

Authors' Notes, April 16, 2007.

This section introduces characters and idempotents with an emphasis on the idempotent point of view. (I have changed the name of this section and added a subsection on examples, April 2007.)

It includes some elementary Galois theory.

It *could* be expanded to nonabelian groups.

Finish the “canonical” way to define characters?

Do I (Ken) prove all the idempotent results carefully enough?

It contains Lemmas 7-12, Corollaries 1 and 2.

K is a field here. (What do I do about that? Change these to F ?)

The sections are

1. Basic facts . . .
2. Idempotents associated with a character
3. Galois theory and characters
4. Nonabelian groups
5. Examples

3 Group Characters and Their Idempotents

3.1 Basic facts about representations

Given an integer t , set $\zeta_t := e^{2\pi i/t}$.

We assume, throughout this section, that G is a finite abelian group. (There are natural generalizations to nonabelian groups, but we will not do them here.) The exponent of G is the least common multiple of the orders of the elements of G ; we will assume that G has exponent t and that $K := \mathbb{Q}(\zeta_t)$ is a subfield of the complex numbers containing all solutions to $x^t = 1$.

A **K -representation** of G is a homomorphism of G into the multiplicative group $GL_m(K)$ of non-singular matrices with entries from the field K . The **degree** of the representation is the integer m , the size of the ring of matrices. A representation is **linear** if the degree of the representation is 1. In this case, the representation is merely a homomorphism into the multiplicative group of K . The trace $tr(A)$ of a matrix A is the sum of the diagonal elements, $tr(A) := \sum_{i=1}^m A_{i,i}$. The **character** of a representation ϕ is the function $\chi : G \rightarrow K$ defined by $\chi(g) = tr(\phi(g))$. If a representation is linear then we will not distinguish between the character and the representation. In particular, if G is abelian, it is customary to use “character” instead of “linear representation.”

The linear representation χ_0 defined by $\chi_0(g) = 1, \forall g \in G$ is called the principal (or trivial) character.

If G is abelian then define G^* to be the set of characters (linear representations) of G . The set G^* is the **dual group** of G and is a group under coordinatewise multiplication ($\chi\psi(g) := \chi(g)\psi(g)$). The group G^* is isomorphic to G .

A finite abelian group G is isomorphic to a direct product of r cyclic groups. The integer r is uniquely defined and is called the **rank** of G . Given a set of r generators x_1, x_2, \dots, x_r so that $G = \langle x_1 \rangle \times \langle x_2 \rangle \times \dots \times \langle x_r \rangle$, we may uniquely define a character by its image on the set $\{x_i : 1 \leq i \leq r\}$. Suppose x_i has order b_i and set $\zeta_{b_i} := e^{\frac{2\pi i}{b_i}}$ equal to a particular b_i -th root of unity. The image of x_i under a character χ is $\zeta_{b_i}^j$ for some integer $j, 0 \leq j < b_i$. Each character of G then provides a unique r -tuple (j_1, j_2, \dots, j_r) where $\chi(x_i) = \zeta_{b_i}^{j_i}$. We will write $\chi_{j_1, j_2, \dots, j_r}$ for the character which maps x_i to $\zeta_{b_i}^{j_i}$. Thus $G^* = \{\chi_{j_1, j_2, \dots, j_r} : 0 \leq j_i < b_i\}$.

We will wish to more precisely identify the set of generator $\{x_i\}$. The abelian group G is a direct product of Sylow p -subgroups, $G := \otimes \prod P_i$. An abelian subgroup P_i of order p^{b_i} is generated by elements x_1, x_2, \dots, x_{d_i} where d_i is the rank of P_i and we may assume the order of x_{i+1} divides the order of x_i .

We may order the primes p_1, \dots, p_t dividing the cardinality of G and then, for each prime p in this list, choose a basis of the Sylow- p subgroup so that the elements x_i have orders which do not increase as i increases.

Once we have identified a generating set for an abelian G , the notation χ_{j_1, \dots, j_r} for a character is well-defined.

