Finite Groups, Representation Theory and Combinatorial Structures *

J Moori
School of Mathematical Sciences, North-West University (Mafikeng)
Mmabatho, 2375, South Africa †

May 19, 2015

Abstract

We introduce background material from Finite Groups and Representation Theory of Finite Groups (Linear and Permutation Representations). We introduce the reader to combinatorial structures such as Designs and Linear Codes and will discuss some of their properties, we also give few examples. We aim to introduce two new methods for constructing codes and designs from finite groups (mostly simple finite groups). We outline some of recent collaborative work by the author with J D Key, B Rorigues and T Le.

Keywords: Group, representation, character, simple groups, maximal subgroups, conjugacy classes, designs, codes.

1 Introduction

Error-correcting codes that have large automorphism groups are useful in applications as the group can help in determining the code's properties, and can be useful in decoding algorithms: see Huffman [15].

In a series of 3 lectures given at the NATO Advanced Study Institute "Information Security and Related Combinatorics" held in Croatia [28], we discussed two methods for constructing codes and designs for finite groups (mostly simple finite groups). The first method dealt with construction of symmetric 1-designs and binary codes obtained from from the action on the maximal subgroups, of a finite group G. This method has been applied to several sporadic simple groups, for example in [18], [22], [23], [31], [32], [33] and [34]. The second method introduces a technique from which a large number of non-symmetric 1-designs could be constructed. Let G be a finite group, M be a maximal subgroup of G and $C_g = [g] = nX$ be the conjugacy class of G containing g. We construct $1-(v, k, \lambda)$ designs $\mathcal{D} = (\mathcal{P}, \mathcal{B})$, where $\mathcal{P} = nX$ and $\mathcal{B} = \{(M \cap nX)^y | y \in G\}$. The parameters v, k, λ and further properties of $\mathcal{D}$ are determined. We also study codes

*AMS Subject Classification (2000): 20D05, 05B05.
†Supports from CIMPA, NRF, University of North-Westl and AIMS are acknowledged.

associated with these designs. In Subsections 5.1, 5.2 and 5.3 we apply the second method to the groups A_7, $PSL_2(q)$ and J_1 respectively.

Our notation will be standard, and it is as in [2] for designs and codes. For groups we use $\mathbb{ATLAS}$ [5]. For the structure of finite simple groups and their maximal subgroups we follow the $\mathbb{ATLAS}$ notation. The groups $G.H$, $G:H$, and $G^{\cdot}H$ denote a general extension, a split extension and a non-split extension respectively. For a prime p, p^n denotes the elementary abelian group of order p^n. If G is a group and M is a G-module, the **socle** of M, written $\mathrm{Soc}(M)$, is the largest semi-simple G-submodule of M. It is the direct sum of all the irreducible G-submodules of M. Determination of $\mathrm{Soc}(V)$ for each of the relevant full-space G-modules $V = F^n$ is highly desirable.

2 Permutation Groups

2.1 Permutation Representations

Theorem 2.1 (Cayley) *Every group G is isomorphic to a subgroup of S_G. In particular if $|G| = n$, then G is isomorphic to a subgroup of S_n.*

Proof: For each $x \in G$, define $T_x : G \longrightarrow G$ by $T_x(g) = xg$. Then T_x is one-to-one and onto; so that $T_x \in S_G$. Now if we define $\tau : G \longrightarrow S_G$ by $\tau(x) = T_x$, then τ is a monomorphism. Hence $G \cong Image(\tau) \leq S_G$. ∎

Definition 2.1 *The homomorphism τ defined in Theorem 2.1 is called the* **left regular representation** *of G.*

Note: *Cayley's Theorem is not that useful when the group G is large or when G is simple. Following results (Theorem 2.3 and Corollary 2.4) provide substantial improvement over Cayley's Theorem. Notice that $A_5 \leq S_5$ and Cayley's Theorem asserts that A_5 is also a subgroup of S_{60}.*

Corollary 2.2 *Let $GL(n, \mathbb{F})$ denote the* **general linear group** *over a field $\mathbb{F}$. If G is a finite group of order n, then G can be embedded in $GL(n, \mathbb{F})$, that is G is isomorphic to a subgroup of $GL(n, \mathbb{F})$.*

Proof: Let T_x be as in Cayley's Theorem. Assume that $G = \{g_1, g_2, \cdots, g_n\}$. Let $P_x = (a_{ij})$ denote the $n \times n$ matrix given by $a_{ij} = 1_{\mathbb{F}}$ if $T_x(g_i) = g_j$ and $a_{ij} = 0_{\mathbb{F}}$, otherwise. Then P_x is a **permutation matrix**, that is a matrix obtained from the identity matrix by permuting its columns. Define $\rho : G \longrightarrow GL(n, \mathbb{F})$ by $\rho(x) = P_x$, then it is not difficult to check that ρ is a monomorphism. ∎
Note: *If $\mathcal{P}_n$ denotes the set of all $n \times n$ permutation matrices, then $\mathcal{P}_n$ is a group under the multiplication of matrices and $\mathcal{P}_n \cong S_n$.*

Example 2.1 Consider the Klein four group $V_4 = \{e, a, b, c, \}$. Then we have

$$T_a(e) = a.e = a,\ T_a(a) = a^2 = e,\ T_a(b) = ab = c,\ T_a(c) = ac = b;$$

$$T_b(e) = b,\ T_b(a) = c,\ T_b(b) = e,\ T_b(c) = a;$$

$$T_c(e) = c,\ T_c(a) = b,\ T_c(c) = e,\ T_c(b) = a.$$

Hence the permutation matrices are

$$P_e = I_4, \quad P_a = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad P_b = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad P_c = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

So that $V_4 \cong \{I_4,\ P_a,\ P_b,\ P_c\} \leq GL(4, \mathbb{F})$

Exercise 2.1 (i) Show that for $n \geq 2$, S_n is isomorphic to a subgroup of A_{n+2}. (ii) Use part (i) to show that A_∞ contains an isomorphic copy of every finite group. (See below for the definition of A_∞.)

Definition 2.2 *Let $X = \mathbb{N}$ and let F be the set of all $\alpha \in S_X$ such that α moves finitely many elements of X. Then $F \leq S_X$. Let A_∞ denote the subgroup of F generated by all 3-cyles of F. It can be shown that A_∞ is a simple group.*

Theorem 2.3 (Generalized Cayley Theorem) *Let H be a sugroup of G and let X be the set of all left cosets of H in G. Then there is a homomorphism $\rho : G \longrightarrow S_X$ such that*

$$Ker(\rho) = \bigcap_{g \in G} gHg^{-1}.$$

Proof: For any $x \in G$, define $\rho_x : X \longrightarrow X$ by $\rho_x(gH) = x(gH)$. Then ρ_x is well-defined, one-to-one and onto. So that $\rho_x \in S_X$. Now define $\rho : G \longrightarrow S_X$ by $\rho(x) = \rho_x$ for all $x \in G$. Then ρ is a homomorphism. We claim that $Ker(\rho) = \bigcap_{g \in G} gHg^{-1}$.

Let $x \in Ker(\rho)$. Then $\rho_x = \rho(x)$ is the identity permutation on X. Hence $\rho_x(gH) = gH$ for all $g \in G$. So that $xgH = gH$, $\forall g \in G$. So $g^{-1}xg \in H$, $\forall g \in G$. This implies that $x \in gHg^{-1}$, $\forall g \in G$. Thus $Ker(\rho) \subseteq \bigcap_{g \in G} gHg^{-1}$. Now if $x \in \bigcap_{g \in G} gHg^{-1}$, then $x \in gHg^{-1}, \forall g \in G$. So that $xgH = gH$ for all $g \in G$, that is ρ_x is the identity permutation. Hence $x \in Ker(\rho)$, so $\bigcap_{g \in G} gHg^{-1} \subseteq Ker(\rho)$. ■

Definition 2.3 *The homomorphism ρ defined above (Theorem 2.3) is called the* **permutation representation** *of G on the left cosets of H in G. The kernel of ρ, $Ker(\rho) = \bigcap_{g \in G} gHg^{-1}$, is called the* **core of** *H in G.*

Exercise 2.2 If ρ is the permutation representation of G on the left cosets of H in G, then show that

(*i*) $Ker(\rho) \leq H$, (*ii*) $G/Ker(\rho)$ is isomorphic to a subgroup of S_X, where $X = G/H = \{gH \mid g \in G\}$.

Corollary 2.4 *If G is an infinite group such that contains a proper subgroup of finite index, then G contains a proper normal subgroup of finite index.*

Proof: Let $H \leq G$ such that $[G : H] = n$. Let $X = G/H$ be the set of all left cosets of H in G. Then $|X| = n$ and there is a homomorphism $\rho : G \longrightarrow S_n$ such that $Ker(\rho) = \bigcap_{g \in G} gHg^{-1}$. Since $G/Ker(\rho)$ is isomorphic to a subgroup of S_n, $G/Ker(\rho)$ is finite. Obviously $Ker(\rho) \trianglelefteq G$, and since $Ker(\rho) \leq H < G$, $Ker(\rho) \neq G$. Note that $Ker(\rho) \neq \{1_G\}$. ■

Corollary 2.5 *If G is a simple group containing a proper subgroup H of finite index n, then G is isomorphic to a subgroup of S_n.*

Proof: By Theorem 2.3, there exists a homomorphism $\rho : G \longrightarrow S_n$ such that $Ker(\rho) = \bigcap_{g\in G} gHg^{-1}$ and $Ker(\rho) \leq H$. Since $Ker(\rho) \trianglelefteq G$ and G is simple, $Ker(\rho) = G$ or $Ker(\rho) = \{1_G\}$. Since $H < G$ and $Ker(\rho) \leq H$, $Ker(\rho) \neq G$. Thus $Ker(\rho) = \{1_G\}$. Hence ρ is a monomorphism; so that $G \cong Image(\rho) \leq S_n$. ■

Exercise 2.3 Prove that if λ and ρ are left and right regular representations of G, then $\lambda(a)$ commutes with $\rho(b)$ for all $a, b \in G$.

Exercise 2.4 (i)* Let G be a group of order $2^m k$, where k is odd. Prove that if G contains an element of order 2^m, then the set of all elements of odd order in G is a normal subgroup. (Hint: Consider G as permutations via Cayley's Theorem, and show that it contains an odd permutation).

(ii) Show that a finite simple group of even order must have order divisible by 4.

Exercise 2.5 (Poincare) If H and K are subgroups of G having finite index, then $H \cap K$ has finite index. (Hint: $[G : H \cap K] \leq [G : H][G : K]$.)

Exercise 2.6 Let G be a finite group and $H \leq G$ with $[G : H] = p$, where p is the smallest prime divisor of $|G|$. Prove that H is normal in G.

Exercise 2.7 Prove that A_6 has no subgroup of prime index.

Definition 2.4 (Conjugate subgroups) *Let G be a group and $H \leq G$ we define H^g by*

$$H^g :\, = gHg^{-1} = \{ghg^{-1} \mid h \in H\}.$$

Then H^g is called the **conjugate** *of H by g. It is routine to check that $H^g \leq G$, $\forall g \in G$.*

Definition 2.5 (Normalizer) *If $H \leq G$, the* **normalizer** *of H in G, denoted by $N_G(H)$, is defined by*

$$N_G(H) :\, = \{g \mid g \in G,\ gHg^{-1} = H\}.$$

If $H \trianglelefteq G$, then $N_G(H) = G$.

Exercise 2.8 (i) Show that $G \geq N_G(H) \trianglerighteq H$. (ii) If $H \trianglelefteq K$, where H and K are subgroups of G, then $N_G(H) \geq K$.

Theorem 2.6 *Let G be a group and $H \leq G$. Let $X = \{gHg^{-1} \mid g \in G\}$. Then there exists a homomorphism $\phi : G \longrightarrow S_X$ such that $Ker(\phi) = \bigcap_{g\in G} gN_G(H)g^{-1}$.*

Proof: Define $\phi_g : X \longrightarrow X$ by $\phi_g(g'Hg'^{-1}) = g(g'Hg'^{-1})g^{-1}$. Then ϕ_g is well-defined and $\phi_g \in S_X$. Now define $\phi : G \longrightarrow S_X$ by $\phi(g) = \phi_g$. Then ϕ is a homomorphism: $\forall a,\ g \in G$ we have $\phi(ab) = \phi_{ab}$ and

$$\begin{aligned}\phi_{ab}(gHg^{-1}) &= ab(gHg^{-1})b^{-1}a^{-1} = a(bgHg^{-1}b^{-1})a^{-1} = a(\phi_b(gHg^{-1}))a^{-1}\\ &= \phi_a(\phi_b(gHg^{-1})) = (\phi_a \circ \phi_b)(gHg^{-1}),\end{aligned}$$

hence $\phi_{ab} = \phi_a \circ \phi_b$ on X and ϕ is a homomorphism.

If $g \in Ker(\phi)$, then $\phi(g) = \phi_g$ is the identity permutation on X. So $\forall g' \in G$ we have $\phi_g(g'Hg'^{-1}) = g'Hg'^{-1}$. Therefore $g(g'Hg'^{-1})g^{-1} = g'Hg'^{-1}$; so $g'^{-1}gg'Hg'^{-1}g^{-1}g' = H$, that is $g'^{-1}gg'H(g'^{-1}gg')^{-1} = H$. Hence $g'^{-1}gg' \in N_G(H)$ and we deduce that $g \in g'N_G(H)g'^{-1}$, $\forall g' \in G$. This shows that $Ker(\phi) \subseteq \bigcap_{g\in G} g.N_G(H)g^{-1}$. (1)

If $a \in \bigcap_{g\in G} gN_G(H)g^{-1}$, then $a \in gN_G(H)g^{-1}$ for all $g \in G$. Thus there is $g' \in N_G(H)$ such that $a = gg'g^{-1}$. Now we have, for all $g \in G$,

$$\begin{aligned} \phi_a(gHg^{-1}) &= agHg^{-1}a^{-1} = gg'g^{-1}gHg^{-1}gg'^{-1}g^{-1} \\ &= gg'Hg'^{-1}g^{-1} = gHg^{-1}, \end{aligned}$$

since $g' \in N_G(H)$. This shows that ϕ_a is the identity on X. Thus $a \in Ker(\phi)$ and hence $Ker(\phi) \supseteq \bigcap_{g\in G} gN_G(H)g^{-1}$. (2) Now from (1) and (2) we obtain that $Ker(\phi) = \bigcap_{g\in G} gN_G(H)g^{-1}$. ■

Note: *The homomorphism ϕ given in Theorem 2.6, is called the* permutation representation *of G on the conjugates of H.*

Exercise 2.9 Prove that a subgroup H of G is normal if and only if it has only one conjugate in G.

Exercise 2.10 If H and K are conjugate subgroups of G, then $H \cong K$. Give an example to show that the converse may be false.

Exercise 2.11 if λ and ρ are left and right regular representations of S_3, show that $\lambda(S_3)$ and $\rho(S_3)$ are conjugate subgroups of S_6.

Exercise 2.12 Let G be a finite group with proper subgroup H. Prove that G is not the set-theoretic union of all conjugates of H. Give an example in which H is not normal and this union is a subgroup.

Exercise 2.13 (i) Assume $H < K < G$. Show that $N_K(H) = N_G(H) \cap K$.

(ii) Prove that $N_G(xHX^{-1}) = xN_G(H)x^{-1}$.

Exercise 2.14 If H and K are subgroups of G, show that $N_G(H \cap K) \geq N_G(H) \cap N_G(K)$. Give an example in which the inclusion is proper.

Exercise 2.15 * Let G be an infinite group containing an element $x \neq 1_G$ having only finitely many conjugates. Prove that G is not simple.

3 Permutation Groups

Definition 3.1 *Let G be a group and X be a set. We say that G* **acts on** *X if there exists a homomorphism $\rho : G \longrightarrow S_X$. Then $\rho(g) \in S_X$ for all $g \in G$. The action of $\rho(g)$ on X, that is $\rho(g)(x)$, is denoted by x^g for any $x \in X$. We say that G is a* **permutation group** *on X.*

Example 3.1 (i) If $G \leq S_X$, then obviously G acts on X naturally.

(ii) By Cayley's theorem any group G acts on itself and the action is given by $a^g = ga,\ \forall a \in G,$ for $g \in G$.

