H + \lambda|K|H$ .

**Proof.** As  $f$  is a homomorphism of groups, it extends by linearity to a homomorphism of group rings and so  $f(D) \cdot f(D^{(-1)}) = (k - \lambda) \cdot f(1_G) + \lambda f(G)$ . But  $f(1_G) = 1_H$  and as  $f$  is a  $|K|$ -to-1 mapping onto  $H$ ,  $f(G) = |K|H$ .  $\square$

### Example 1.

Suppose  $G = C_7 := \langle x : x^7 = 1 \rangle$  is the cyclic group of order seven and  $R = \mathbb{Z}$  is the ring of integers. Then in  $R[G] = \mathbb{Z}[C_7]$ , we have elements  $D := x + x^2 + x^4$  and  $D^{(-1)} := x^3 + x^5 + x^6$ . Then  $D + D^{(-1)} = x + x^2 + x^3 + x^4 + x^5 + x^6 = G - 1_G$  and so  $DD^{(-1)} = 3 \cdot 1_G + D + D' = 2 \cdot 1_G + 1G$ .

**More on Example 4.** Write an element  $\sum_{i=0}^1 \sum_{j=0}^7 a_{i,j} x^j y^i$  of the group ring  $\mathbb{Z}[C_8 \times C_2]$  as an array

$$\begin{bmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} & a_{0,4} & a_{0,5} & a_{0,6} & a_{0,7} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} & a_{1,5} & a_{1,6} & a_{1,7} \end{bmatrix}$$

The element  $D := 1 + x + y + x^3y + x^5y + x^7y$  may then be written as the array

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

while  $D^{(-1)} := 1 + x^7 + y + x^5y + x^3y + xy$  may be written as

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

The product of these two elements in the group ring will be the element

$$4 + 2G = \begin{bmatrix} 6 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \end{bmatrix}.$$

The subgroup  $\langle y \rangle$  is a normal subgroup of order two in  $G = C_8 \times C_2$  and so any image of a difference set in  $G$  must obey the equation  $f(D) \cdot f(D^{-1}) = 4 \cdot 1_H + 4H$  where  $H$  is isomorphic to the cyclic group of order 8. Our difference set, above, on mapping into  $C_8 = \langle x : x^8 = 1 \rangle$  becomes the group ring element  $f(D) = 2 + x + x^3 + x^5 + x^7 = 2 + x(\langle x^2 \rangle)$ . (Written as an array,  $f(D) = [2 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1]$ .)

One may verify that in  $\mathbb{Z}[C_8]$ ,  $f(D)f(D^{-1}) = 4 + 4C_8$ .

Suppose we wish to find *all*  $(16, 6, 2)$  difference sets in  $C_8 \times C_2$ . We instead search for all sets  $D$  of size six in this group  $G$  with the property that  $D \cdot D^{-1} = 4 + 2G$ . This search can then be aided by looking at smaller homomorphic images and first solving the equation  $f(D) \cdot f(D^{-1}) = 4 + 2f(G)$  in a factor group of  $G$ .

## 2.6 Equations In A Group

Given a finite group  $G$ , we examine the integral group ring  $\mathbb{Z}[G] := \{ \sum_{g \in G} a_g g : a_g \in \mathbb{Z} \}$ . This group ring is an algebra; it is commutative if and only if  $G$  is abelian. By an “equation in  $G$ ” we will mean an equation in the group ring  $\mathbb{Z}[G]$ .

Given a set  $S \subseteq G$ , we write  $S^{(t)} := \sum_{s \in S} s^t$ . We equate  $S$  with the sum of its elements, that is, we write  $S$  when we really mean,  $S^{(1)}$ . Thus  $G$  is the sum of the group elements of  $G$ . Note that if  $G$  is a group then  $G^{(t)} = G$  for all nonzero integers  $t$ , while  $G^2 = |G| \cdot G$ ; the parentheses are a crucial part of the notation.

If a combinatorial configuration has a regular automorphism group then the combinatorics of the configuration, the “counting” of various substructures, may be viewed as computations in the group ring  $\mathbb{Z}[G]$ . We are interested in studying certain equations in the group ring  $\mathbb{Z}[G]$  and applying the group theoretic results in an analysis of the underlying combinatorial configurations. This is a significant application of algebra to combinatorics and an area of much modern research.