If R is a subring of $\mathbb{C}[G]$, we may extend a character χ by linearity to the group ring $R[G]$, defining

$$\chi\left(\sum_{g \in G} \alpha_g g\right) = \sum_{g \in G} \alpha_g \chi(g).$$

3.1.1 The Fourier transform

Given an abelian group G with dual group G^* we may define a map $\hat{F} : \mathbb{C}[G] \rightarrow \mathbb{C}[G^*]$ as follows.

$$\hat{F}(Y) := \sum_{\chi \in G^*} \chi(Y) \chi.$$

The function \hat{F} is the **Fourier transform** of the abelian group G .

The characters $\chi \in G^*$ form (of course) the standard basis for $\mathbb{C}[G^*]$.

References. See Ledermann's text, [39], for a good introduction to representations and characters. Other **references** are Curtis and Reiner, [10], Milies and Sehgal, [55] Gorenstein, chapters 3 and 4, [19], pp. 58-171. Gorenstein, chapter 4, introduces character theory; the inner product on characters defined on p. 120 of Gorenstein.

3.2 The idempotent associated with a character

Given a character $\chi : G \rightarrow (\mathbb{C}^*, \cdot)$, we define the group ring element

$$e_\chi := \frac{1}{|G|} \sum_{g \in G} \chi(g) g^{-1} = \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)} g.$$

(See Ledermann [39], Milies-Sehgal [55], Theorem 5.1.11, p. 185.)

The group ring elements e_χ are important members of the group ring $\mathbb{C}[G]$. In particular, $\hat{F}(e_\chi) = \chi$, that is, the elements e_χ are mapped, by the Fourier transform, to the standard basis elements of $\mathbb{C}[G^*]$.

We make a series of observations about the elements e_χ .

Given, K , a subfield of the complex numbers, define (as in a previous section) an inner product on $K[G]$ by $\langle \alpha, \beta \rangle := \frac{1}{|G|} \sum a_g \overline{b_g}$. If χ is a character of G then we can verify directly that $\langle e_\chi, e_\chi \rangle = 1$. Similarly $\chi(e_\chi) = 1$.

Since the sum $\sum_{j=0}^{t-1} \zeta_t^j$ of all the t -th roots of unity is zero then if $\chi \neq \chi'$ we have $\langle e_\chi, e_{\chi'} \rangle = 0$. Equivalently, $\chi(e_{\chi'}) = 0$. Thus the set $\{e_\chi : \chi \in G^*\}$ is an orthonormal set and so is an independent set in the vector space $\mathbb{C}[G]$. Since the cardinality of G^* is that of G , which is the dimension of $\mathbb{C}[G]$ as a \mathbb{C} -vector space, then $\{e_\chi : \chi \in G^*\}$ is an orthonormal basis for $\mathbb{C}[G]$.

A basis of a vector space provides a coordinate system for the elements of the space. Every element of the vector space has a unique representation as a linear combination of the basis elements. So, given $X \in \mathbb{C}[G]$, we wish to determine the "coordinates" x_χ so that we may write $X = \sum_{\chi \in G^*} x_\chi e_\chi$. Applying a specific character χ to both sides of this equation, we see that $\chi(X) = x_\chi$, that is,

$$X = \sum_{\chi \in G^*} \chi(X) e_\chi.$$

As a result of the uniqueness of coordinates of an element with respect to a basis, we also have that $X = Y$ iff and only if $\chi(X) = \chi(Y)$ for all $\chi \in G^*$.

We now have two different bases for the group ring $\mathbb{C}[G]$. The first basis is the standard basis $\{g : g \in G\}$. The second basis is the **dual basis** $\{e_\chi : \chi \in G^*\}$.

We are especially interested in subsets of the group G . If a combinatorial object is a special subset $X \subseteq G$ of a group G then as a group ring element, X has coordinates zeroes and ones with respect to the standard basis $\{g : g \in G\}$. (Thus the standard basis reveals the “setness” of X .) But many special combinatorial objects will be determined by the character values of the set X ; these will be the coordinates of X under the dual basis. We will attempt to use both bases, in a finite “Fourier” analysis of the combinatorial object X .