(iii) If $H \leq G$, then G acts on G/H, the set of all left cosets of H in G. The action is given by: for $g \in G$, $(aH)^g = gaH,\ \forall a \in G$.

(iv) If $H \leq G$, then G acts on the set of all conjugates of H in G by $(aHa^{-1})^g = g(aHa^{-1})g^{-1} = gaHa^{-1}g^{-1}$.

Definition 3.2 (Orbits) *Let G act on a set X and let $x \in X$. Then the* **orbit** *of x under the action G is defined by*

$$x^G :\ = \{x^g \mid g \in G\}.$$

Theorem 3.1 *Let G act on a set X. The set of all orbits of G on X form a partition of X.*

Proof: Define the relation $\sim$ on X by $x \sim y$ if and only if $x = y^g$ for some $g \in G$. Then $\sim$ is an equivalence relation on X (check) and $[x] = \{x^g \mid g \in G\} = x^G$. Hence the set of all orbits of G on X partitions X. ■

Example 3.2 (i) If G acts on itself by the left regular representation, then $\forall g \in G$ we have $g^G = \{g^h \mid h \in G\} = \{hg \mid h \in G\} = Gg = G$. Hence under the action of G, we have only *one orbit*, namely G itself.

(ii) If G acts on G/H, the set of left cosets of H in G, then $\forall aH \in G/H$ we have

$$(aH)^G = \{(aH)^g \mid g \in G\} = \{gaH \mid g \in G\} = G/H.$$

In this case we have only *one orbit*, namely G/H.

(iii) In the case when G acts on itself by *conjugation,* that is for $g \in G$ we have $\forall x \in G \quad x^g :\ = gxg^{-1}$, then

$$x^G = \{x^g \mid g \in G\} = \{gxg^{-1} \mid g \in G\} = [x]$$

the conjugacy class of x in G. Note that $|x^G| = |[x]| = [G : C_G(x)]$. In this case the number of orbits is equal to the number of conjugacy classes of G.

(iv) If G acts on the set of all its subgroups by conjugation, that is $H^g = gHg^{-1},\ \forall g \in G,\ \forall H \leq G$, then for a fixed H in G we have

$$H^G = \{H^g \mid g \in G\} = \{gHg^{-1} \mid g \in G\}$$

the set of all conjugates of H in G. Later we will prove that the number of conjugates of H in G is equal to $[G : N_G(H)]$. Hence $|H^G| = [G : N_G(H)]$. In this case the number of orbits of G is equal to the number of conjugacy classes of subgroups of G.

Definition 3.3 (Stabilizer) *If G acts on a set X and $x \in X$ then the* **stabilizer** *of x in G, denoted by G_x is the set $G_x = \{g \mid x^g = x\}$. That is G_x is the set of elements of G that fixes x.*

Theorem 3.2 *Let G act on a set X. Then*
(i) G_x is a subgroup of G for each $x \in X$.
(ii) $|x^G| = [G : G_x]$, that is the number of elements in the orbit of x is equal to the index of G_x in G.

Proof: (i) Since $x^{1_G} = x$, $1_G \in G_x$. Hence $G_x \neq \emptyset$. Let g, h be two elements of G_x. Then $x^g = x^h = x$. So $(x^g)^{h^{-1}} = (x^h)^{h^{-1}} = x^{1_G} = x$, and therefore $x^{gh^{-1}} = x$, $\forall x \in X$. Thus $gh^{-1} \in G_x$.

(ii) Since

$$\begin{aligned} x^g = x^h \quad &\Leftrightarrow \quad x = x^{hg^{-1}} \Leftrightarrow hg^{-1} \in G_x \\ &\Leftrightarrow \quad (G_x)g = (G_x)h, \end{aligned}$$

the map $\gamma : x^G \longrightarrow G/G_x$ given by $\gamma(x^g) = (G_x)g$ is well-defined and one-to-one. Obviously γ is onto. Hence there is a one-to-one correspondence between x^G and G/G_x. Thus $|x^G| = |G/G_x|$. ∎

Exercise 3.1 *Let G act on a set X. If $y = x^g$ for some $x, y \in X$, show that $g^{-1}G_x g = G_{x^g} = G_y$.*

Corollary 3.3 *If G is a finite group acting on a finite set X then $\forall x \in X$, $|x^G|$ divides $|G|$.*

Proof: By Theorem 3.2 we have $|x^G| = [G : G_x] = |G|/|G_x|$. Hence $|G| = |x^G| \times |G_x|$. Thus $|x^G|$ divides $|G|$.∎

Theorem 3.4 (Applications of Theorem 3.2) *(i) If G is a finite group, then $\forall g \in G$ the number of conjugates of g in G is equal to $[G{:}C_G(g)]$.*

(ii) If G is a finite group and H is a subgroup of G, then the number of conjugates of H in G is equal to $[G{:}N_G(H)]$.

Proof: (i) Since G acts on itself by conjugation, using Theorem 3.2 we have $|g^G| = [G{:}G_g]$. But since

$$g^G = \{g^h \mid h \in G\} = \{hgh^{-1} \mid h \in G\} = [g]$$

and

$$G_g = \{h \in G \mid g^h = g\} = \{h \in G \mid hgh^{-1} = g\} = \{h \in G \mid hg = gh\} = C_G(g),$$

we have

$$|g^G| = |[g]| = [G{:}G_g] = [G{:}C_G(g)] = \frac{|G|}{|C_G(g)|}.$$

(ii) Let G act on the set of all its subgroups by conjugation. Then by Theorem 3.2 we have $|H^G| = [G{:}G_H]$. Since $H^G = \{H^g \mid g \in G\} = \{gHg^{-1} \mid g \in G\} = [H]$ and $G_H = \{g \in G \mid H^g = H\} = \{g \in G \mid gHg^{-1} = H\} = N_G(H)$ we have $|[H]| = |H^G| = [G{:}G_H] = [G{:}N_G(H)] = \frac{|G|}{|N_G(H)|}$. ∎

Theorem 3.5 (Cauchy - Frobenius) *Let G be a finite group acting on a finite set X. Let n denote the number of orbits of G on X. Let $F(g)$ denote the number of elements of X fixed by $g \in G$. Then $n = \frac{1}{|G|}\sum_{g \in G} F(g)$.*

Proof: Consider $S = \sum_{g\in G} F(g)$. Let $x \in X$. Since there are $|G_x|$ elements in G that fix x, x is counted $|G_x|$ times in S. If $\Delta = x^G$, then $\forall y \in \Delta$ we have $|\Delta| = |x^G| = |y^G| = [G{:}G_x] = [G{:}G_y]$. Hence $|G_x| = |G_y|$. Thus Δ contributes $[G{:}G_x].|G_x|$ to the sum S. But $[G{:}G_x].|G_x| = |G|$ is independent to the choice of Δ and hence each orbit of G on X contributes $|G|$ to the sum S. Since we have n orbits, we have $S = n|G|$. ■

Definition 3.4 (Transitive Groups) *Let G be a group acting on a set X. If G has only one orbit on X, then we say that G is* **transitive** *on X, otherwise we say that G is* **intransitive** *on X. If G is transitive on X, then $x^G = X \forall\, x \in X$. This means that $\forall x,\ y \in X,\ \exists g \in G$ such that $x^g = y$.*

Note: *If G is a finite transitive group acting on a finite set X, then Theorem 3.2 (ii) implies that $|x^G| = |X| = |G|/|G_x|$. Hence $|G| = |X| \times |G_x|$.*

Definition 3.5 (Multiply Transitive Groups) *Let G act on a set X and let $|X| = n$ and $1 \leq k \leq n$ be a positive integer. We say that G is k* **- transitive** *on X if for every two ordered k - tuples $(x_1, x_2, \cdots, x_k)$ and $(y_1, y_2, \cdots, y_k)$ with $x_i \neq x_j$ and $y_i \neq y_j$ for $i \neq j$ there exists $g \in G$ such that ${x_i}^g = y_i$ for $i = 1, 2, \cdots, k$. The transitivity introduced in Definition 3.4 is the same as 1 - transitive.*

Exercise 3.2 Let G be a group acting on a set X. Assume that $|X| = n$. Let $1 \leq k \leq n$ be a positive integer.

(i) Show that if G is k - transitive, then G is also $(k-1)$ transitive, when $k > 1$.

(ii) If $\exists H \leq G$ such that H is k - transitive on X, then G is also k - transitive.

Exercise 3.3 Let G be a transitive group on a set X, $|X| = k \geq 2$. Show that G is k - transitive on X if and only if G_x is $(k-1)$ - transitive on $X - \{x\}$, for every $x \in X$.

Theorem 3.6 *If G is a k - transitive group on a set X with $|X| = n$, then*

$$|G| = n(n-1)(n-2)\cdots(n-k+1)|G_{[x_1,x_2,\cdots,x_k]}|$$

for every choice of k- distinct $x_1, x_2, \cdots, x_k \in X$, where $G_{[x_1,x_2,\cdots,x_k]}$ denote the set of all elements g in G such that ${x_i}^g = x_i$, $1 \leq i \leq k$.

Proof: Let $x_1 \in X$. Then since G is k - transitive, we have $|G| = n \times |G_{x_1}|$ (1) and G_{x_1} is $(k-1)$ - transitive, by Exercise 3.3, on $X - \{x_1\}$. Choose $x_2 \in X - \{x_1\}$. Then since G_{x_1} is $(k-1)$ - transitive on $X - \{x_1\}$ we have $|G_{x_1}| = |X - \{x_1\}| \times |(G_{x_1})_{x_2}|$, that is $|G_{x_1}| = (n-1) \times |G_{[x_1,x_2]}|$ and $G_{[x_1,x_2]}$ is $(k-2)$ - transitive on $X - \{x_1, x_2\}$. (2) Notice that (1) and (2) imply that $|G| = n(n-1) \times |G_{[x_1,x_2]}|$. If we continue this way, we will get

$$|G| = n(n-1)(n-2)\cdots(n-k+1)|G_{[x_1,x_2,\cdots,x_k]}|.$$

■

Theorem 3.7 *Let G act transitively on a finite set X with $|X| > 1$. Then there exists $g \in G$ such that g has no fixed points.*

Proof: By the Cauchy - Frobenius theorem we have

$$\begin{aligned} 1 = n &= \frac{1}{|G|}\sum_{g\in G} F(g) \\ &= \frac{1}{|G|}[F(1_G) + \sum_{g\in G-\{1_G\}} F(g)] \\ &= \frac{1}{|G|}[|X| + \sum_{g\in G-\{1_G\}} F(g)]. \end{aligned}$$

If $F(g) > 0$ for all $g \in G$, then we have

$$\begin{aligned} 1 = \frac{1}{|G|}[|X| + \sum_{g\in G-\{1_G\}} F(g)] &\geq \frac{1}{|G|}[|X| + |G| - 1] \\ &\geq 1 + \frac{|X|-1}{|G|} > 1, \end{aligned}$$

which is a contradiction. Hence $\exists\, g \in G$ such that $F(g) = 0$. ■

Exercise 3.4 Let G be a group of permutations on a set X and let $x, y \in X$. If $x^t = y$ for some $t \in G$, prove that $G_x \cong G_y$. (Hint: Use Exercise 3.1.)

Exercise 3.5 Use Cauchy - Frobenius to prove Lagrange's Theorem. (Hint: Consider the left - regular action of G.)

Exercise 3.6 If G is a finite group and c is the number of conjugacy classes of elements of G, show that $c = \frac{1}{|G|}\sum_{x\in G}|C_G(x)|$. (Hint: Consider the conjugation action of G on its elements and use Cauchy - Frobenius Theorem).

Exercise 3.7 Let G be a finite group of order p^n, where p is a prime. Assume that G acts on a set X with p not dividing $|X|$. Prove that there exists $x \in X$ such that $x^g = x$ for all $g \in G$. [Hint: use Corollary 3.3.]

Exercise 3.8 Assume that V ia vector space of dimension n over $\mathbb{Z}_p$ and $GL(n, p)$ is the corresponding general linear group acting on V. If G is a subgroup of $GL(n, p)$ with $|G| = p^m$, prove that there exists a non-zero vector $v \in V$ such that $gv = v$ for all $g \in G$. [Hint: since $G \leq GL(n, p)$, G acts on V.]

4 Representation Theory of Finite Groups

4.1 Basic Concepts

Definition 4.1 *Let G be a group. Let $f : G \longrightarrow GL(n, \mathbb{F})$ be a homomorphism. Then we say that f is a* **Matrix Representation** *of G of degree n (or dimension n), over the field $\mathbb{F}$.*

If $Ker(f) = \{1_G\}$, then we say that f is a **faithful** representation of G. In this situation $G \cong Image(f)$; so that G is isomorphic to a subgroup of $GL(n, \mathbb{F})$.

Example 4.1 (i) The map $f : G \longrightarrow GL(1, \mathbb{F})$ given by $f(g) = 1_{\mathbb{F}}$ for all $g \in G$ is called the **trivial representation** of G over $\mathbb{F}$. Notice that $GL(1, \mathbb{F}) = \mathbb{F}^*$.

(ii) Let G be a permutation group acting on a finite set X, where $X = \{x_1, x_2, \cdots, x_n\}$. Define $\pi : G \longrightarrow GL(n, \mathbb{F})$ by $\pi(g) = \pi_g$ for all $g \in G$, where π_g is the **permutation matrix** induced by g on X. That is $\pi_g = (a_{ij})$ an $n \times n$ matrix having $0_{\mathbb{F}}$ and $1_{\mathbb{F}}$ as entries in such way that

$$\begin{aligned} a_{ij} &= 1_{\mathbb{F}} \quad \text{if } g(x_i) = x_j \\ &= 0_{\mathbb{F}} \quad \text{otherwise.} \end{aligned}$$

Then π is a representation of G over $\mathbb{F}$, and π is called the **permutation representation** of G on X.

(iii) Take $X = G$ in part (ii). Define a permutation action on G by $g : x \longrightarrow xg$ for all $x \in G$. Then the associated representation π is called the **right regular representation** of G.

Exercise 4.1 Let $N \trianglelefteq G$. Assume that $\overline{\rho}$ is a representation of G/N. Define $\rho : G \longrightarrow GL(n, \mathbb{F})$, where n is the degree of $\hat{\rho}$, by $\rho(g) = \overline{\rho}(gN)$. Then show that ρ is a representation of G.

Exercise 4.2 Let $N \trianglelefteq G$. Assume that ρ is a representation of degree n on G. If $N \leq Ker(\rho)$, then show that the mapping $\overline{\rho} : G/N \longrightarrow GL(n, \mathbb{F})$ given by $\overline{\rho}(gN) = \rho(g)$ is a representation of G/N.

Theorem 4.1 *Let G be a group. Then the derived subgroup G' lies in the kernel of any representation of G of degree 1.*

Proof: Assume that $f : G \longrightarrow GL(1, \mathbb{F})$ is a representation of degree one of G. Let $a, b \in G$. Then

$$f(aba^{-1}b^{-1}) = f(a)f(b)[f(a)]^{-1}[f(b)]^{-1}.$$

Since $GL(1, \mathbb{F}) = F^*$ is abelian we have

$$f(aba^{-1}b^{-1}) = f(a)[f(a)]^{-1}f(b)[f(b)]^{-1} = 1_{\mathbb{F}}.$$

Thus $[a, b] = aba^{-1}b^{-1} \in Kerf$. Since G' is generated by the set of all commutators, $G' \subseteq Ker(f)$. ■

Exercise 4.3 Let $\mathbb{F} = GF(q)$ be the **Galois Field** of q elements, where $q = p^k$ for some prime p. Show that $|GL(n, \mathbb{F})| = (q^n - 1).(q^n - q) \cdots (q^n - q^{n-1})$.

Definition 4.2 (Special Linear Group $SL(n, \mathbb{F})$) *Let $\mathbb{F}$ be any field.*

$$SL(n, \mathbb{F}) = \{A \mid A \in GL(n, \mathbb{F}),\ det(A) = 1_{\mathbb{F}}\}.$$

Then it is not difficult to show that $SL(n, \mathbb{F}) \leq GL(n, \mathbb{F})$.