We will sketch a number of examples of combinatorial objects which may also be viewed as “equations in groups.”

### 2.6.1 Distance Regular Graphs

The **distance** between two vertices  $x$  and  $y$  is the length of the shortest path between them.

A graph is **regular** of degree  $k$  if every vertex has degree  $k$ . The graph is **strongly regular** if it has the additional property that there exists integers  $\lambda$  and  $\mu$  such that given two distinct vertices  $x$  and  $y$ , the number of vertices adjacent to both is either  $\lambda$  or  $\mu$ , depending on whether  $x$  and  $y$  are adjacent or not.

Given a regular graph  $\Gamma$ , let  $N_i(x)$  represent all the vertices of distance  $i$  from  $x$ . Let  $d$  be the diameter of  $\Gamma$ . If two vertices,  $x, y$  are of distance  $i$ , we define  $p_{jk}^i(x, y)$  to be the number of vertices  $z$  such that  $d(x, z) = j$  and  $d(z, y) = k$ . If the parameter  $p_{jk}^i$  is independent of the pair  $x, y$  (and thus only depends on  $i$ , the distance between them), and if this is true for all  $i, j, k, 0 \leq i, j, k \leq d$ , then the graph is **distance regular**.

Given two vertices of distance  $k$ , we define  $p_{ij}^k(x, y)$  to be the number of vertices  $z$  of distance  $i$  from  $x$  and distance  $j$  from  $y$ . If this parameter only depends on  $k$ , never on  $x$  and  $y$ , then the graph is **distance regular**.

Distance regular graphs of diameter  $d$  have the special property that the adjacency matrix generates an algebra of dimension  $d + 1$  which is also closed under the “Hadamard” (entrywise) product. This phenomena provides a rich interplay between different areas of group theory, combinatorics and linear algebra.

Distance regular graphs of diameter two are said to be **strongly regular**. A **strongly regular graph** which is a Cayley graph  $C(S, G)$  is equivalent to the existence of a **partial difference set**  $S$  in  $G$ .

#### A strongly regular graph

Consider the group  $G = \langle x, y : x^3 = y^3 = [x, y] = 1 \rangle \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3$ . Let  $S = \{x, x^2, y, y^2\}$  and construct a graph on the vertices of  $G$  by defining two elements  $g$ , and  $h$  to be adjacent if and only if  $gh^{-1} \in S$ .

This graph is strongly regular with parameters  $(9,4,1,2)$ . Its adjacency matrix satisfies the equation  $A^2 = 4I + A + 2(J - I - A)$ , where  $J$  is the matrix of all ones. In the group ring  $\mathbb{Z}[G]$ , the element  $S = x + x^2 + y + y^2$  satisfies the equation  $S^2 = 4 \cdot 1 + S + 2(G - 1 - S)$ . The character values of the element  $S$  correspond to the eigenvalues of the matrix  $A$ .

### The cube – a distance regular graph of diameter 3

A cube has eight vertices and 12 edges. Place one vertex on the origin of three-space  $\mathbb{R}^3$  and three other vertices at  $(1, 0, 0)$ ,  $(0, 1, 0)$  and  $(0, 0, 1)$ . Since all eight vertices now have coordinates consisting solely of zeroes and ones, we might view these vertices as members of the elementary abelian group  $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ .

Or, we may start with  $G$ , the elementary abelian group of order 8, generated by involutions  $x, y$ , and  $z$  and define some sets which correspond to the edges of the cube.

Let  $S = \{x, y, z\} \subseteq G$ . Call two group elements  $g, h$  adjacent if  $gh^{-1} \in S$ . The graph thus formed on the eight members of  $G$  is exactly the graph of the cube.