The character table of G serves as a change of coordinates matrix for this change of basis. (Let M be the character table of G , written as a matrix with columns labeled by the standard basis of G and rows labeled by the characters. An element $X \in \mathbb{C}[G]$ may be written in two ways: $X = \sum_{g \in G} \alpha_g g = \sum_{\chi \in G^*} \beta_\chi e_\chi$. Write α for the column vector with entries α_g and β for the column vector with entries β_χ . Then $\beta = M\alpha$.)

Critical

Lemma 7 (Critical Lemma)

Let G be a finite abelian group. Any element $X \in \mathbb{C}[G]$ is uniquely defined by its images under the characters $\chi \in G^*$. Indeed, $X = \sum_{\chi} \chi(X) e_\chi$.

The elements e_χ are “primitive idempotents” of the ring $\mathbb{C}[G]$. We mean by this that, there are no idempotents e_1, e_2 such that $e_\chi = e_1 + e_2$. In addition, the set $\{e_\chi : \chi \in G^*\}$ are “orthogonal”: given characters χ , and ψ , then $e_\chi e_\psi = 0$ if $\chi \neq \psi$.

Xe

Corollary 1 Let $X \in \mathbb{C}[G]$ and $\chi \in G^*$. Then $Xe_\chi = \chi(X)e_\chi$.

Proof (of corollary 1.) Clearly the group ring elements Xe_χ and $\chi(X)e_\chi$ have the same image, $\chi(X)$, under the character χ . But their image under any other character $\chi' (\chi' \neq \chi)$ is zero, so Xe_χ and $\chi(X)e_\chi$ have identical images under *all* characters of G and so, by Lemma 7, are equal. ■

3.2.1 Aliases

The importance of Corollary 1 must be stressed. Given a character χ , if Y is *any* element of the group ring such that $\chi(Y) = \chi(X)$, then since $Xe_\chi = \chi(X)e_\chi = \chi(Y)e_\chi = Ye_\chi$, we may use $\chi(X)e_\chi, Xe_\chi$ and Ye_χ interchangeably. This simple argument turns out to be a powerful tool. Lemma 7 and the combinatorial incentive to work in $\mathbb{Z}[G]$ suggest the following definition.

Definition. Let X be an element of $\mathbb{Z}[G]$ (G abelian) and χ a character of G . An element $A \in \mathbb{Z}[G]$ is a χ -**alias** for X if $\chi(A) = \chi(X)$. More generally, if $\Phi = \{\chi_1, \chi_2, \dots, \chi_t\}$ is a set of characters of G then A is a Φ -**alias** for X if $\chi_j(X) = \chi_j(A), \forall \chi_j \in \Phi$. It should be stressed that an alias is a member of the integral group ring $\mathbb{Z}[G]$, not necessarily a member of the field \mathbb{C} . If Φ is a proper subset of the dual group G^* , then there will likely be many different Φ -aliases for a fix element $X \in \mathbb{Z}[G]$.

If X is a combinatorial object, a special subset $X \subseteq G$ of G , then X is (viewed as being) in the integral group ring $\mathbb{Z}[G]$. The concept of an “alias” allows us to carry character values into the integral group ring and so do “combinatorial” and “Fourier” analysis simultaneously.

By the orthogonality relations, any sum of the primitive idempotents is also an idempotent, indeed, the identity of the ring $\mathbb{C}[G]$ is the sum of all the primitive idempotents, $1 = \sum_{\chi} e_\chi$ and so we have the interesting statement:

$$X = \sum_{\chi \in G^*} \chi(X) e_\chi = \sum_{\chi \in G^*} X e_\chi.$$

Note that in the first sum we are multiplying the basis elements by scalars (“coordinates”) $\chi(X)$ and in the second sum we are multiplying the basis elements by the group ring element X .