Theorem 4.2 *Let $F = GF(q)$ with $q = p^k$ for some prime p. Then*

$$SL(n, \mathbb{F}) \trianglelefteq GL(n, \mathbb{F})$$

and

$$|SL(n, \mathbb{F})| = |GL(n, \mathbb{F})|/(q - 1).$$

Proof: Let $\rho : GL(n,\mathbb{F}) \longrightarrow F^*$ be given by $\rho(A) = det(A)$, for all $A \in GL(n,\mathbb{F})$. Then ρ is a homomorphism (check). If $a \in \mathbb{F}^*$, then

$$\rho : \left(\begin{array}{c|cccc} a & 0 & 0 & \cdots & 0 \\ \hline 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & & & \\ 0 & 0 & 0 & \cdots & 1 \end{array}\right) \longmapsto a,$$

so that ρ is onto. We also have $Ker(\rho) = \{A \mid A \in GL(n,\mathbb{F}),\ det(A) = 1_{\mathbb{F}}\} = SL(n,\mathbb{F})$. Since $Ker(\rho) \trianglelefteq GL(n,\mathbb{F})$, $SL(n,\mathbb{F}) \trianglelefteq GL(n,\mathbb{F})$. Now since $GL(n,\mathbb{F})/Ker(\rho) \cong Image(\rho)$, we have that $GL(n,\mathbb{F})/SL(n,\mathbb{F}) \cong F^*$. Hence

$$|GL(n,\mathbb{F})/SL(n,\mathbb{F})| = |F^*| = q - 1.$$

■

Corollary 4.3 *If $\rho : G \longrightarrow GL(n,\mathbb{F})$ is a representation of G, then $\rho(g) \in SL(n,\mathbb{F})$ for all $g \in G'$.*

Proof: Let $h = [a,b]$ be a commutator in G. Then we have $\rho(h) = \rho(aba^{-1}b^{-1}) = \rho(a)\rho(b)\rho(a^{-1})\rho(b^{-1})$. Now since

$$\begin{aligned} det(\rho(h)) &= det(\rho(a)).det(\rho(b)).det(\rho(a^{-1}))det(\rho(b^{-1})) \\ &= det(\rho(aa^{-1})).det(\rho(bb^{-1})) \\ &= det(\rho(1_G)).det(\rho(1_G)) \\ &= det(I_n).det(I_n) = 1, \end{aligned}$$

we have $\rho(h) \in SL(n,\mathbb{F})$. ■

Exercise 4.4 (Special triangular Group) Let $STL(N,\mathbb{F})$ denote the set of all invertible lower triangular $n \times n$ matrices whose diagonal entries are all $1_{\mathbb{F}}$. Then $STL(n,\mathbb{F}) \leq GL(n,\mathbb{F})$. Show that if $\mathbb{F} = GF(q)$ where $q = p^k$ for some prime p, then $STL(n,\mathbb{F})$ is Sylow p-subgroup of $GL(n,\mathbb{F})$.

Definition 4.3 (Characters) *Let $f : G \longrightarrow GL(n,\mathbb{F})$ be a representation of G over the field $\mathbb{F}$. The function $\chi : G \longrightarrow \mathbb{F}$ defined by $\chi(g) = tr(f(g))$ is called the* **character** *of f.*

Definition 4.4 (Class functions) *If $\phi : G \longrightarrow \mathbb{F}$ is a function that is constant on conjugacy classes of G, that is $\phi(g) = \phi(xgx^{-1}), \forall x \in G$, then we say that ϕ is* **a class function.**

Lemma 4.4 *A character is a class function.*

Proof: Let χ be a character of G. Then χ is afforded by a representation $\rho : G \longrightarrow GL(n,\mathbb{F})$. Let $g \in G$; then $\forall x \in G$ we have

$$\begin{aligned} \chi(xgx^{-1}) &= tr(\rho(xgx^{-1})) \\ &= tr(\rho(x).\rho(g).\rho(x^{-1})) \\ &= tr(\rho(x).\rho(g).[\rho(x)]^{-1}) \\ &= tr(\rho(g)), \quad \text{see Note 5.1.1 below} \\ &= \chi(g). \end{aligned}$$

■

Note: *Similar matrices have the same trace. If $A = (a_{ij})$ and $B = (b_{ij})$ are two matrices, then*

$$tr(AB) = \sum_{i=1}^{n}(\sum_{j=1}^{n} a_{ij}b_{ji}) = \sum_{j=1}^{n}(\sum_{i=1}^{n} b_{ji}a_{ij}) = tr(BA).$$

Now if $B = PAP^{-1}$, then $tr(B) = tr(PAP^{-1}) = tr(P^{-1}PA) = tr(A)$. **Note:** *If χ is a character afforded by a representation $\rho : G \longrightarrow GL(n, \mathbb{F})$, then χ is not linear (in general) :*

$$\chi(gg') = tr(\rho(gg')) = tr(\rho(g)\rho(g')) \neq tr(\rho(g)) \times tr(\rho(g')) = \chi(g) \times \chi(g').$$

Later we will show that χ is linear if and only if $deg(\rho) = 1$.

Definition 4.5 (Equivalent Representations) *Two representations $\rho, \phi : G \longrightarrow GL(n, \mathbb{F})$ are said to be* **equivalent** *if there exists a $n \times n$ matrix P over $\mathbb{F}$ such that $P^{-1}\rho(g)P = \phi(g)$, $\forall g \in G$.*

Since similar matrices have the same trace, it follows that equivalent representations have the same character.

Theorem 4.5 *Equivalent representations have the same character.*

Proof: Let χ_1 and χ_2 be characters afforded by ρ_1 and ρ_2 two representations of degree n over a field $\mathbb{F}$. Assume that ρ_1 is equivalent to ρ_2. Then there is a $n \times n$ matrix P such that $P^{-1}\rho_1(g)P = \rho_2(g)$, $\forall g \in G$. Now $\forall g \in G$ we have

$$\chi_2(g) = tr(\rho_2(g)) = tr(P^{-1}\rho_1(g)P) = tr(\rho_1(g)) = \chi_1(g).$$

Hence $\chi_1 = \chi_2$. ■

Definition 4.6 *Let S be a set of $(n \times n)$ matrices over $\mathbb{F}$. We say that S is* **reducible** *if $\exists\ m, k \in \mathbb{N}$, and there exists $P \in GL(n, \mathbb{F})$ such that $\forall A \in S$ we have*

$$PAP^{-1} = \begin{pmatrix} B & 0 \\ C & D \end{pmatrix}$$

where B is an $m \times m$ matrix, D and C are $k \times k$ and $k \times m$ matrices respectively. Here 0 denotes the $m \times k$ zero matrix.

If there is no such P, we say that S is **irreducible**.

If $C = 0$, the zero $k \times m$ matrix, for all $A \in S$, then we say that S is **fully reducible**.

We say that S is **completely reducible** if $\exists\ P \in GL(n, \mathbb{F})$ such that

$$PAP^{-1} = \begin{pmatrix} B_1 & 0 & \cdot & \cdot & 0 \\ 0 & B_2 & 0 & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdot & \cdot & B_k \end{pmatrix}, \quad \forall A \in S,$$

where each B_i is irreducible.

Example 4.2 *Let $\mathbb{F} = \mathbb{C}$; consider*

$$S = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{C} \right\}.$$

Then S is a **reducible** *set over $\mathbb{C}$. Let $P = \begin{pmatrix} 1 & -i \\ 0 & 1 \end{pmatrix}$. Then $P^{-1} = \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}$ and*

$$P^{-1} \begin{pmatrix} a & -b \\ b & a \end{pmatrix} P = \begin{pmatrix} a+ib & 0 \\ b & a-ib \end{pmatrix}, \ \forall a, b \in \mathbb{C}.$$

In fact we can show that S is **fully reducible***. For this let $P = \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$. Then $P^{-1} = \frac{1}{2} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}$ and $P^{-1} \begin{pmatrix} a & -b \\ b & a \end{pmatrix} P = \begin{pmatrix} a-ib & 0 \\ 0 & a+ib \end{pmatrix}$.*

Exercise 4.5 Let $S = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}$. Show that S is reducible, but it is not fully reducible.

Definition 4.7 *Let $f : G \longrightarrow GL(n, \mathbb{F})$ be a representation of G over $\mathbb{F}$. Let $S = Im(f) = \{f(g) \mid g \in G\}$. Then $S \subseteq GL(n, \mathbb{F})$. We say that f is* **reducible, fully reducible,** *or* **completely reducible** *if S is reducible, fully reducible or completely reducible.*

Definition 4.8 (Sum of representations) *let $\rho : G \longrightarrow GL(n, \mathbb{F})$ and $\phi : G \longrightarrow GL(m, \mathbb{F})$ be two representations of G over $\mathbb{F}$. Define $\rho + \phi : G \longrightarrow GL(n+m, \mathbb{F})$ by*

$$(\rho + \phi)(g) := \begin{pmatrix} \rho(g) & 0_{n \times m} \\ 0_{m \times n} & \phi(g) \end{pmatrix} = \rho(g) \oplus \phi(g),$$

for all $g \in G$. Then $\rho + \phi$ is a representation of G over $\mathbb{F}$, of degree $n + m$.

If χ_1 and χ_2 are the characters of ρ and ϕ respectively, and if χ is the character of $\rho + \phi$, then $\forall g \in G$ we have

$$\chi(g) = trace \begin{pmatrix} \rho(g) & 0 \\ 0 & \phi(g) \end{pmatrix} = tr(\rho(g)) + tr(\phi(g)) = \chi_1(g) + \chi_2(g) = (\chi_1 + \chi_2)(g).$$

Hence $\chi = \chi_1 + \chi_2$.

Example 4.3 Let $G =< a, b >$ such that $a^2 = b^2 = 1_G$ and $ab = ba$. Define $f : G \longrightarrow GL(2, \mathbb{C})$ by $f(a) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $f(b) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. Then f is a faithful representation of degree 2. It is not difficult to see that f is completely reducible

Exercise 4.6 Represent the permutations of S_3 as permutation matrices. Calculate the character of this representation.

Theorem 4.6 (Maschke's theorem) *Let G be a finite group. Let f be a representation of G over a filed $\mathbb{F}$ whose characteristic is either 0 or is a prime that does not divide $|G|$. If f is reducible, then f is fully reducible.*

Proof: In fact we will show that if there is a matrix P such that $\forall g \in G$

$$P^{-1}f(g)P = \begin{pmatrix} A(g) & 0 \\ B(g) & C(g) \end{pmatrix}$$

then there is a matrix Q such that

$$\forall g \in G, Q^{-1}f(g)Q = \begin{pmatrix} A(g) & 0 \\ 0 & C(g) \end{pmatrix}.$$

Let $\overline{f}(g) = P^{-1}f(g)P$ and let $L = \begin{pmatrix} I_r & 0 \\ T & I_s \end{pmatrix}$ where r and s are the degrees of $A(g)$ and $C(g)$ respectively, and T is an $s \times r$ matrix. We need to determine T such that L is an invertible matrix over $\mathbb{F}$ independent of g and

$$L^{-1}\overline{f}(g)L = \begin{pmatrix} A(g) & 0 \\ 0 & C(g) \end{pmatrix}, \ \forall g \in G. \quad (1)$$

Then $Q = PL$. Relation (1) implies that

$$\begin{pmatrix} A(g) & 0 \\ B(g) & C(g) \end{pmatrix}\begin{pmatrix} I_r & 0 \\ T & I_s \end{pmatrix} = \begin{pmatrix} I_r & 0 \\ T & I_s \end{pmatrix}\begin{pmatrix} A(g) & 0 \\ 0 & C(g) \end{pmatrix},$$

that is

$$\begin{pmatrix} A(g) & 0 \\ B(g) + C(g)T & C(g) \end{pmatrix} = \begin{pmatrix} A(g) & 0 \\ T.A(g) & C(g) \end{pmatrix}.$$

Hence we find that

$$B(g) + C(g)T = T.A(g), \ \forall g \in G. \quad (2).$$

Since $\overline{f}$ is a matrix representation of G, $\overline{f}(gh) = \overline{f}(g).\overline{f}(h)$ for all $g, h \in G$. So for all g and h in G we have

$$\begin{pmatrix} A(gh) & 0 \\ B(gh) & C(gh) \end{pmatrix} = \begin{pmatrix} A(g) & 0 \\ B(g) & C(g) \end{pmatrix}\begin{pmatrix} A(h) & 0 \\ B(h) & C(h) \end{pmatrix},$$

that is

$$\begin{pmatrix} A(gh) & 0 \\ B(gh) & C(gh) \end{pmatrix} = \begin{pmatrix} A(g)A(h) & 0 \\ B(g)A(h) + C(g)B(h) & C(g)C(h) \end{pmatrix}.$$

We obtain the relations:
(i) $A(gh) = A(g)A(h)$
(ii) $C(gh) = C(g)C(h)$
(iii) $B(gh) = B(g)A(h) + C(g)B(h)$.

Relations (i) and (ii) show that A and C are matrix representations of G over $\mathbb{F}$. By multiplying (iii) and $A(h^{-1})$ we obtain that

$$B(gh)A(h^{-1}) = B(g) + C(g)B(h)A(h^{-1}) \ \ \forall g, h \in G. \quad (3)$$

If we fix g and let h runs over all elements of G, then using (3) we get

$$\sum_{h \in G} B(gh)A(h^{-1}) = \sum_{h \in G} B(g) + \sum_{h \in G} C(g)B(h)A(h^{-1})$$

$$= |G|B(g) + C(g) \sum_{h \in G} B(h)A(h^{-1}). \quad (4)$$

Now let $x = gh$. Since h runs over all elements of G, so also does x. Hence

$$\sum_{h \in G} B(gh)A(h^{-1}) = \sum_{x \in G} B(x)A(x^{-1}g) = \sum_{x \in G} B(x)A(x^{-1})A(g)$$

$$= (\sum_{x \in G} B(x)A(x^{-1}))A(g). \quad (5)$$

Now relations (4) and (5) give

$$(\sum_{x \in G} B(x)A(x^{-1}))A(g) = |G|B(g) + C(g)(\sum_{h \in G} B(h)A(h^{-1})). \quad (6)$$

Since the characteristic of $\mathbb{F}$ does not divide $|G|$, $|G| \neq 0$ in $\mathbb{F}$. Hence we can divide both sides of relation (6) by $|G|$. We get

$$(\frac{1}{|G|} \sum_{x \in G} B(x)A(x^{-1}))A(g) = B(g) + C(g)(\frac{1}{|G|} \sum_{h \in G} B(h)A(h^{-1})). \quad (7)$$

Finally by comparing relations (7) and (2), if we let

$$T = \frac{1}{|G|}(\sum_{x \in G} B(x)A(x^{-1})),$$

then T satisfies the relation (2). ■

Theorem 4.7 *[The general form of Maschke's theorem] Let G be a finite group and $\mathbb{F}$ a field whose characteristic is either 0 or is a prime that does not divide $|G|$. Then every representation of G over $\mathbb{F}$ is completely reducible.*

Proof: Let f be a representation of G over $\mathbb{F}$. If f is irreducible, then it is completely reducible. Hence assume that f is reducible. Then by Maschke's theorem f is fully reducible, and therefore for all $g \in G$, $f(g)$ is similar to

$$\begin{pmatrix} A(g) & 0 \\ 0 & C(g) \end{pmatrix}$$

.