Furthermore, set  $R_0 := 1, R_1 := x+y+z, R_2 := xy+xz+xyz$  and  $R_3 := xyz$ . Then the sets  $R_i$  partition the group  $G$ , (that is,  $G$ , written as a formal sum of group elements, is equal to  $R_0 + R_1 + R_2 + R_3$ ,) the  $R_i$  are fixed by inversion, ( $R_i = R_i^{(-1)} \forall i$ ) and the vector space  $\langle R_i : i = 0, 1, 2, 3 \rangle$  is an algebra of dimension 4. All of this means that the vertices and edges of the cube is a distance regular graph of diameter three with a regular automorphism group.

The strongly regular graphs are exactly the distance regular graphs of diameter 2. The graph of the cube, above, is distance regular of diameter 3.

Research question: Classify small distance regular graphs of diameter three with a regular automorphism group. Of special interest: graphs without triangles.

### 2.6.2 Difference Sets, Relative Difference Sets, Perfect Ternary Arrays

Let  $D$  be a subset of  $G$  of size  $k$  and suppose  $DD^{(-1)} = (k - \lambda)1 + \lambda G$ .  $D$  is said to be a  $(v, k, \lambda)$  **difference set** in  $G$ . The set of elements of  $G$  and the set of translates,  $\{gD : g \in G\}$  of  $D$  form a symmetric  $(v, k, \lambda)$  design. (Further information about difference sets may be found in [30], [57], or [?].)

The Fano plane may be created by the  $(7, 3, 1)$  difference set  $x + x^2 + x^4$  in the group  $\mathbb{Z}_7$ .

For which parameters  $(v, k, \lambda)$  do difference sets exist? Are there parameters  $(v, k, \lambda)$  for which there exist nonabelian groups with difference sets, but the abelian groups do not have difference sets? (If so, noncommutativity may play an important role in the theory of difference sets.)

Many difference sets are constructed using relative difference sets. Let  $G$  be a finite group with a normal subgroup  $N$ . Set  $n := |N|, m := [G : N]$  and suppose  $R$  is a subset of  $G$  such that  $RR^{(-1)} = (k)1 + \lambda(G - N)$ . The set  $R$  is called a **relative difference set** with respect to  $N$ . Obviously, not only are we interested in the parameters  $(m, n, k, \lambda)$  for the existence of these relative difference sets, but we might also ask if existence depends on the group  $G$  or the normal subgroup  $N$ . And what happens if we drop the normality condition on  $N$ ?

The existence of an  $(m, n, k, \lambda)$  relative difference set in a group  $G$  with normal subgroup  $N$  implies the existence of an  $(mn, k, n\lambda)$  difference set in the quotient group  $G/N$ . For this reason we may divide the parameters  $(m, n, k, \lambda)$  into four cases or types. These are:

**Type I, Semiregular:**  $(m, k, n\lambda) = (m, m, m)$ . Here  $k = m$  and so  $n\lambda = m$ . These exist for  $m$  a prime power, (Type IA) or, when a Hadamard difference set  $(4u^2, 2u^2 - u, u^2 - u)$  for  $m = 4u^2$  or  $m = 8u^2$  and  $n = 2$  (Type IB.)

**Type II, Affine type:**  $(m, k, n\lambda) = (m, m - 1, m - 2)$ . Here  $k = m - 1$  and  $n\lambda = m - 2 = k - 1$ .

**Type III, Singer type:**  $(m, k, n\lambda) = (\frac{q^{d+1}-1}{q-1}, q^d, q^d - q^{d-1})$ . These exist whenever there is a field of order  $q$ , that is, whenever  $q$  is a power of a prime.

**Types IV, General type:** all the others.

Suppose  $D := \sum_{g \in G} a_g g$  where  $a_g$  is 1, 0, or  $-1$ . If  $DD^{(-1)} = k1_G$ , then  $D$  is called a **perfect ternary array** (PTA.) (See [1].) These sets obey a group equation similar to that of difference sets and relative difference sets. Since we now allow  $-1$  as a coefficient, a PTA gives rise to a “positive” subset and a

“negative” subset in the group. (See [1] for an introduction to PTAs; see [43] for a PTA in the simple group  $A_5$ .)