Obviously X itself is a G^* -alias for X , so, given $X \in \mathbb{Z}[G]$, χ -aliases of X exist for all χ . In practice, X will be unknown but we will have some information about $\chi(X)$ and so will construct some aliases for X . Our goal is to construct X by building up the sum

$$X = \sum_{\chi \in G^*} A_\chi e_\chi$$

where each element A_χ is a χ -alias of X . This constructive approach will be detailed in a later section.

(See Ledermann [39], or Milies-Sehgal [55] for further details.)

3.2.2 An equivalence relation on characters

We give some basic facts on characters. (Recall that $\zeta_m := e^{2\pi i/m}$.)

A character χ maps a finite group G into a finite subgroup of the multiplicative group $S^1 := \{z \in \mathbb{C} : |z| = 1\}$. Every finite subgroup of S^1 is cyclic and so the factor group $G/Ker(\chi)$ is cyclic, say of order m , and is generated by some element $gKer(\chi)$ where $\chi(g) = \zeta_m$.

A character χ maps the group G into the complex numbers under multiplication. The kernel $Ker(\chi)$ of χ is the subgroup of G of all elements mapped by χ to 1.

Definition. The **order** of a character χ is the cardinality of the factor group $G/Ker(\chi)$.

There are several equivalent definitions of the order of a character:

Lemma 8 *The character χ has order m if and only if G is mapped onto the set $\langle \zeta_m \rangle := \{(\zeta_m)^j : j \in \mathbb{Z}\}$. The order of $\chi \in G^*$ is then the least positive integer m such that, in G^* , $\chi^m = 1_{G^*}$.*

The proof of this lemma is just the Fundamental Homomorphism Theorem: $G/Ker(\chi) \cong \langle \zeta_m \rangle \cong \langle \chi \rangle$.

Definition. We define $\chi \sim \chi' \iff Ker(\chi) = Ker(\chi')$. This is an important relation on characters.

Lemma 9 *The relation \sim on G^* is an equivalence relation.*

The proof of this lemma is straightforward.

Given a group G with dual group G^* , we write G^*/\sim for the set of equivalence classes of characters.

Lemma 10 *If G is cyclic and χ, χ' are characters of G , then $\chi \sim \chi'$ if and only if χ, χ' have the same order.*

Definition. Given an element $X \in \mathbb{Z}[G]$, we say X divides $Y \in \mathbb{Z}[G]$ if there exists an element $Z \in \mathbb{Z}[G]$ such that $Y = XZ$. (We will be primarily interested in the case where $X \in \mathbb{Z}$ is an integer.) We say $Y \equiv Z \pmod X$ if X divides $Y - Z$.

3.3 Galois theory and characters

A bijection of a field which preserves the two operations of addition and multiplication is an **automorphism** of a field. The collection of field automorphisms of K fixing the rationals \mathbb{Q} is the Galois group of K , often written $Gal_{\mathbb{Q}}(K)$. We will assume that the ground field is the field of rationals, \mathbb{Q} , and often write $\Gamma(K)$ for $Gal_{\mathbb{Q}}(K)$.

If G is finite with exponent m then the splitting field of G is $\mathbb{Q}(\zeta_m)$ where $\zeta_m := e^{\frac{2\pi i}{m}}$. Define the map $\sigma_j : \{\zeta_m^i\} \rightarrow \{\zeta_m^i\}$ by $\sigma_j(\zeta_m^i) = (\zeta_m^i)^j$ and extend this map by linearity to all of $\mathbb{Q}(\zeta_m)$. If j is relatively prime to m then σ_j is a member of $\Gamma(\mathbb{Q}(\zeta_m))$. Indeed, all members of the Galois group take this form. Therefore the Galois group $\Gamma(\mathbb{Q}(\zeta_m)) = \{\sigma_j : (j, m) = 1\}$ of $\mathbb{Q}(\zeta_m)$ is isomorphic to the multiplicative group, $U(m)$, of units of m .

charorder

equivrel

orderandequiv

Given an intermediate field K , $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$, with Galois group $\Gamma(K)$, we say that elements $k_1, k_2 \in K$ are **algebraically conjugate** if there is an element σ of the Galois group $\Gamma(K)$ such that $\sigma(k_1) = k_2$.