Since A and B are representations of G over F, we can apply Maschke's theorem to these representations. Repeating this process we obtain that $f(g)$ is similar to

$$\begin{pmatrix} B_1(g) & 0 & \cdot & \cdot & 0 \\ 0 & B_2(g) & 0 & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdot & \cdot & B_k(g) \end{pmatrix},$$

where $B_i, 1 \leq i \leq k$ are all irreducible representations of G over $\mathbb{F}$. ■

Theorem 4.8 *[Schur's Lemma] Let ρ and ϕ be two irreducible representations, of degree n and m respectively, of a group G over a field $\mathbb{F}$. Assume that there exists an $m \times n$ matrix P such that $P\rho(g) = \phi(g)P$ for all $g \in G$. Then either $P = 0_{m\times n}$ or P is non-singular so that $\rho(g) = P^{-1}\phi(g)P$ (that is ρ and ϕ are equivalent representations of G).*

Proof: Let $r = rank(P)$. Then there are non-singular matrices L and M such that $P = LE_rM$, where

$$E_r = \begin{pmatrix} 0_{m-r\times r} & 0_{m-r\times n-r} \\ I_r & 0_{r\times n-r} \end{pmatrix}_{m\times n},$$

and L and M are $m \times m$ and $n \times n$ matrices respectively. Since for all $g \in G$ we have $P\rho(g) = \phi(g)P$, we obtain that

$$LE_rM\rho(g) = \phi(g)LE_rM.$$

Hence

$$E_rM\rho(g)M^{-1} = L^{-1}\phi(g)LE_r. \quad (1)$$

Using the relation (1), we can partition the matrices $M\rho(g)M^{-1}$ and $L^{-1}\phi(g)L$ in the following way, provided that $r \neq 0$, and $m \neq r$ or $n \neq r$:

$$M\rho(g)M^{-1} = \begin{pmatrix} A(g) & B(g) \\ C(g) & D(g) \end{pmatrix}_{n\times n},$$

and

$$L^{-1}\phi(g)L = \begin{pmatrix} A'(g) & B'(g) \\ C'(g) & D'(g) \end{pmatrix}_{m\times m},$$

where $A(g)$ is $r \times r$, $B(g)$ is $r \times n-r$, $C(g)$ is $n-r \times r$, $D(g)$ is $n-r \times n-r$, $A'(g)$ is $m-r \times m-r$, $B'(g)$ is $m-r \times r$, $C'(g)$ is $r \times m-r$, $D'(g)$ is $r \times r$. We can easily deduce that

$$E_rM\rho(g)M^{-1} = \begin{pmatrix} 0_{m-r\times r} & 0_{m-r\times n-r} \\ A(g) & B(g) \end{pmatrix}$$

and

$$L^{-1}\phi(g)LE_r = \begin{pmatrix} B'(g) & 0_{m-r\times n-r} \\ D'(g) & 0_{r\times n-r} \end{pmatrix}.$$

Now using the relation (1) we must have

$$\begin{pmatrix} 0_{m-r\times r} & 0_{m-r\times n-r} \\ A(g) & B(g) \end{pmatrix} = \begin{pmatrix} B'(g) & 0_{m-r\times n-r} \\ D'(g) & 0_{r\times n-r} \end{pmatrix}.$$

Hence $B'(g) = 0_{m-r\times r}$ and $B(g) = 0_{r\times m-r}$ for all $g \in G$. This shows that ρ and ϕ are reducible, which is a contradiction. Thus either $r = 0$ or $m = n = r$. If $r = 0$, then $P = 0_{m\times n}$. If $m = n = r$, then P is invertible and $\rho(g) = P^{-1}\phi(g)P$. ■

Definition 4.9 (Algebraically Closed Fields) . *A field F is said to be* **Algebraically closed** *if every polynomial equation $p(x) = 0_F$ with $P(x) \in F[x]$ has all its roots in F.*

For example the complex field $\mathbb{C}$ is an algebraically closed field by the Fundamental Theorem of Algebra. The first proof for the fundamental theorem of algebra was given by Gauss in his doctoral dissertation in 1799 at the age of 22 (in fact gauss gave several independent proofs, he published his last proof in 1849 at the age of 72).

For an algebraically closed field, the Schur's Lemma (Theorem 4.8) has the following noteworthy corollary.

Corollary 4.9 *If ρ is an irreducible representation of degree n of a group G over an algebraically closed field F, then the only matrices which commute with all matrices $\rho(g)$, $g \in G$, are the scalar matrices aI_n, $a \in F$.*

Proof: Let P be an $n \times n$ matrix such that $P\rho(g) = \rho(g)P$, for all $g \in G$. Then for any $a \in F$ we have

$$(aI_n - P)\rho(g) = \rho(g)(aI_n - P), \quad for\ all \;\; g \in G \qquad (1)$$

Let $m(x) = det(xI_n - P)$ be the characteristic polynomial of P. Since $m(x)$ is a polynomial over F and F is algebraically closed, there is $a_0 \in F$ such that $m(a_0) = 0_F$. Hence $det(a_0I_n - P) = 0$. So that $a_0I_n - P$ is singular. Now using relation (1) and Schur's Lemma, we must have $a_0I_n - P = 0$. Thus $P = a_0I_n$. ■

Exercise 4.7 Let G be a finite group and ρ and ϕ be representations of degrees n and m respectively, over a a field F. Assume that $char(F)$ does not divide the order of G. Let S be an $m \times n$ matrix over F. Show that $S\rho(g) = \phi(g)S$ for all g in G if and only if there is an $m \times n$ matrix T over F such that $S = \sum_{g\in G} \phi(g^{-1})T\rho(g)$.

Exercise 4.8 Maschke's Theorem becomes false if the hypothesis that $char(F)$ does not divide the order of G is omitted. Let $F = GF(2)$ and $G =< a >$ be acyclic group of order 2. Define $\rho : G \to GL(2, F)$ by $\rho(1_G) = I_2$ and $\rho(a) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Show that ρ is reducible but not fully reducible. (Hint use Exercise 5.1.5.)

Exercise 4.9 Show that Corollary 5.1.9 is false if $F = \mathbb{R}$.

Theorem 4.10 *Let ρ and ϕ be two inequivalent irreducible representations, of degrees n and m respectively, of a group G over a field F. If T is an $m \times n$ matrix over F, then*

$$\sum_{g\in G} \phi(g^{-1})T\rho(g) = 0_{m\times n}.$$

Proof: Let $S = \sum_{g\in G} \phi(g^{-1})T\rho(g)$. Then for any $x \in G$ we have

$$S\rho(x) = \sum_{g\in G} \phi(g^{-1})T\rho(gx) = \sum_{g\in G} \phi(x)\phi(x^{-1}g^{-1})T\rho(gx) =$$

$$\phi(x)(\sum_{g\in G} \phi((gx)^{-1})T\rho(gx)) = \phi(x)(\sum_{z\in G} \phi(z^{-1})T\rho(z)) = \phi(x)S.$$

Since ρ and ϕ are inequivalent irreducible representations of G, by Schur's lemma we must have $S = 0_{m\times n}$.

■

Definition 4.10 *Let G be a finite group and F a field such that $char(F)$ does not divide the order of G. If ρ and ϕ are two functions from G into F, we define an* **inner product** $<,>$ *by the following rule:*

$$< \rho, \phi >= \frac{1}{|G|} \sum_{g\in G} \rho(g)\phi(g^{-1}),$$

where $\frac{1}{|G|}$ stands for $|G|^{-1}$ in F.

Theorem 4.11 *The inner product $<,>$ defined above is bilinear and symmetric:*

(i) $< \rho_1 + \rho_2, \phi >=< \rho_1, \phi > + < \rho_2, \phi >$,

(ii) $< \rho, \phi_1 + \phi_2 >=< \rho, \phi_1 > + < \rho, \phi_2 >$,

(iii) $< a\rho, \phi >= a < \rho, \phi >=< \rho, a\phi >$, *for all $a \in F$,*

(iv) $< \rho, \phi >=< \phi, \rho >$.

Proof: the bilinear properties (i), (ii) and (iii) are easy to verify. Let us prove the the symmetry:

$$< \rho, \phi >= \frac{1}{|G|} \sum_{g\in G} \rho(g)\phi(g^{-1}) = \frac{1}{|G|} \sum_{g\in G} \rho(g^{-1})\phi(g) = \frac{1}{|G|} \sum_{g\in G} \phi(g)\rho(g^{-1}) =< \phi, \rho > .$$

■

Note: *If $\rho : G \longrightarrow F^*$ is a group homomorphism, then*

$$< \rho, \rho >= \frac{1}{|G|} \sum_{g\in G} \rho(g)\rho(g^{-1}) = \frac{1}{|G|} \sum_{g\in G} \rho(1_G) = \frac{1}{|G|} \sum_{g\in G} 1_F = \frac{1}{|G|} \times (|G|1_F) = 1_F.$$

5 Characters of Finite Groups

In this section, unless explicit exception is made, the group G will be finite and all representations and matrices will be over the complex field $\mathbb{C}$.
Note: *By the general form of Maschke's theorem (Theorem 4.7), all representations of G are completely reducible.* **Note:** *If If $\rho : G \longrightarrow GL(n, \mathbb{C})$ is a representation of G, then we denote the (i, j) entry of $\rho(g)$ by $\rho_{ij}(g)$. Hence we can regard ρ_{ij} is a map from G into $\mathbb{C}$.*

Theorem 5.1 *[Orthogonality of irreducible representations] Let G be a finite group and ρ and ϕ two irreducible representations of G.*

(i) If ρ and ϕ are inequivalent, then $<\rho_{rs}, \phi_{ij}>= 0$, for all i, j, r, s.

(ii) $<\rho_{rs}, \rho_{ij}>= \delta_{is}\delta_{jr}/deg(\rho)$.

Proof: (i) Using Theorem 5.1.10 we have

$$\sum_{g\in G} \phi(g^{-1})E_{jr}\rho(g) = 0_{m\times n}, \quad (1)$$

where E_{jr} is the $m \times n$ matrix with (j, r) entry 1 and other entries 0, with $n = deg(\rho)$ and $m = deg(\phi)$. Now from (1) we get

$$\frac{1}{|G|}\sum_{g\in G} \phi(g^{-1})E_{jr}\rho(g) = 0_{m\times n}. \quad (2)$$

Since the (i, s) entry of the left hand-side of the relation (2) is

$$\frac{1}{|G|}\sum_{g\in G} \phi_{ij}(g^{-1})\rho_{rs}(g) =< \phi_{ij}, \rho_{rs}>,$$

we have $<\phi_{ij}, \rho_{rs}>= 0$.

(ii) Let $S_{jr} = \frac{1}{|G|}\sum_{g\in G} \rho(g^{-1})E_{jr}\rho(g)$. Then for any $x \in G$ we have (see Exercise 5.1.7) $S_{jr}\rho(x) = \rho(x)S_{jr}$, and from Corollary 5.1.9 we deduce that S_{jr} is an scalar matrix. Hence let $S_{jr} = \lambda_{jr}I_n$, where $\lambda_{jr} \in \mathbb{C}$. Then we have

$$\lambda_{jr}I_n = \frac{1}{|G|}\sum_{g\in G} \rho(g^{-1})E_{jr}\rho(g). \quad (3)$$

By comparing the (i, s) entry of the left and right hand-side of (3), we get

$$\lambda_{jr}\delta_{is} = \frac{1}{|G|}\sum_{g\in G} \rho_{ij}(g^{-1})\rho_{rs}(g).$$

That is

$$\lambda_{jr}\delta_{is} =< \rho_{ij}, \rho_{rs}> .$$

Since $<\rho_{ij}, \rho_{rs}>=<\rho_{rs}, \rho_{ij}>$, we get

$$\lambda_{jr}\delta_{is} =< \rho_{ij}, \rho_{rs}>=< \rho_{rs}, \rho_{ij}>= \lambda_{si}\delta_{rj}. \quad (4)$$

Now if $i \neq s$ or $j \neq r$, we have $<\rho_{ij}, \rho_{rs}>= 0$ and (ii) holds. Suppose that $i = s$ and $j = r$. Then by (4) we have

$$< \rho_{ij}, \rho_{ji}>= \lambda_{jj} = \lambda_{ii}. \quad (5)$$

Hence we have

$$\lambda_{11} = \lambda_{22} = \cdots = \lambda_{nn} = \lambda \in \mathbb{C},$$

so that

$$n\lambda = \sum_{i=1}^{n} \lambda_{ii} = \sum_{i=1}^{n} < \rho_{i1}, \rho_{1i} >, \; by \; (5),$$

$$= \sum_{i=1}^{n} (\frac{1}{|G|} \sum_{g \in G} \rho_{1i}(g^{-1})\rho_{i1}(g))$$

$$= \frac{1}{|G|} \sum_{g \in G} (\sum_{i=1}^{n} \rho_{1i}(g^{-1})\rho_{i1}(g)). \quad (6)$$

Since $\sum_{i=1}^{n} \rho_{1i}(g^{-1})\rho_{i1}(g)$ is the $(1,1)-$entry of $\rho(g^{-1})\rho(g)$ and since $\rho(g^{-1})\rho(g) = \rho(g^{-1}g) = \rho(1_G) = I_n$, we have

$$\sum_{i=1}^{n} \rho_{1i}(g^{-1})\rho_{i1}(g) = 1.$$

Now relation (6) implies that

$$n\lambda = \frac{1}{|G|} \sum_{g \in G} 1 = \frac{1}{|G|} \times |G| = 1.$$

Hence $\lambda = \frac{1}{n}$. Therefore by (5) we get

$$< \rho_{ij}, \rho_{ji} > = \frac{1}{n} = \delta_{ii}\delta_{jj}/deg(\rho).$$

■

Theorem 5.2 *[Orthogonality of irreducible characters] Let G be a finite group and ρ and ϕ two irreducible representations of G. If χ_ρ and χ_ϕ are characters of ρ and ϕ respectively, then*

(i) $< \chi_\rho, \chi_\phi > = 1$ *if ρ and ϕ are equivalent, and* $< \chi_\rho, \chi_\phi > = 0$ *otherwise,*

(ii) $< \chi_\rho, \chi_\rho > = 1$.

Proof: (i) Let $n = deg(\rho)$ and $m = deg(\phi)$. Then we have

$$\begin{aligned} < \chi_\rho, \chi_\phi > &= \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g)\chi_\phi(g^{-1}) \\ &= \frac{1}{|G|} \sum_{g \in G} \{[\sum_{i=1}^{n} \rho_{ii}(g)][\sum_{i=1}^{n} \phi_{jj}(g^{-1})]\} \\ &= \sum_{i=1}^{n} \sum_{j=1}^{m} [\frac{1}{|G|} \sum_{g \in G} \rho_{ii}(g)\phi_{jj}(g^{-1})] \\ &= \sum_{i=1}^{n} \sum_{j=1}^{m} < \rho_{ii}, \phi_{jj} > . \quad (1) \end{aligned}$$

If ρ and ϕ are inequivalent, then $<\rho_{ii}, \phi_{jj}>= 0$ by part (ii) of Theorem 5.1, Hence using the relation (1) above we get $<\chi_\rho, \chi_\phi>= 0$.

If If ρ and ϕ are equivalent, then $\chi_\rho = \chi_\phi$ by Theorem 5.1.5. Now we have

$$\begin{aligned} <\chi_\rho, \chi_\phi> &= <\chi_\rho, \chi_\rho> \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} <\rho_{ii}, \rho_{jj}>, \ by\ (1), \\ &= \sum_{i=1}^{n} <\rho_{ii}, \rho_{ii}>= \sum_{i=1}^{n}\frac{1}{n}, \ by\ Theorem\ 5.2.1, \\ &= n \times \frac{1}{n} = 1. \end{aligned}$$

(ii) As above. ■

Corollary 5.3 *Two irreducible representations of a finite group G are equivalent if and only if they have the same characters.*

Proof: Let ρ and ϕ be two irreducible representations of G. If ρ and ϕ are equivalent then $\chi_\rho = \chi_\phi$ by Theorem 5.1.5. Conversely assume that $\chi_\rho = \chi_\phi$. Then by Theorem 5.2.2 (part (ii)) we have $<\chi_\rho, \chi_\phi>= 1$. Thus ρ and ϕ are equivalent by Theorem 5.2.2. ■

Note: *Maschke's theorem (Theorem 5.1.7) implies that if ρ is a representation of G, then ρ is equivalent to $\sum_{i=1}^{k}\rho_i$ where ρ_i, s are irreducible representations of G. We also have $\chi_\rho = \sum_{i=1}^{k}\chi_{\rho_i}$.*

Exercise 5.1 If ρ is a representation of G such that ρ is equivalent to $\sum_{i=1}^{k}\rho_i$ where ρ_i, s are irreducible representations of G, then ρ_i are unique up to equivalence.

Theorem 5.4 (Generalisation of Corollary 5.2.3) *Two representations of a finite group G are equivalent if and only if they have the same characters.*

Proof: Let ρ and ϕ be two representations of G. If ρ and ϕ are equivalent then $\chi_\rho = \chi_\phi$ by Theorem 5.1.5.