For example, in the quaternion group  $Q_4$ , generated by  $i$  and  $j$  (where  $k = ij$ ,  $-k = ji$ ;  $i^2 = j^2 = -1$ ), the element  $D = 1 - (i + j + k)$  is a perfect ternary array. This perfect ternary array has been used to create a number of Hadamard difference sets in nonabelian groups of order  $2^{2d}$ .

### 2.6.3 Packings and Coverings in Groups

Given a group  $G$  and a natural number  $\lambda$ , we say that  $D \subseteq G$  is a  $\lambda$ -cover of  $G$  if

$$DD^{(-1)} = k \cdot 1 + \lambda G + S,$$

where  $S \in \mathbb{Z}[G]$  has nonnegative entries.

A  $(v, k, \lambda)$  difference set is a  $\lambda$  cover where  $S = 0$ . Think of a  $\lambda$ -cover as something “close” to a  $(v, k, \lambda)$  difference set. Given  $k, \lambda$ , we hope to find the largest group  $G$  with a  $\lambda$ -cover of size  $k$ ; we hope to minimize the size of the “error”  $S$ .

For example, suppose  $k = 7$  and  $\lambda = 1$ . A 1-cover in a group of order 43 would provide a  $(43, 7, 1)$  difference set and thus a projective plane of order 6. This does not exist. So, what is the largest group that has a 1-cover of size 7? In other words, how far from  $v = 43$  must we go to obtain a 1-cover?

One can fairly quickly rule out a 1-cover of size 7 in groups of order 42 and 41. Is there a group  $G$  of order 40 and a set  $D$  of order 7 such that  $DD^{(-1)} = 7 \cdot 1 + G + S$ ? (If so,  $S$  has size 2.) The answer is, Yes, but in only one group, according to a computer search using the software, GAP.

#### The group [40,3] in the GAP small group tables

The group [40,3] in the GAP small group tables has a 1-cover of size 7; this is the only group of order 40 to have a 1-cover.

[40,3] is a semidirect product (I think) of  $C_5$  by  $C_8$ . Set  $D = 1 + a + ab + b^2 + a^2b^2 + a^2b^4 + ab^5$  or  $D = 1 + a + ab + b^2 + a^2b^2 + ab^5 + a^4b^6$  where  $a$  has order 5 and  $b$  has order 8.

A nice little GAP project – lets look at all groups of order 100 or less, and various small values of  $\lambda$ . Here are some research problems in packings and coverings:

1. Find parameters  $(v, k, \lambda)$  for which there are packings in nonabelian groups but not in abelian groups.
2. Classify the sets  $S$  which occur in  $(v, k, 1)$  coverings or packings of groups. (Note that  $(G, S)$  is a Cayley graph.)

### 2.6.4 Matrices with constant line sum

An  $n \times n$  matrix with constant row and column sum may be viewed as an element of  $\mathbb{Z}[S_n]$ . Given a particular matrix,  $M$ , what is the smallest subgroup  $G$  of  $S_n$  such that the matrix is embeddable in  $\mathbb{Z}G$ ?

For example, the matrix

$$\begin{pmatrix} 0 & a & b \\ b & 0 & a \\ a & b & 0 \end{pmatrix}$$

may be viewed as an element of the group ring  $\mathbb{Z}[C_3]$ . (Think of it as  $aX + bX^2$  where

$$X = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.)$$

However, the matrix

$$\begin{pmatrix} 0 & a & b \\ 0 & b & a \\ a+b & 0 & 0 \end{pmatrix}$$

is not in  $\mathbb{Z}[C_3]$ . But this last matrix may be viewed as a member of the group ring  $\mathbb{Z}[S_3]$ , where  $S_3$  is generated by the matrices

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Take a strongly regular graph, such as the Petersen graph, with parameters  $(10,3,0,1)$ , and ask, what is the smallest group on which this adjacency matrix is in (may be mapped into) the group algebra? (There will be a relationship between this group and  $S_5$ , the full automorphism group of the Petersen graph.) There is a connection between matrices with constant line sums and doubly stochastic matrices and magic squares. (See [40].)

An  $n \times n$  matrix which is a circulant may be viewed as a member of  $\mathbb{Z}[C_n]$ .