If σ is a Galois automorphism then we may use the standard basis $\{g : g \in G\}$ of $\mathbb{C}[G]$ to extend σ by linearity to all of $\mathbb{C}[G]$, defining

$$\sigma\left(\sum_{g \in G} \alpha_g g\right) := \sum_{g \in G} \sigma(\alpha_g) g.$$

This makes σ into a \mathbb{Q} -algebra isomorphism, that is, σ preserves sums and products and treats rational numbers as scalars.

Suppose $\chi : G \rightarrow S^1 \subset \mathbb{C}^*$ is a character. Then so is the function $\sigma\chi$. Thus we may also extend Galois automorphisms to act on characters. We say that two characters χ_1 and χ_2 are **algebraically conjugate** if there is an automorphism σ of the Galois group such that $\sigma\chi_1 = \chi_2$.

The relation of algebraic conjugacy is an equivalence relation on characters. But it is a relation we have already seen. . .

Lemma 11 *Let G be an abelian group. Two characters are algebraically conjugate if and only if they have the the same kernel.*

Proof If there exists a Galois automorphism σ such that $\chi_2 = \sigma\chi_1$ then $\sigma^{-1}\chi_2 = \chi_1$ and so $\chi_1(g) = 1$ if and only if $\chi_2(g) = 1$. Thus equivalent characters have the same kernel.

Conversely, if $\chi_1 \sim \chi_2$, then $\text{Ker}(\chi_1) = \text{Ker}(\chi_2)$. Write $K = \text{Ker}(\chi_1)$. The factor group G/K is equivalent to a cyclic group C_m of order m , isomorphic to the multiplicative group $\langle \zeta_m \rangle$ in $\mathbb{Q}(\zeta)$. (See Lemma 8.) The automorphism group of C_m is the group of units $U(m)$, isomorphic to the Galois group $\Gamma(\mathbb{Q}(\zeta_m))$. The group $U(m)$ is transitive on the generators of C_m so given a generator gK of the factor group G/K , there is a Galois automorphism σ mapping $\chi_1(g)$ to $\chi_2(g)$. This forces $\chi_2 = \sigma\chi_1$.

Lemma 11 tells us that the relation of “algebraic conjugacy” on characters is the relation \sim defined earlier.

The Galois automorphisms of $\mathbb{Q}(\zeta_m)$ fixing \mathbb{Q} may be extended in by linearity to the group ring $\mathbb{Q}(\zeta_m)[G]$: given $\sigma \in \Gamma$, define

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

Since each automorphism σ fixes \mathbb{Q} , it will fix any member of $\mathbb{Q}[G]$. A combinatorial object viewed as a member of $\mathbb{Q}[G]$ is fixed by these automorphisms. This allows us to simplify our search for combinatorial objects by focusing *only* on the “rational idempotents”, the sum of certain primitive complex idempotents under the action of the Galois group.

Lemma 12 *Let $\zeta_m := e^{2\pi i/m}$. The Galois group $\Gamma := \text{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_m))$ is isomorphic to $U(m) := \{a : \text{GCD}(a, m) = 1\}$, the multiplicative group of units of \mathbb{Z}_m . Indeed, the Galois group is precisely those functions which map ζ to ζ^a where $a \in U(m)$. The set of elements of $K := \mathbb{Q}(\zeta_m)$ fixed by all $\sigma \in \Gamma$ is precisely \mathbb{Q} .*

Suppose two characters χ and ψ have the same kernel, and thus $\chi \sim \psi$. There is a Galois automorphism σ of $\mathbb{Q}(\zeta_m)$ such that as functions, $\chi = \sigma\psi$. This automorphism is uniquely determined by χ and ψ , that is, the size of the equivalence class of a character χ is the cardinality of $U(m)$.

3.4 Nonabelian Groups

Much of the material discussed in this section carries over to the situation where G is a nonabelian group. We replace “characters” by “representations”, “ideals” by “left ideals”, and so on.