Conversely assume that $\chi_\rho = \chi_\phi$. Assume that an irreducible representation ψ_i appears m_i times in ρ and n_i times in ϕ. Then adding dummy terms if necessary, we have $\rho \sim \sum_{i=1}^{k} m_i\psi_i$ and $\phi \sim \sum_{i=1}^{k} n_i\psi_i$. Then $\chi_\rho = \sum_{i=1}^{k} m_i\chi_{\psi_i}$ and $\chi_\phi = \sum_{i=1}^{k} n_i\chi_{\psi_i}$. Since $\chi_\rho = \chi_\phi$, we have $\sum_{i=1}^{k} m_i\chi_{\psi_i} = \sum_{i=1}^{k} n_i\chi_{\psi_i}$. Hence for any j we have

$$\begin{aligned} m_j &= <m_j\chi_{\psi_j}, \chi_{\psi_j}>=<\sum_{i=1}^{k} m_i\chi_{\psi_i}, \chi_{\psi_j}> \\ &= <\sum_{i=1}^{k} n_i\chi_{\psi_i}, \chi_{\psi_j}>= n_j. \end{aligned}$$

Thus $\sum_{i=1}^{k} m_i\psi_i = \sum_{i=1}^{k} n_i\psi_i$. So $\rho \sim \phi$.
■

Definition 5.1 (Irreducible Characters) *If χ_ρ is a character afforded by a representation ρ of G, then we say that χ_ρ is an* **irreducible character** *if ρ is an irreducible representation. Notice that if χ is an irreducible character of G and if ϕ is a representation of G such that $\chi_\phi = \chi$, then ϕ is also irreducible by Theorem 5.2.4.*

Theorem 5.5 *The set of all irreducible characters of G is a linearly independent set over $\mathbb{C}$.*

Proof: Let $\chi_1, \chi_2, \cdots, \chi_m$ be a finite set of distinct irreducible characters of a finite group G. assume that there are $\lambda_1, \lambda_2, \cdots, \lambda_m$ in $\mathbb{C}$ such that

$$\lambda_1\chi_1 + \lambda_2\chi_2 + \cdots + \lambda_m\chi_m = 0, \quad (1)$$

the zero function from G into $\mathbb{C}$. Since $\chi_i \neq \chi_j$ for $i \neq j$, χ_i and χ_j are afforded by inequivalent irreducible representations of G (by Theorem 5.2.4). Hence we have $< \chi_i, \chi_j >= 1$ if $i = j$ and 0 otherwise. Now using the relation (1) above we get

$$\begin{aligned} 0 &= < 0, \chi_j >=< \sum_{i=1}^{m} \lambda_i\chi_i, \chi_j > \\ &= < \sum_{i=1}^{m} \lambda_i < \chi_i, \chi_j >= \lambda_j, 1 \leq j \leq m. \end{aligned}$$

Therefore $\{\chi_1, \chi_2, \cdots, \chi_m\}$ is a linearly independent set over $\mathbb{C}$. ■

Theorem 5.6 *If G has r distinct conjugacy classes of elements, then G has at most r irreducible characters.*

Proof: Let $S = \{[g_1], [g_2], \cdots, [g_r]\}$ be the set of all conjugacy classes of elements of G and let V be the vector space of functions from S into $\mathbb{C}$. Define $f_i : S \longrightarrow \mathbb{C}$, for $1 \leq i \leq r$, by $f_i([g_i]) = 1$ and $f_i([g_j]) = 0$ if $i \neq j$. Then $\{f_1, f_2, \cdots, f_r\}$ is a basis for V. Thus $dim(V) = r$.

Let $Irr(G)$ denote the set of all distinct irreducible characters of G. Since a character is a class function, we can regard $Irr(G)$ as a subset of V. Now since $Irr(G)$ is a linearly independent subset of V by Theorem 5.2.5, we have $|Irr(G)| \leq dim(V)$, that is $|Irr(G)| \leq r$. ■

Exercise 5.2 (i) If $\chi = \sum_{i=1}^{k} \lambda_i\chi_i$, where χ_i are distinct irreducible characters of G and λ_i are non-negative integers, show that $< \chi, \chi >= \sum_{i=1}^{k} \lambda_i^2$.

(ii) If χ is a character of G, then show that χ is irreducible if and only if $< \chi, \chi >= 1$.

Assume that $\{C_1, C_2, \cdots, C_r\}$ is the set of all conjugacy classes of elements of G with $C_1 = 1_G$. Unless otherwise stated g_i will denote an arbitrary element of the conjugacy class C_i and we put

$$h_i = |C_i| = |G|/|C_G(g_i)|.$$

Let $Irr(G) = \{\chi_1, \chi_2, \cdots, \chi_k\}$ be the set of all distinct irreducible characters of G with the assumption that χ_1 is the character afforded by the *trivial representation* $\rho(g) = 1$ for all g in G.

Theorem 5.7 *We have the following*

(i) $\sum_{g\in G} \chi_1(g) = |G|$,

(ii) $\sum_{g\in G} \chi_i(g) = 0$, *if* $i \neq 1$,

(iii) $\sum_{j=1}^{r} h_j\chi_i(g_j) = \delta_{1i}|G|$.

Proof: (i) Since $\chi_1(g) = 1$ for all g in G, we have

$$\sum_{g\in G} \chi_1(g) = \sum_{g\in G} 1 = |G|.$$

(ii) If $i \neq 1$, then $<\chi_i, \chi_1>= 0$. hence

$$0 = \frac{1}{|G|}\sum_{g\in G} \chi_i(g)\chi_1(g^{-1}) = \frac{1}{|G|}\sum_{g\in G} \chi_i(g).$$

Thus $\sum_{g\in G} \chi_i(g) = 0 \times |G| = 0$.

(iii) If $i = 1$, then by part (i) we have $\sum_{g\in G} \chi_1(g) = |G|$ and hence

$$|G| = \sum_{g\in G} \chi_1(g) = \sum_{j=1}^{r} h_j\chi_1(g_j).$$

If $i \neq 1$, then by part (ii) we have $\sum_{g\in G} \chi_i(g) = 0 = \delta_{1i}$ and hence

$$0 = \delta_{1i} = \sum_{g\in G} \chi_i(g) = \sum_{j=1}^{r} h_j\chi_i(g_j).$$

■

Exercise 5.3 (i) Let ρ be an irreducible representation of G. Show that $deg(\rho) = 1$ if and only if $ker(\rho) \geq G'$.

(ii) Show that all irreducible representations of an abelian group are of degree one.

Note: *If* χ_ρ *and* χ_ϕ *are two characters of* G*, we know that*

$$<\chi_\rho, \chi_\phi>= \frac{1}{|G|}\sum_{g\in G} \chi_\rho(g)\chi_\phi(g^{-1}).$$

Hence

$$\begin{aligned} <\chi_\rho, \chi_\phi> &= \frac{1}{|G|}\sum_{i=1}^{r} h_i\chi_\rho(g_i)\chi_\phi(g_i^{-1}) \\ &= \sum_{i=1}^{r} \frac{h_i}{|G|}\chi_\rho(g_i)\chi_\phi(g_i^{-1}) \\ &= \sum_{i=1}^{r} \frac{1}{|C_G(g_i)|}\chi_\rho(g_i)\chi_\phi(g_i^{-1}). \end{aligned}$$

Example 5.1 Consider the symmetric group S_3. Representing the elements of S_3 as permutation matrices, we obtain the following faithful representation $\pi : S_3 \longrightarrow GL(3,\mathbb{C})$

$$\pi(1_{S_3}) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \pi((12)) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \pi((23)) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

$$\pi((13)) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \pi((123)) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \pi((132)) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Then it is easy to see that

$$\chi_\pi(1_{S_3}) = 3, \chi_\pi((12)) = \chi_\pi((13)) = \chi_\pi((23)) = 1, \chi_\pi((123)) = \chi_\pi((132)) = 0.$$

Notice that $\chi_\pi(g)$ is equal to the number of fixed points of g on $\{1,2,3\}$.

Now

$$\begin{aligned} < \chi_\pi, \chi_\pi > &= \frac{1}{6}\{1[\chi_\pi(1_{S_3})]^2 + 3[\chi_\pi((12))]^2 + 2[\chi_\pi((123))\chi_\pi((132))]\} \\ &= \frac{1}{6}\{1[9] + 3[1] + 2[0]\} = 12/6 = 2. \end{aligned}$$

this shows that χ_π (and hence π) is not irreducible. Hence $\chi_\pi = \chi_i + \chi_j$, where χ_i and χ_j are two distinct irreducible characters of S_3. (Note: If χ is a character of a group G such that $< \chi, \chi >= 2$, then there are $\chi_i, \chi_j \in Irr(G)$ such that $\chi = \chi_i + \chi_j$, $i \neq j$. Because if $\chi = \sum_{i=1}^k \lambda_i \chi$, then $< \chi, \chi >= 2$ implies

$$2 =< \chi, \chi >=< \sum_{i=1}^k \lambda_i \chi, \sum_{i=1}^k \lambda_i \chi >= \sum_{i=1}^k \lambda_i^2.$$

Hence there are $i \neq j$ for which $\lambda_i = \lambda_j = 1$. So that $\chi = \chi_i + \chi_j$.)

Since

$$deg(\chi_\pi) = 3 = \chi_\pi(1_{S_3}) = \chi_i(1_{S_3}) + \chi_j(1_{S_3}),$$

W.L.O.G we may assume that $deg(\chi_i) = 1$ and $deg(\chi_j) = 2$. Let us now consider the actions of χ_1 (the trivial character) and χ_π on the conjugacy clases of S_3:

S_3	C_1	C_2	C_3
Class Rep	1_{S_3}	(12)	(123)
h_i	1	3	2
χ_1	1	1	1
χ_π	3	1	0

Now

$$\begin{aligned} < \chi_\pi, \chi_1 > &= \frac{1}{6}\{1[\chi_\pi(1_{S_3})\chi_1(1_{S_3})] + 3[\chi_\pi((12))\chi_1((12))] + 2[\chi_\pi((123))\chi_1((132))]\} \\ &= \frac{1}{6}\{3 + 3 + 0\} = 1. \end{aligned}$$

thus χ_1 appears only once in χ_π and hence $\chi_\pi = \chi_1 + \chi_2$ where χ_2 is a nontrivial irreducible character of S_3. Now we have

$$\chi_2(g) = \chi_\pi(g) - \chi_1(g) = \chi_\pi(g) - 1, \; for\ all\ g \in S_3.$$

So that we have

$$\chi_2(1_{S_3}) = 3 - 1 = 2, \chi_2((12)) = \chi_2((13)) = \chi_2((23)) = 1 - 1 = 0$$

and

$$\chi_2((123)) = \chi_2((132)) = 0 - 1 = -1.$$

Since $|Irr(S_3)| \leq 3$, We may have one more irreducible character [in fact later we will show that for any finite group G, $|Irr(S_3)| = r$, the number of conjugacy classes if G.]. Define $\rho : S_3 \longrightarrow \mathbb{C}$ by $\rho(g) = 1$ if g is even and $\rho(g) = -1$ if g is odd. Then ρ is a representation of degree 1 with $\chi_\rho = \rho$. Notice that $\chi\rho \neq \chi_1$ and

$$\chi_\rho(1_{S_3}) = \chi_\rho((132)) = \chi_\rho((123)) = 1$$

and

$$\chi_\rho((12)) = \chi_\rho((13)) = \chi_\rho((23)) = -1.$$

Since $deg(\chi_\rho) = 1$, χ_ρ is irreducible (note that

$$< \chi_\rho, \chi_\rho >= \frac{1}{6}[1(1) + 3(-1)(-1) + 2(1)(1)] = \frac{1}{6}[1 + 3 + 2] = 1.)$$

This character is the third irreducible character of S_3, namely χ_3. We are now able to produce the following table for S_3, which is called the **Character Table** of S_3 over $\mathbb{C}$.

Class Rep	1_{S_3}	(12)	(123)
h_i	1	3	2
χ_1	1	1	1
χ_2	2	0	-1
χ_3	1	-1	1

Notice that

$$< \chi_1, \chi_2 >=< \chi_1, \chi_3 >=< \chi_2, \chi_3 >= 0;$$

$$\sum_{g \in G} \chi_1(g) = 1(1) + 3(1) + 2(1) = 6 = |S_3|;$$

$$\sum_{g \in G} \chi_2(g) = 1(2) + 3(01) + 2(-1) = 0;$$

$$\sum_{g \in G} \chi_3(g) = 1(1) + 3(-1) + 2(1) = 0.$$

Let $\phi : S_3 \longrightarrow GL(2, \mathbb{C})$ be given by

$$\phi(1_{S_3}) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \phi((12)) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \phi((13)) = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix},$$

$$\phi((23)) = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}, \phi((123)) = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \phi((132)) = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

Then ϕ is a faithful representation of S_3 with $\chi_\phi = \chi_2$. Hence ϕ is an irreducible representation of S_3.

Theorem 5.8 (Regular Representation) *Let χ_π be the character afforded by the right regular representation of G. Let $k = |Irr(G)|$. Then we have*

(i) $\chi_\pi = \sum_{i=1}^{k} \chi_i(1_G)\chi_i$,

(ii) $\chi_\pi(1_G) = \sum_{i=1}^{k} [\chi_i(1_G)]^2 = |G|$,

(iii) $\chi_\pi(g) = \sum_{i=1}^{k} \chi_i(1_G)\chi_i(g) = 0$, *for all* $g \in G - \{1_G\}$.

Proof: Assume that $\chi_\pi = \sum_{i=1}^{k} n_i\chi_i$, where n_i are non-negative integers. We claim that $n_i = deg(\chi_i)$. We know that $\pi(g)$ is a permutation on G, for all $g \in G$. Since $xg = x$ if and only if $g = 1_G$, $\pi(g)$ moves all the letters if $g \neq 1_G$. Hence $\chi_\pi(g) =| G |$, if $g = 1_G$, and 0 otherwise.

Since

$$< \chi_\pi, \chi_j >=< \sum_{i=1}^{k} n_i\chi_i, \chi_j >= \sum_{i=1}^{k} n_i < \chi_i, \chi_j >,$$

by the orthogonality of irreducible characters we have

$$< \chi_\pi, \chi_j >= n_j < \chi_j, \chi_j >= n_j.$$

Thus

$$\begin{aligned} n_j &= < \chi_\pi, \chi_j >= \frac{1}{| G |} \sum_{g\in G} \chi_\pi(g)\chi_j(g^{-1}) \\ &= \frac{1}{| G |}(| G | \chi_j(1_G)) = \chi_j(1_G) = deg(\chi_j), for\ all\ j. \end{aligned}$$

(i) By above

$$\chi_\pi = \sum_{i=1}^{k} n_i\chi_i = \sum_{i=1}^{k} \chi_i(1_G)\chi_i.$$

(ii) Since $\chi_\pi(1_G) =| G |$, by part (i) we have

$$\chi_\pi(1_G) =| G |= \sum_{i=1}^{k} \chi_i(1_G)\chi_i(1G) = \sum_{i=1}^{k}[\chi_i(1_G)]^2.$$

(iii) Since $\chi_\pi(g) = 0$ for all $g \in G - \{1_G\}$, by part (i) we have

$$0 = \chi_\pi(g) = \sum_{i=1}^{k} \chi_i(1_G)\chi_i(g).$$

■

Exercise 5.4 *Let A be a square matrix over a field F. Assume that for some $n \in \mathbb{N}$ we have $A^n = I$, the identity matrix. If F contains all the nth roots of 1, show that A is similar to a diagonal matrix.*

Lemma 5.9 *If ρ is a representation of G and g is an element of G, show that there is a representation ϕ of G such that ϕ is equivalent to ρ and $\phi(g)$ is a diagonal matrix.*

Proof: Let $\mid G \mid = n$. Then $g^n = 1_G$, so that $[\rho(g)]^n = I_m$, where $m = deg(\rho)$. Since $\mathbb{C}$ contains all the solutions for the equation $x^n = 1$, $\rho(g)$ is similar to a diagonal matrix D_g. So there is a non-singular matrix P such that $D_g = P\rho(g)P^{-1}$. Now define $\phi : G \to GL(m, \mathbb{C})$ by $\phi(h) = P\rho(h)P^{-1}$, for all h in G. Then ϕ is a representation of G equivalent to ρ with $\phi(g)$ diagonal. ■

Definition 5.2 (Algebraic Integers) *A complex number α is said to be an* **Algebraic Integer** *if it is a root of an equation of the form*

$$x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n = 0, a_i \in \mathbb{Z}.$$

Remark 5.1 (Algebraic Numbers) A complex number α is said to be an **Algebraic Number** if there is $p(x) \in \mathbb{Q}[x]$ such that $P(\alpha) = 0$. It can be shown that the set of all algebraic numbers is a subfield of $\mathbb{C}$. If α is not an algebraic number, then we say that it is **Transcendental**. For example i and $\sqrt{2}$ are algebraic numbers (in fact they are algebraic integers). Hermite, C (1822–1905) and later Hilbert, D proved that e is transcendental. Lindemann, CLF (1852–1939) in 1882 proved the transcendence of π. Hilbert's 7th problem is concerned with the transcendence of complex numbers of the form a^b:

Hilbert's Seventh Problem If $a, b \in \mathbb{C}$ such that a is an algebraic number and $a \notin \{0, 1\}$, and b is an irrational algebraic number, then a^b is transcendental.