### 2.6.5 Factoring Groups and other projects

**Factoring Groups.** Two subsets  $H$  and  $K$  of a group  $G$  are said to **factor**  $G$  if  $HK = G$ . The factoring is trivial if  $H$  or  $K$  is a subgroup of  $G$ . We seek nontrivial factorings. The two subsets form a **near-factor** of  $G$  if  $HK = G - 1$ . See Caen, Gregory, Hughes [8] and Schmidt, Simion [63] for some open questions on factors and near-factors of finite groups.

**Polynomial Addition Sets.** Let  $f(x)$  be a polynomial with integer coefficients. Let  $S$  be a subset of a group such that  $f(S) = \lambda G$  for some integer  $\lambda$ . Then  $S$  is a **polynomial addition set**. See [45], where the focus is on quadratic polynomials (eg. strongly regular graphs) and cyclic polynomials  $f(x) = x^m - d$ .

Research question: If  $f$  is a quadratic irreducible polynomial, are there any abelian groups, other than  $p$ -groups, which have an  $f$ -addition set?

See the paper [45] (and dissertation) of S. L. Ma for more on polynomial addition sets.

**Difference Families.** Let  $D_1, D_2, D_3, \dots, D_n$  be a collection of subsets, all of cardinality  $k$ , of a group  $G$  with the property that  $\sum D_i D_i^{(-1)} = k \cdot 1 + \lambda G$ . Then the set  $\{D_i : i = 1, \dots, n\}$  is a **difference family** in  $G$ .

For example, if  $G = Z_{13}$ , the cyclic group of order 13, then  $D_1 = \{0, 1, 4\}$ ,  $D_2 = \{0, 2, 8\}$  is a difference family. If  $k = 3$  and  $\lambda = 1$ , Cameron ([9], page 118) calls these Netto systems. They are constructed using finite fields and in turn, allow one to construct Steiner triple systems.

**Williamson Matrices.** Williamson matrices are constructed from objects  $A, B, C, D$  in a group of order  $v$ ; these give a Hadamard matrix of order  $4v$ .

**Generalizations.** Suppose  $X = \bigcup_{i=1}^t X_i$  is a set of size  $vt$  and a group  $G$  of order  $v$  acts regularly on each of the orbits  $X_i$ . A subset  $Y \subseteq X$  with  $G$  as an automorphism group may be viewed as a collection of elements  $D_i \in \mathbb{Z}[G]$ .

Some combinatorial objects can be constructed from in this way;  $G$  does not act transitively on the point set  $X$  but partitions the point set into a collection of orbits all of equal size.

In a similar way, if  $G$  fixes a single point and acts regularly on a collection of orbits, we may view the subconfigurations thus created as elements  $D_i \in \mathbb{Z}[G]$ .

There are other generalizations ... Poincot's generalized difference sets, for example...

### 2.6.6 Research projects

Some open problems:

1. Which groups have  $(96, 20, 4)$  difference sets?
2. Which groups have  $(64, 28, 12)$  difference sets?

3. Is there a  $(160, 54, 18)$  difference set?
4. Is there a  $(288, 42, 6)$  difference set?
5. Which groups of order 16 or 32 have relative difference sets?
6. Are there relative difference sets where  $m$  and  $n$  are relatively prime?
7. Which groups have a  $(9, 9, 9, 1)$  relative difference set?
8. Which small groups have affine difference sets?
9. Is there a  $(12, 6, 12, 2)$  relative difference set?
10. Classify the Cayley graphs  $(G, S)$  which occur in  $(v, k, 1)$  coverings or packings of groups.
11. Construct  $(4\lambda + 3, 2\lambda + 1, \lambda)$  designs by assuming a group of order  $k = 2\lambda + 1$  fixes a point and acts regularly on two sets  $X_1, X_2$ .

(We could use the software *GAP* to search through small groups for these combinatorial objects.)

### 2.6.7 Summary

The group ring  $R[G]$  provides a natural framework for solving combinatorial equations in which the combinatorial design has a sharply transitive automorphism group. In the next section we will see how computations in the group ring  $R[G]$  may be aided by  $R$ -representations of the group  $G$ .