The main idea of this section is the change of basis from the standard basis $\{g : g \in G\}$ of the group ring to a “Fourier” basis related to the characters. If G is nonabelian, this change of basis to a “Fourier” basis of idempotents is more complicated. The irreducible representations of degree $d > 1$ no longer correspond to a single primitive idempotent, but instead can be associated with d^2 elements in the “Fourier” basis. Given a representation ϕ of degree d , we might describe an element $e_{\phi(s,t)}, 1 \leq s, t, \leq d$ which has the property that $\chi(e_{\phi(s,t)}) = 0$ for all other irreducible representations χ while $\phi(e_{\phi(s,t)})$ is a $d \times d$ matrix with a 1 in the (s,t) entry and zeroes elsewhere. If $s \neq t$, then this element is not an idempotent; if $d > 1$ this element $e_{\phi(s,t)}$ is not in the center of $\mathbb{Z}[G]$. A basis for $\mathbb{C}[G]$ may then be formed by the set of all such $e_{\phi(s,t)}$ as s, t range through the interval $1 \leq s, t \leq \deg(\phi)$ and ϕ ranges through the set of irreducible representations of G . This new basis is of value in computations in $\mathbb{Z}[G]$ but it is no longer a basis of central primitive idempotents.

Often, given a nonabelian group G with a putative difference set, one may work with the largest abelian homomorphic image G/G' and apply the character theory to the integral group ring $\mathbb{Z}[G/G']$. In many cases this gives sufficient information to rule out a difference set.

3.5 Some Examples

We conclude this section with some small examples and exercises, motivated by combinatorial configurations. (All of the objects below have combinatorial significance.)

Exercises

1. Write the set $D = 1 + x + x^3 \in \mathbb{C}[C_8]$ as a linear combination of primitive idempotents e_χ . We will collect terms as much as possible.

Solution. The group $G = C_8$ has eight characters. Let $\zeta_8 = e^{\pi i/4}$ and label the characters $\chi_j, (j = 0, 1, 2, \dots, 7)$ where $\chi(x) = \zeta_8^j$. Then the dual group is $G^* = \{\chi_j\}$.

Four characters $(\chi_1, \chi_3, \chi_5, \chi_7)$ send x to a primitive 8-th root of unity and so send D to either $1 + \sqrt{2}i$ or $1 - \sqrt{2}i$.

Two characters (χ_2, χ_6) send x to either i or $-i$ and so map D to 1.

If $x \mapsto -1$ then $D \mapsto -1$; if $x \mapsto 1$ then D maps to 3.

Thus

$$D = 3e_{\chi_0} - e_{\chi_4} + (e_{\chi_2} + e_{\chi_6}) + (1 + \sqrt{2}i)(e_{\chi_1} + e_{\chi_3}) + (1 - \sqrt{2}i)(e_{\chi_5} + e_{\chi_7}).$$

2. Write the set $D = x + x^2 + y + y^2 = (\langle x \rangle - 1) + (\langle y \rangle - 1) \in \mathbb{C}[C_3 \times C_3]$ as a linear combination of primitive idempotents e_χ . Collect terms as much as possible. Verify that D gives a partial difference set by checking that the character values are -2 and 1 (as long as the character is nontrivial.)
3. Write the set $D = 1 + x + x^2 + x^3 y \in \mathbb{C}[C_4 \times C_2]$ as a linear combination of primitive idempotents e_χ . Collect terms as much as possible.
4. Write the difference set $D = x + x^2 + x^3 + y + y^2 + y^3 = (\langle x \rangle - 1) + (\langle y \rangle - 1) \in \mathbb{C}[C_4 \times C_4]$ as a linear combination of primitive idempotents e_χ . (Collect terms as much as possible.)
5. Write the difference set $D = 1 + x^3 + x^5 + x^7 + y + xy \in \mathbb{C}[C_8 \times C_2]$ as a linear combination of primitive idempotents e_χ . (Collect terms as much as possible.)