A O Gelfond in 1934 proved that Hilbert's seventh problem is true. For example $2^{\sqrt{2}}$, 2^i and i^i are transcendental. But what about the case when a and b are both transcendental? It is not known whether π^π, π^e or e^e is transcendental. However note that since

$$e^\pi = \frac{1}{e^{-\pi}} = \frac{1}{i^{2i}} = i^{-2i},$$

e^π is transcendental.

Now we establish some basic results on algebraic integers. In th following we show that the set of all algebraic integers form a ring. This ring plays a fundamental role in Number Theory.

Lemma 5.10 *Let $\alpha_1, \alpha_2, \cdots, \alpha_k$ be complex numbers, not all zero, and suppose that $\alpha \in \mathbb{C}$ satisfy equations of the form*

$$\alpha\alpha_i = \sum_{j=1}^{k} a_{ij}\alpha_j, i = 1, 2, \cdots, k, \quad (1)$$

where $a_{ij} \in \mathbb{Z}$. Then α is an algebraic integer.

Proof: Equations in (1) represents a linear homogeneous system for $\alpha_1, \alpha_2, \cdots, \alpha_k$. Since, by the hypothesis, system (1) has non-zero solution, the determinant of the coefficient matrix must be equal to zero, that is

$$det \begin{pmatrix} \alpha - a_{11} & -a_{12} & -a_{13} & \cdots & -a_{1k} \\ -a_{21} & \alpha - a_{22} & -a_{23} & \cdots & -a_{2k} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ -a_{k1} & -a_{k2} & -a_{k3} & \cdots & \alpha - a_{kk} \end{pmatrix} = 0.$$

We can see that the above determinant is a monic polynomial of degree k in α with integer coefficients. Hence α is an algebraic integer. ■

Lemma 5.11 *If α and β are algebraic integers, so are $\alpha + \beta$ and $\alpha\beta$.*

Proof: Suppose that α and β satisfy the following polynomial equations

$$\alpha^r = a_1\alpha^{r-1} + a_2\alpha^{r-2} + \cdots + a_{r-1}\alpha + a_r, a_i \in \mathbb{Z},$$

$$\beta^s = b_1\beta^{s-1} + b_2\beta^{s-2} + \cdots + b_{s-1}\beta + b_s, b_i \in \mathbb{Z}.$$

Then for any non-negative integer l, α^l can be written as a linear combination (with integer coefficients) of $1, \alpha, \alpha^2, \cdots, \alpha^{r-1}$. Similarly for any non-negative integer m, β^m can be written as a linear combination (with integer coefficients) of $1, \beta, \beta^2, \cdots, \beta^{s-1}$.

Let $\alpha_1, \alpha_2, \cdots, \alpha_k$ be the products $\alpha^i\beta^j$, where $i.j \in \mathbb{Z}$, $0 \le i \le r-1$ and $0 \le j \le s-1$, arranged in some fixed order. Then any product of the form $\alpha^l\beta^m$ can be represented in terms of $\alpha^i\beta^j$, that is in terms of $\alpha_1, \alpha_2, \cdots, \alpha_k$ with integer coefficients. Hence there are equations

$$(\alpha + \beta)\alpha_i = \sum_{j=1}^{k} c_{ij}\alpha_j, 0 \le i \le k, c_{ij} \in \mathbb{Z},$$

$$(\alpha\beta)\alpha_i = \sum_{j=1}^{k} d_{ij}\alpha_j, 0 \le i \le k, d_{ij} \in \mathbb{Z}.$$

Now Lemma 5.2.10 implies that $\alpha + \beta$ and $\alpha\beta$ are algebraic integers. ■

Exercise 5.5 Let $\alpha \in \mathbb{Q}$. If α is an algebraic integer, show that $\alpha \in \mathbb{Z}$.

Theorem 5.12 *If χ is a character of a group G, then for any $g \in G, \chi(g)$ is an algebraic integer.*

Proof: Since G is finite, $g^n = 1_G$ for some $n \in \mathbb{N}$. Let ρ be a representation of degree m of G that affords χ. Then $[\rho(g)]^n = I_m$, and by Lemma 5.2.9 $\rho(g)$ is similar to a diagonal matrix. W.L.O.G we may assume that $\rho(g)$ itself is diagonal (because similar matrices have the same trace). So let

$$\rho(g) = diag(\epsilon_1, \epsilon_2, \cdots, \epsilon_m) = \begin{pmatrix} \epsilon_1 & 0 & 0 & \cdots & 0 \\ 0 & \epsilon_2 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \cdots & \epsilon_m \end{pmatrix},$$

with $\epsilon_i \in \mathbb{C}$. Now since $[\rho(g)]^n = I_m$, we have $\epsilon_i^n = 1$, which imply that ϵ_i's are nth roots of unity and hence are all algebraic integers. Since $\chi(g) = trace(\rho(g)) = \sum_{i=1}^m \epsilon_i$, by Lemma 5.2.11 we have that $\chi(g)$ is an algebraic integer. In fact $\chi(g)$ is a sum of nth roots of unity, where $n = o(g)$. ■

If bar (-) denotes the complex conjugation $\overline{a+bi} = a - bi$ in $\mathbb{C}$, then we have the following result on the conjugation of character values:

Corollary 5.13 *If χ is a character of a group G, then for any $g \in G$ we have $\chi(g^{-1}) = \overline{\chi(g)}$.*

Proof: By the Theorem 5.2.12, we have $\chi(g) = \sum_{j=1}^m \epsilon_j$, where ϵ_i's are nth roots of unity with $n = o(g)$ and $\rho(g)$ similar to $diag(\epsilon_1, \epsilon_2, \cdots, \epsilon_m)$. Since $\rho(g^{-1}) = [\rho(g)]^{-1}$, $\rho(g^{-1})$ is similar to

$$[diag(\epsilon_1, \epsilon_2, \cdots, \epsilon_m)]^{-1} = diag(\epsilon_1^{-1}, \epsilon_2^{-1}, \cdots, \epsilon_m^{-1})$$

and hence $\chi(g^{-1}) = \sum_{j=1}^m \epsilon_j^{-1}$. We know that $\epsilon_j = exp(\frac{2k_j\pi}{n} i)$ for some $k_j \in \mathbb{Z}$ such that $0 \leq k_j \leq n-1$. Since $\epsilon_j \overline{\epsilon_j} = |\epsilon_j|^2 = 1$, we deduce that $\overline{\epsilon_j} = \epsilon_j^{-1}$ for all $0 \leq j \leq m$. Hence

$$\chi(g^{-1}) = \sum_{j=1}^m \epsilon_j^{-1} = \sum_{j=1}^m \overline{\epsilon_j} = \overline{(\sum_{j=1}^m \epsilon_j)} = \overline{\chi(g)}.$$

■

Exercise 5.6 Let ρ be a representation of a group G. Assume that χ is the character afforded by ρ. Show that

(i) $|\chi(g)| \leq \chi(1_G)$, for all $g \in G$.

(ii) If $|\chi(g)| = \chi(1_G)$, then $\rho(g)$ is a scalar matrix.

(iii)* $\chi(g) = \chi(1_G)$ if and only if $g \in ker(\rho)$.

Definition 5.3 (F-Algebra) *If F is afield and A is a vector space over F, then we say that A is an F-Algebra if*

(i) A is a ring with identity,

(ii) for all $\lambda \in F$ and $x, y \in A$, we have $\lambda(xy) = \lambda(x)y = x(\lambda y)$.

Example 5.2 (i) $M_{n\times n}(F)$ is the algebra of all $n \times n$ matrices over a field F.

(ii) Let V be vector space over F. Consider $End(V) = L(V, V) = Hom_F(V, V)$. Then $End(V)$ is a ring with identity under the **addition** and **composition** of linear transformations on V, that is $(f + g)(\alpha) = f(\alpha) + g(\alpha)$ and $(f \circ g)(\alpha) = f(g(\alpha))$. for all $\alpha \in V$ and all $f, g \in End(V)$. Define the **scalar multiplication** on $End(V)$ by $(\lambda f)(\alpha) = \lambda f(\alpha)$, for all $f \in End(V)$ and for all $\alpha \in V$. Then $End(V)$ is a vector space over F. Now

$$\begin{aligned}[\lambda(f \circ g)](\alpha) &= \lambda[(f \circ g)(\alpha)] = \lambda[f(g(\alpha))] \\ &= (\lambda f)(g(\alpha)) = [(\lambda f) \circ g](\alpha).\end{aligned}$$

Hence $\lambda(f \circ g) = (\lambda f) \circ g$. Similarly we have

$$\begin{aligned}[\lambda(f \circ g)](\alpha) &= \lambda[(f \circ g)(\alpha)] \\ &= (f \circ g)(\lambda\alpha), \textit{since } f \circ g \in End(V) \\ &= f(g(\lambda\alpha)) = f(\lambda g(\alpha)) \\ &= [f \circ (\lambda g)](\alpha),\end{aligned}$$

so that $\lambda(f \circ g) = f \circ (\lambda g)$.

Thus we have shown that $End(V)$is an F-Algebra.

Now we introduce another example of an algebra, the one which plays an important part in the theory of representations, namely the Group Algebra $\mathbb{C}[G]$.

Definition 5.4 (Group Algebra) *Let G be a finite group and F be any field. Then by $F[G]$ we mean the set of* **formal forms** $\{\sum_{g \in G} \lambda_g.g : \lambda_g \in F\}$. *We define the operations on $F[G]$ by*

(i) $\sum_{g \in G} \lambda_g g + \sum_{g \in G} \mu_g g := \sum_{g \in G}(\lambda_g + \mu_g)g$,

(ii) $\lambda(\sum_{g \in G} \lambda_g g) := \sum_{g \in G}(\lambda\lambda_g)g$, $\lambda \in F$,

(iii) $(\sum_{g \in G} \lambda_g g).(\sum_{g \in G} \mu_g g) := \sum_{g \in G}[\sum_{h \in G} \lambda_h \mu_{h^{-1}g}]g$.

Notice that the definition of multiplication given in (iii) is the result of assuming linearity and the multiplication in G. Under the above operations, $F[G]$ is an F-algebra. The element of $F[G]$ for which $\lambda_g = 1_F$ and $\lambda_h = 0_F$ if $h \neq g$ is identified by g, that is $1_F.g = g$. Under this identification we embed G into $F[G]$ and in fact G becomes a basis for $F[G]$.

Remark 5.2 (i) If $|G| > 1$, then $F[G]$ has always zero divisors: Let $g \in G$ such that $o(g) = m \neq 1$. Then $1_G - g$ and $1_G + g + g^2 + \cdots + g^{m-1}$ are two non-zero elements of $F[G]$, and we have

$$(1_G - g).(1_G + g + g^2 + \cdots + g^{m-1}) = 1_G - g^m = 1_G - 1_G = 0.$$

(ii) Consider the group $G = V_4 = \{e, a, b, c\}, F = \mathbb{C}$. let $e + ia + \sqrt{2}\, b$ and $\sqrt{2}\, b - ic$ be two elements of $\mathbb{C}[G]$. Then

$$\begin{aligned}(e + ia + \sqrt{2}\, b).(\sqrt{2}\, b - ic) &= \sqrt{2}\, b - ic + \sqrt{2}\, iab - i^2 ac + 2b^2 - i\sqrt{2}\, bc \\ &= \sqrt{2}\, b - ic + \sqrt{2}\, ic + b + 2e - i\sqrt{2}\, a \\ &= 2e - i\sqrt{2}\, a + (\sqrt{2} + 1)b + i(\sqrt{2} - 1)c.\end{aligned}$$

Alternatively we can use part (iii) of the Definition 5.2.4, and we get

$$\begin{aligned}(e + ia + \sqrt{2}\, b).(\sqrt{2}\, b - ic) &= (0 + 0 + \sqrt{2} \times \sqrt{2} + 0)e \\ &+ (1 \times 0 + i \times 0 + \sqrt{2} \times -i + 0)a \\ &+ (\sqrt{2} + i \times -i + 0 + 0)b + (-1 + \sqrt{2} + 0 + 0)c.\end{aligned}$$

(iii) Obviously G is a subgroup of $U_{F[G]}$.

Exercise 5.7 (i) Let $G = D_8 =< r, s : r^4 = s^2 = e, rs = sr^{-1} >$. Assume that $\alpha = r^2 + r - 2s$ and $\beta = -3r^2 + rs$ are two elements of the integral group ring $\mathbb{Z}[G]$. Compute $\beta\alpha$, $\alpha\beta - \beta\alpha$ and $\beta\alpha\beta$.

(ii) Consider the following elements of $\mathbb{Z}[S_3]$:

$$\alpha = 3(1\ 2) - 5(2\ 3) + 14(1\ 2\ 3), \beta = 6e + 2(2\ 3) - 7(1\ 2\ 3),$$

where $e = 1_{S_3}$. Compute the following elements of $\mathbb{Z}[S_3] : 2\alpha - 3\beta, \beta\alpha, \alpha\beta$.

Definition 5.5 (Class Sums) *Let $C_1, C_2, \cdots, C_r$ be the conjugacy classes of elements of G. For $1 \leq i \leq r$ we define the* **Class Sums** *K_i by $K_i = \sum_{g \in C_i} g$. Then clearly $K_i \in F[G]$ and we have the following result:*

Theorem 5.14 *The set $\{K_1, K_2, \cdots, K_r\}$ is a basis for the centre of the group ring $\mathbb{C}[G]$.*

Proof: If $g \in G$, then $g^{-1}C_i g = C_i$. Hence we have

$$g^{-1}K_i g = g^{-1}(\sum_{h \in C_i} h)g = \sum_{h \in C_i} g^{-1}hg = \sum_{h' \in C_i} h' = K_i.$$

Thus $K_i g = gK_i$ for all $g \in G$. Hence $K_i \in Z(\mathbb{C}[G])$, where $Z(\mathbb{C}[G])$ denotes the centre of $\mathbb{C}[G]$.

Since distinct conjugacy classes are disjoint, $\{K_1, K_2, \cdots, K_r\}$ is a linearly independent set (why?). Now let $u = \sum_{g \in G} \lambda_g g$ be an element of $Z(\mathbb{C}[G])$. Let $x \in G$. Then

$$xu = \sum_{g \in G} \lambda_g xg = \sum_{g \in G} \lambda_g (xgx^{-1})x,$$

$$ux = \sum_{g \in G} \lambda_g (gx) = \sum_{g \in G} \lambda_{xgx^{-1}} (xgx^{-1})x,$$

and since $ux = xu$, we get $\sum_{g \in G} \lambda_g (xgx^{-1})x = \sum_{g \in G} \lambda_{xgx^{-1}} (xgx^{-1})x$. Hence $\lambda_g = \lambda_{xgx^{-1}}$ for all $x \in G$. Thus the coefficients of all conjgates of g are the same in u. Hence $u = \sum_{i=1}^{r} (\lambda_i \sum_{g \in C_i} g) = \sum_{i=1}^{r} \lambda_i K_i$. Thus $\{K_1, K_2, \cdots, K_r\}$ is a basis for $Z(\mathbb{C}[G])$. ■

Remark 5.3 Let ρ be a representation of G. Then ρ is a homomorphism from G into $GL(n, \mathbb{C})$ for some $n \in \mathbb{N}$. We can extend ρ by linearity to an $\mathbb{C}$-algebra homomorphism $\rho : \mathbb{C}[G] \longrightarrow M_{n \times n}(\mathbb{C})$. Conversely if $\rho : \mathbb{C}[G] \longrightarrow M_{n \times n}(\mathbb{C})$ is a representation of $\mathbb{C}[G]$ (that is ρ is an $\mathbb{C}$-algebra homomorphism), then $\rho(1_G) = I_n$. It follows that for all $g \in G$, $\rho(g)$ is non-singular and $[\rho(g)]^{-1}$ is equal to $\rho(g^{-1})$. Hence the restriction of ρ to G (note that $G \subseteq \mathbb{C}[G]$) will be a representation of G over $\mathbb{C}$.

Theorem 5.15 *If ρ is an irreducible representation of degree m of $\mathbb{C}[G]$ with the character χ, then* *(i)* $\rho(K_i) = d_i I_m, d_i \in \mathbb{C}$,

(ii) $K_i K_j = \sum_{k=1}^{r} \lambda_{ijk} K_k, \lambda_{ijk} \in \mathbb{N} \cup \{0\}$,

(iii) $d_i d_j = \sum_{k=1}^{r} \lambda_{ijk} d_k$,

(iv) $d_i = h_i \chi(g_i)/\chi(1_G), h_i = |C_i|, g_i \in C_i$.

Proof: (i) Since $K_i \in Z(\mathbb{C}[G])$ by Theorem 5.2.14, $\rho(K_i)$ commutes with all elements of $\rho(G)$. Now since ρ is irreducible, it follows from Corollary 5.1.9 that $\rho(K_i) = d_i I_m$ for some $d_i \in \mathbb{C}$.

(ii) Since $K_i, K_j \in Z(\mathbb{C}[G])$, we have $K_i K_j \in Z(\mathbb{C}[G])$. So by Theorem 5.2.14, $\exists \lambda_{ijk} \in \mathbb{C}$ such that $K_i K_j = \sum_{k=1}^{r} \lambda_{ijk} K_k$. If we write this equation in terms of elements of G, then since the coefficients on the left hand-side are non-negative integers, λ_{ijk} must be non-negative integers.

(iii) Using parts (i) and (ii), we get

$$\begin{aligned} d_i d_j I_m &= \rho(K_i)\rho(K_j) = \rho(K_i K_j) = \rho(\sum_{k=1}^{r} \lambda_{ijk} K_k) \\ &= \sum_{k=1}^{r} \lambda_{ijk} \rho(K_k) = (\sum_{k=1}^{r} \lambda_{ijk} d_k) I_m. \end{aligned}$$

Hence $d_i d_j = \sum_{k=1}^{r} \lambda_{ijk} d_k$.

(iv) By part (i) we have

$$\begin{aligned} h_i \chi(g_i) &= \sum_{g \in C_i} \chi(g) = \sum_{g \in C_i} trace(\rho(g)) \\ &= trace(\sum_{g \in C_i} \rho(g)) = trace(\rho(\sum_{g \in C_i} g)) = trace(\rho(K_i)) \\ &= trace(d_i I_m) = m d_i = d_i \chi(1_G). \end{aligned}$$

Hence $d_i = h_i \chi(g_i)/\chi(1_G)$. ■

Corollary 5.16 *The d_i's in Theorem 5.2.15 are algebraic integers.*

Proof: By part (iii) of Theorem 5.2.15, we have $d_i d_j = \sum_{k=1}^{r} \lambda_{ijk} d_k$, where λ_{ijk} are non-negative integers. For a fixed j, let B be the $r \times r$ matrix (λ_{ijk}) and D be the column matrix $(d_k)_{r \times 1}$. Then we have $(d_j I_r) D = BD$ and hence $(B - d_j I_r) D = 0_{r \times r}$.

Since by Theorem 5.2.15 (part (iv)) we have

$$d_1 = h_1 \chi(1_G)/\chi(1_G) = h_1 = 1 \neq 0,$$

D is a non-zero matrix. Hence $B - d_j I_r$ is a singular matrix, so that $det(B - d_j I_r) = 0$. Since λ_{ijk} are integers, the equation $det(B - d_j I_r) = 0$ produces a polynomial equation for d_j with integer coefficients and leading coefficient of ± 1. Thus d_j is an algebraic integer. ∎

Note: *If C_i is a conjugacy class of G, then $C_{i'} = \{g \in G : g^{-1} \in C_i\}$ is also a conjugacy class of G. Obviously $C_i = C_{i'}$ if and only if $g \sim g^{-1}$ for all $g \in C_i$.*

Theorem 5.17 (Orthogonality relations) *Let $Irr(G) = \{\chi_1, \chi_2, \cdots, \chi_k\}$. Then*

(i) $\frac{1}{|G|}\sum_{g\in G} \chi_i(g)\overline{\chi_j(g)} = \delta_{ij}$, *row-orthogonality.*

(ii) $\sum_{s=1}^{k} \chi_s(g_i)\chi_s(g_j) = \delta_{ij'}|C_G(g_j)|$, *column-orthogonality relation.*

Proof: (i)

$$\begin{aligned}\delta ij &= <\chi_i, \chi_j>= \frac{1}{|G|}\sum_{g\in G}\chi_i(g)\chi_j(g^{-1})\\ &= \frac{1}{|G|}\sum_{g\in G}\chi_i(g)\overline{\chi_j(g)}\end{aligned}$$

by Corollary 5.2.13.

(ii) We know that $K_iK_j = \sum_{m=1}^{r}\lambda_{ijm}K_m$. Then 1_G occurs in the expansion of K_iK_j if and only if $i = j'$ (that is g_i is conjugate to g_j^{-1}). Thus $\lambda_{ij1} = 0$ if $i \neq j'$ and $\lambda_{ij1} = h_i$ if $i = j'$. For each $1 \leq s \leq k$, using Theorem 5.2.15 we get

$$\begin{aligned}d_id_j &= [h_i\chi_s(g_i)/\chi_s(1_G)] \times [h_j\chi_s(g_j)/\chi_s(1_G)]\\ &= \sum_{m=1}^{r}\lambda_{ijm}[h_m\chi_s(g_m)/\chi_s(1_G)].\end{aligned}$$

Thus

$$h_ih_j\chi_s(g_i)\chi_s(g_j) = \sum_{m=1}^{r}\lambda_{ijm}h_m\chi_s(1_G)\chi_s(g_m).$$

Therefore

$$h_ih_j\sum_{s=1}^{k}\chi_s(g_i)\chi_s(g_j) = \sum_{m=1}^{r}[\lambda_{ijm}h_m\sum_{s=1}^{k}\chi_s(1_G)\chi_s(g_m)] =$$

$$\lambda_{ij1}h_1\sum_{s=1}^{k}\chi_s(1_G)\chi_s(1_G) + \sum_{m=2}^{r}[\lambda_{ijm}h_m\sum_{s=1}^{k}\chi_s(1_G)\chi_s(g_m)] = \lambda_{ij1}|G| + 0,$$

by Theorem 5.2.8. This show that

$$\begin{aligned}\sum_{s=1}^{k}\chi_s(g_i)\chi_s(g_j) &= \lambda_{ij1}|G|/h_ih_j\\ &= 0 \times |G|/h_ih_j = 0,\ if\ i \neq j'\\ &= h_i \times |G|/h_ih_j = |G|/h_j = |C_G(g_j)|,\ if\ i = j'.\end{aligned}$$

Hence $\sum_{s=1}^{k}\chi_s(g_i)\chi_s(g_j) = \delta_{ij'}|C_G(g_j)|$.∎

Exercise 5.8 Show that $\sum_{s=1}^{k} \chi_s(g_i)\overline{\chi_s(g_j)} = \delta_{ij}|C_G(g_j)|$.

Theorem 5.18 (The number of irreducible characters) *The number of irreducible characters of a group G equals the number of comjugacy classes of G.*

Proof: Let $Irr(G) = \{\chi_1, \chi_2, \cdots, \chi_k\}$ and let r be the number of conjugacy classes of G. Then by the Theorem 5.2.6 we have $k \leq r$. Now let

$$S = \{(\chi_1(g_i), \chi_2(g_i), \cdots, \chi_k(g_i)) : 1 \leq i \leq r\}.$$

We claim that S is a linearly independent subset of $\mathbb{C}^k$. Assume that $\exists \lambda_i \in \mathbb{C}$ such that

$$\sum_{i=1}^{r} \lambda_i(\chi_1(g_i), \chi_2(g_i), \cdots, \chi_k(g_i)) = 0.$$

Then we must have $\sum_{i=1}^{r} \lambda_i \chi_s(g_i) = 0, 1 \leq s \leq k$. So for each j we have

$$[\sum_{i=1}^{r} \lambda_i \chi_s(g_i)]\chi_s(g_j) = 0, 1 \leq s \leq k.$$

Hence

$$\sum_{s=1}^{k}[\sum_{i=1}^{r} \lambda_i \chi_s(g_i)]\chi_s(g_j) = 0 \; for \; all \; j.$$

So that

$$\sum_{i=1}^{r} \lambda_i[\sum_{s=1}^{k} \chi_s(g_i)\chi_s(g_j)] = 0 \; for \; all \; j.$$

Now applying Theorem 5.2.17 (ii), we get

$$\sum_{i=1}^{r} \lambda_i \delta_{ij'}|C_G(g_j)| = 0.$$

That is $\lambda_{j'}|C_G(g_j)| = 0$, so that $\lambda_{j'} = 0$ for all $1 \leq j \leq r$. This shows that $\lambda_j = 0$ for all $1 \leq j \leq r$. Thus S is a linearly independent subset of $\mathbb{C}^k$, and hence we have

$$r = |S| \leq dim(\mathbb{C}^k) = k.$$

Therefore $r = k$ as required. ■

Note: *Let Δ be the $r \times r$ matrix $(\chi_i(g_j)) = (a_{ij})$. Then Δ is called the* **character table** *of G. The rows are indexed by the irreducible characters of G and the columns by the conjugacy classes of G. We take the first row and first column to be indexed by the trivial character and 1_G respectively, that is χ_1 is the trivial character and $g_1 = 1_G$. Theorem 5.2.18 shows that columns of Δ are linearly independent, and hence Δ is non-singular. In particular the rows of Δ are also linearly independent.*

Exercise 5.9 Compute Δ^{-1}. [Hint: First let $B = (b_{jl})_{r \times r}$, where $b_{jl} = \frac{1}{|C_G(g_j)|}\overline{\chi_l(g_j)}$. Then show that $B = \Delta^{-1}$].

Note: *Property (ii) in Theorem 5.2.17 implies that*

$$\begin{aligned}\sum_{s=1}^{r}[\chi_s(g_i)]^2 &= 0 \ \textit{if } g_i \textit{ not conjugate to } g_i^{-1} \\ &= |C_G(g_i)| \ \textit{otherwise.}\end{aligned}$$

In particular we have $\sum_{s=1}^{r}[\chi_s(1_G)]^2 = |G|$, *which is the result we proved in Theorem 5.2.8. This shows that the sum of squares of the degrees of the irreducible characters of* G *is* $|G|$.

Exercise 5.10 Let ρ be a representation of G of degree m. Define $\rho*$ from G into $GL(m,\mathbb{C})$ by $\rho*(g) = [\rho(g^{-1})]^t$, transpose of $\rho(g^{-1})$. Then show that

(i) $\rho*$ is a representation of degree m of G,

(ii) $\chi_{\rho*}(g) = \overline{\chi_\rho(g)}$, for all $g \in G$,

(iii) If ρ is irreducible, so is $\rho*$,

(iv) If $\rho \sim \phi$, then $\rho* \sim \phi*$.

Theorem 5.19 *The degree of an irreducible representation of a finite group* G *divides* $|G|$.

Proof: By Theorem 5.2.15 (iv), $\frac{h_k\chi_i(g_k)}{\chi_i(1_G)}$ are algebraic integers for all k and i. By Theorem 5.2.12, each $\chi_j(g_k)$ is an algebraic integer. Hence

$$\alpha = \sum_{j=1}^{r}\sum_{k=1}^{r} h_k \frac{\chi_i(g_k)}{\chi_i(1_G)}\chi_j(g_k)$$

is an algebraic integer by Lemma 5.2.11. Now

$$\begin{aligned}\alpha &= \sum_{j=1}^{r}\sum_{g\in G}\frac{\chi_i(g)\chi_j(g)}{\chi_i(1_G)} = \sum_{j=1}^{r}\sum_{g\in G}\frac{1}{\chi_i(1_G)}[\chi_i(g)\chi_j(g)] \\ &= \sum_{j=1}^{r}\sum_{g\in G}\frac{1}{\chi_i(1_G)}[\chi_i(g)\overline{\chi_j(g^{-1})}] \\ &= \frac{1}{\chi_i(1_G)}\sum_{j=1}^{r}[\sum_{g\in G}[\chi_i(g)\overline{\chi_j*(g)}] = \frac{|G|}{\chi_i(1_G)}\sum_{j=1}^{r}\delta_{ij*} = |G|/\chi_i(1_G),\end{aligned}$$

by Theorem 5.2.17, part (i). Hence $\alpha \in \mathbb{Q}$. Since α is an algebraic integer and $\alpha \in \mathbb{Q}$, we must have $\alpha \in \mathbb{Z}$. Thus $\chi_i(1_G)$ divides $|G|$. ■

Note: *The integers* λ_{ijk} *defined in the Theorem 5.2.15 (ii) are called* ***Class Algebra Constants****. In the following corollary we will produce a formula for these integers. This formula plays an important role in the application of character theory of finite groups.*

Corollary 5.20

$$\lambda_{ijk} = \frac{|G|}{|C_G(g_i)||C_G(g_j)|} \sum_{s=1}^{r} \frac{\chi_s(g_i)\chi_s(g_j)\overline{\chi_s(g_k)}}{\chi_s(1_G)}.$$

Proof: Let ρ_s denote the representation that affords χ_s. Since $K_iK_j = \sum_{m=1}^{r} \lambda_{ijm}K_m$, we have

$$\rho_s(K_i)\rho_s(K_j) = \rho_s(K_iK_j) = \sum_{m=1}^{r} \lambda_{ijm}\rho_s(K_m). \quad (*)$$

Now since $\rho_s(K_i) = d_iI_n$ and $\rho_s(K_j) = d_jI_n$, where n is the degree of ρ_s (see Theorem 5.2.15), we have

$$\rho_s(K_i) = h_i\frac{\chi_s(g_i)}{\chi_s(1_G)}I_n \text{ and } \rho_s(K_j) = h_j\frac{\chi_s(g_j)}{\chi_s(1_G)}I_n,$$

by Theorem 5.2.15. Now by using the relation (*) above, we get

$$h_i\frac{\chi_s(g_i)}{\chi_s(1_G)} \times h_j\frac{\chi_s(g_j)}{\chi_s(1_G)} = \sum_{m=1}^{r} \lambda_{ijm}h_m\frac{\chi_s(g_m)}{\chi_s(1_G)}.$$

Hence

$$\sum_{m=1}^{r} \lambda_{ijm}h_m\chi_s(g_m) = h_ih_j\chi_s(g_i)\chi_s(g_j)/\chi_s(1_G), \quad (1)$$

multiplying by both sides of (1) by $\overline{\chi_s(g_k)}$ and summing from $s = 1$ to $s = r$ we obtain

$$\sum_{m=1}^{r} \lambda_{ijm}h_m[\sum_{s=1}^{r} \chi_s(g_m)\overline{\chi_s(g_k)}] = h_ih_j\sum_{s=1}^{r} \frac{\chi_s(g_i)\chi_s(g_j)\overline{\chi_s(g_k)}}{\chi_s(1_G)}. \quad (2)$$

Since

$$\sum_{s=1}^{r} \chi_s(g_m)\overline{\chi_s(g_k)} = \delta_{km}|C_G(g_k)|$$

by Exercise 5.2.7, we have

$$\sum_{m=1}^{r} \lambda_{ijm}h_m\delta_{km}|C_G(g_k)| = h_ih_j\sum_{s=1}^{r} \frac{\chi_s(g_i)\chi_s(g_j)\overline{\chi_s(g_k)}}{\chi_s(1_G)}.$$

So that

$$\lambda_{ijk}h_k|C_G(g_k)| = h_ih_j\sum_{s=1}^{r} \frac{\chi_s(g_i)\chi_s(g_j)\overline{\chi_s(g_k)}}{\chi_s(1_G)}.$$

Thus

$$\lambda_{ijk}|G| = \frac{|G||G|}{|C_G(g_i)||C_G(g_j)|}\sum_{s=1}^{r} \frac{\chi_s(g_i)\chi_s(g_j)\overline{\chi_s(g_k)}}{\chi_s(1_G)}.$$

This gives the desired formula for λ_{ijm}.■

Example 5.3 (i) If $g^2 = 1_G$, then $\chi_i(g) \in \mathbb{Z}$ for all $\chi_i \in Irr(G)$: Because $g^2 = 1_G$ implies that $g = g^{-1}$. If $g = 1_G$, then $\chi_i(g) = \chi_i(1_G) = deg(\chi_i) \in \mathbb{Z}$. If g is not the identity, then $o(g) = 2$ and hence $\chi_i(g)$ is a sum of 2nd roots of unity. Since the roots are 1 and -1, clearly $\chi_i(g) \in \mathbb{Z}$.

(ii) If g is conjugate to g^{-1}, then $\chi_i(g) \in \mathbb{R}$ for all $\chi_i \in Irr(G)$: Because g conjugate to g^{-1} implies that $\chi_i(g) = \chi_i(g^{-1}) = \overline{\chi_i(g)}$. Thus $\chi_i(g) \in \mathbb{R}$.

(iii) Assume that $g \in G$ is an element of order three and $g \sim g^{-1}$. Then $\chi_i(g) \in \mathbb{Z}$ for all $\chi_i \in Irr(G)$: Because $g \sim g^{-1}$ implies that $\chi_i(g) \in \mathbb{R}$ for all $\chi_i \in Irr(G)$, by part (ii). Let $\chi_i(g) = \varepsilon_1 + \varepsilon_2 + \cdots + \varepsilon_m$, where $\epsilon_i \in \{1, -\frac{1}{2} - \frac{\sqrt{3}}{2}i, -\frac{1}{2} + \frac{\sqrt{3}}{2}i\}$. Assume that for some j, $1 \leq j \leq m$, we have

$$\epsilon_j = -\frac{1}{2} - \frac{\sqrt{3}}{2}i \text{ or } \epsilon_j = -\frac{1}{2} + \frac{\sqrt{3}}{2}i.$$

Then since $\chi_i(g) \in \mathbb{R}$, $\overline{\epsilon_j}$ must also appear in $\chi_i(g)$. Now since $\epsilon_j + \overline{\epsilon_j} = -1$, we deduce that $\chi_i(g) \in \mathbb{Z}$.

Example 5.4 (Character Table of S_4) In S_4 there are 5 conjugacy classes and hence $Irr(S_4) = 5$. Consider the map $\rho_2 : S_4 \longrightarrow \mathbb{C}$ given by $\rho_2(\alpha) = 1$ if α is even and $\rho_2(\alpha) = -1$ if α is odd. Then ρ_2 is a representation of degree 1 and hence $\rho_2 = \chi_{\rho_2}$. let denote this character by χ_2. Then we have

$$\chi_2(1_{S_4}) = \chi_2((1\ 2)(3\ 4)) = \chi_2((1\ 2\ 3)) = 1$$

and

$$\chi_2((1\ 2)) = \chi_2((1\ 2\ 3\ 4)) = -1.$$

So we have the following table:

Classes of S_4	1_{S_4}	(1 2)(3 4)	(1 2)	(1 2 3 4)	(1 2 3)
h_i	1	3	6	6	8
χ_2	1	1	-1	-1	1

Since

$$\begin{aligned} < \chi_2, \chi_2 > &= \frac{1}{24}[1 + 3(1)(1) + 6(-1)(-1) + 6(-1)(-1) + 8(1)(1)] \\ &= \frac{1}{24}[1 + 3 + 6 + 6 + 8] = 24/24 = 1, \end{aligned}$$

χ_2 is irreducible.

Now let $\pi : S_4 \longrightarrow GL(4, \mathbb{C})$ be the natural permutation representation of S_4. Then $\chi_\pi(g)$ is equal to the number of fixed points of g on the set $\{1, 2, 3, 4\}$. Then we have

Classes of S_4	1_{S_4}	(1 2)(3 4)	(1 2)	(1 2 3 4)	(1 2 3)
h_i	1	3	6	6	8
χ_π	4	0	2	0	1

It is not difficult to see that $< \chi_\pi, \chi_\pi >= 2$ and $< \chi_\pi, \chi_1 >= 1$, where χ_1 is the trivial charascter. hence $\chi_\pi = \chi_1 + \chi_3$, where χ_3 is an irreducible character of degree $4 - 1 = 3$. Then we have $\chi_3(g) = \chi_\pi(g) - \chi_1(g)$, for all g in S_4.

Now it remains to find two more irreducible characters of S_4, namely χ_4 and χ_5. Since $\sum_{i=1}^{5}[\chi_i(1_{S_4})]^2 = |G| = 24$, we have

$$[\chi_4(1_{S_4})]^2 + [\chi_5(1_{S_4})]^2 = 24 - (1+1+9) = 24 - 11 = 13 = 4 + 9.$$

This implies that we can assume $deg(\chi_4) = 2$ and $deg(\chi_4) = 3$. So far we have the following information for the character table of S_4 :

Classes of S_4	1_{S_4}	(1 2)(3 4)	(1 2)	(1 2 3 4)	(1 2 3)
h_i	1	3	6	6	8
χ_1	1	1	1	1	1
χ_2	1	1	-1	-1	1
χ_3	3	-1	1	-1	0
χ_4	2	a	b	c	d
χ_5	3	e	f	g	h

We are able to complete the character table by means of the orthogonality relations. First notice that, since $g \sim g^{-1}$ for all $g \in S_4$, we have $\{a, b, c, d, e, f, g, h\} \subseteq \mathbb{R}$. Using Example 5.2.3, parts (i) and (ii), we have $\{a, e, b, f, d, h\} \subseteq \mathbb{Z}$. Now using the orthogonality of the first two columns we get

$$1 + 1 - 3 + 2a + 3e = 0,$$

so that

$$2a + 3e = 1. \quad (1)$$

Since $\sum_{i=1}^{5}[\chi_i((1\ 2)(3\ 4))]^2 = |C_{S_4}((1\ 2)(3\ 4))|$, by Note 5.2.7, we have

$$1 + 1 + 1 + a^2 + e^2 = \frac{24}{3} = 8,$$

and hence

$$a^2 + e^2 = 5. \quad (2)$$

Using relations (1) and (2) we obtain $a = 2$ and $e = -1$.

Similarly the orthogonality of the first column with columns three and five give

$$1 - 1 + 3 + 2b + 3f = 0,\ 1 + 1 + 0 + 2d + 3h = 0.$$

We deduce that

$$2b + 3f = -3 \quad (3)$$

and

$$2d + 3h = -2. \quad (4)$$

Since

$$\sum_{i=1}^{5}[\chi_i((1\ 2))]^2 = |C_{S_4}((1\ 2))| = \frac{24}{6} = 4$$

and

$$\sum_{i=1}^{5}[\chi_i((1\ 2\ 3))]^2 = |C_{S_4}((1\ 2\ 3))| = \frac{24}{8} = 3,$$

we get

$$b^2 + f^2 = 4 - 3 = 1 \quad (5)$$

and

$$d^2 + h^2 = 3 - 2 = 1. \quad (6)$$

Now relations (3) and (5) imply that $b = 0$ and $f = -1$. Similarly relations (4) and (6) imply that $d = -1$ and $h = 0$. At this stage we produce the following information on the character table of S_4 :

Classes of S_4	1_{S_4}	(1 2)(3 4)	(1 2)	(1 2 3 4)	(1 2 3)
h_i	1	3	6	6	8
χ_1	1	1	1	1	1
χ_2	1	1	-1	-1	1
χ_3	3	-1	1	-1	0
χ_4	2	2	0	c	-1
χ_5	3	-1	-1	g	0

Using the orthogonality of columns 3 and 4 we obtain

$$1 + 1 - 1 + 0 \times c - g = 0$$

and hence $g = 1$. Now the orthogonality of columns 4 and 5 gives

$$1 - 1 + (-1) \times 0 + c(-1) + 1 \times 0 = 0,$$

and hence $c = 0$. This completes the character table of S_4 :

Classes of S_4	1_{S_4}	(1 2)(3 4)	(1 2)	(1 2 3 4)	(1 2 3)
h_i	1	3	6	6	8
χ_1	1	1	1	1	1
χ_2	1	1	-1	-1	1
χ_3	3	-1	1	-1	0
χ_4	2	2	0	0	-1
χ_5	3	-1	-1	1	0

Exercise 5.11 (Characters of cyclic groups) . Let $G = \langle x \rangle$ be a cyclic group of order n. Let $e^{2k\pi i/n}$ be the nth roots of unity in $\mathbb{C}$, $k = 0, 1, 2, ..., n-1$. Define $\rho_k : G \to \mathbb{C}^*$ by $\rho_k(x^m) = [e^{2k\pi i/n}]^m$. Show that ρ_k define the n distinct irreducible representations of G.

Exercise 5.12 Use the above exercise to construct the character table of the cyclic groups of order 2, 3, 4. 5 and 6.

Exercise 5.13 Calculate the character table of the $\mathbb{V}_4$, the Klien 4-group.

Note: *If G is an abelian group, then all irreducible representations of G are of degree 1. In general, we would like to know how many of the irreducible representations of an arbitrary group G are of degree 1. In the following theorem we give the answer to this question.*

Theorem 5.21 *Let G be a finite group. The number of representations of G of degree 1 is equal to $[G : G']$.*

Proof: If ρ is a representation of degree one of G, then by Exercise 5.3(i) we have $Ker(\rho) \supseteq G'$. Now the define $\phi : G/G' \to \mathbb{C}^*$ by $\phi(gG') = \rho(g)$, for all $g \in G$. Then ϕ defines a representation of degree one for the group G/G' (note that since $G' \subseteq Ker(\rho)$, ϕ is well-defined.) Since G/G' is abelian, it has $[G{:}G']$ conjugacy classes. Hence the group G/G' has $[G{:}G']$ irreducible characters. Since G/G' is abelian, all its irreducible characters are of degree one (see Exercise 5.3, part (ii).) Now consider the natural homomorphism $\pi : G \to G/G'$. If ψ is a representation of G/G' of degree one, then $\psi \circ \pi$ is a representation of degree one of G. Now it is not difficult to see that we have a one-to-one correspondence between the set of all representations of degree one of G and the set of all the irreducible representations of the group G/G'.■

Exercise 5.14 Compute the character table of A_4.

Exercise 5.15 Calculate the character tables of Q (the quaternion group of order 8) and D_8. Show that they have same character tables.

Exercise 5.16 Calculate the character table of A_5. Recall that A_5 is a non-abelain simple group of order 60 and hence $(A_5)' = A5$.

Note: *In the Exercises 5.1.1 and 5.1.2 we observed that there is a one-to-one correspondence between representations of G/N and representations of G with kernel containing N. Furthermore it is not difficult to show that, under this correspondence, irreducible representations correspond to irreducible representations. We put this result in terms of characters in the following theorem. If χ is a character afforded by a representation ρ of G, we define $\ker(\chi)$ to be $\ker(\rho)$.*

Theorem 5.22 *Let $N \trianglelefteq G$.*

(i) *If χ is a character of G and $N \trianglelefteq \ker(\chi)$, then χ is constant on cosets of N in G and $\widehat{\chi}$ on G/N defined by $\widehat{\chi}(gN) = \chi(g)$ is a character of G/N.*

(ii) *If $\widehat{\chi}$ is a character of G/N, then the function χ defined by $\chi(g) = \widehat{\chi}(gN)$ is a character of G.*

(iii) *In both* (i) *and* (ii), $\chi \in Irr(G)$ *iff* $\widehat{\chi} \in Irr(G/N)$.

Proof: (i) and (ii) follow from Exercise 5.1.1 and 5.1.2.
(iii) Let S be a set of coset representatives of N in G. Then we have

$$\begin{aligned} 1 = \langle \chi, \chi \rangle &= \frac{1}{|G|} \sum_{g \in G} \chi(g) \cdot \chi(g^{-1}) \\ &= \frac{1}{|G|} \sum_{g \in S} |N| \cdot \chi(g) \cdot \chi(g^{-1}) \\ &= \frac{1}{|G|} \sum_{g \in S} |N| \cdot \widehat{\chi}(gN) \cdot \widehat{\chi}(g^{-1}N) \\ &= \frac{1}{|G|} \sum_{gN \in G/N} |N| \cdot \widehat{\chi}(gN) \cdot \widehat{\chi}(gN)^{-1} \\ &= \frac{1}{|G/N|} \sum_{gN \in G/N} \widehat{\chi}(gN) \cdot \widehat{\chi}(gN)^{-1} = \langle \widehat{\chi}, \widehat{\chi} \rangle \, . \end{aligned}$$

■

Example 5.5 Consider the group $G = S_4$. Let $N = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \trianglelefteq G$. If $C_i = [g_i]$ is a class of G, then $\widehat{C_i} = [g_i N]$ is a class of G/N. However, distinct classes in G may produce equal classes in G/N. Referring to the character table of S_4 (See Example 5.2.4), we see that

$$\{\chi |\ \chi \in Irr(G),\ N \subseteq \ker(\chi)\} = \{\chi_1, \chi_2, \chi_4\}.$$

Hence $Irr(G/N) = \{\widehat{\chi}_1, \widehat{\chi}_2, \widehat{\chi}_4\}$. Using the character table of S_4 we have

Classes of S_4	1_{S_4}	(1 2)(3 4)	(1 2)	(1 2 3 4)	(1 2 3)
χ_1	1	1	1	1	1
χ_2	1	1	-1	-1	1
χ_2	2	2	0	0	-1

Observe that columns 1 and 2 are identical, as are columns 3 and 4. Deleting repeats, we obtain the character table of G/N

Classes of G/N	N	(1 2)N	(1 2 3)N
$\widehat{\chi}_1$	1	1	1
$\widehat{\chi}_2$	1	-1	1
$\widehat{\chi}_4$	2	0	-1

we can see that G/N is a group of order 6 and it is not abelian. Hence $G/N \cong S_3$. (See the character table of S_3 in the Example 5.2.1)

Note: *If $N \trianglelefteq G$, then the character table of G determines whether or not G/N is abelian. There is no way to determine from the character table of G whether or not N is abelian.*

Corollary 5.23 *Let $g \in G$ and $N \trianglelefteq G$. Then $|C_G(g)| \geq |C_{G/N}(gN)|$.*

Proof: We know that

$$\begin{aligned}
Irr(G/N) &= \{\widehat{\chi} \mid \chi \in Irr(G),\ N \subseteq \ker(\chi)\}. \\
|C_{G/N}(gN)| &= \sum_{\widehat{\chi} \in Irr(G/N)} \widehat{\chi}(gN) \cdot \widehat{\chi}(gN)^{-1} \\
&= \sum_{\widehat{\chi} \in Irr(G/N)} \widehat{\chi}(gN) \cdot \overline{\widehat{\chi}(gN)} = \sum_{\widehat{\chi} \in Irr(G/N)} |\widehat{\chi}(gN)|^2 \\
&= \sum \{|\chi(g)|^2 \mid \chi \in Irr(G),\ N \subseteq \ker(\chi)\} \\
&\leq \sum_{\chi \in Irr(G)} |\chi(g)|^2 = |C_G(g)|.
\end{aligned}$$

■

6 Group Actions and Permutation Characters

Suppose that G is a finite group acting on a finite set Ω. For $\alpha \in \Omega$, the *stabilizer* of α in G is given by

$$G_\alpha = \{g \in G | \alpha^g = \alpha\}.$$

Then $G_\alpha \leq G$ and $[G : G_\alpha] = |\Delta|$, where Δ is the orbit containing α.

The action of G on Ω gives a permutation representation π with corresponding permutation character χ_π denoted by $\chi(G|\Omega)$. Then from elementary representation theory we deduce that

Lemma 6.1 *(i) The action of G on Ω is isomorphic to the action of G on the G/G_α, that is on the set of all left cosets of G_α in G. Hence $\chi(G|\Omega) = \chi(G|G_\alpha)$.*

(ii) $\chi(G|\Omega) = (I_{G_\alpha})^G$, the trivial character of G_α induced to G.

(iii) For all $g \in G$, we have $\chi(G|\Omega)(g) =$ number of points in Ω fixed by g.

Proof: For example see Isaacs [12] or Ali [1]. ■

In fact for any subgroup $H \leq G$ we have

$$\chi(G|H)(g) = \sum_{i=1}^{k} \frac{|C_G(g)|}{|C_H(h_i)|},$$

where $h_1, h_2, ..., h_k$ are representatives of the conjugacy classes of H that fuse to $[g] = C_g$ in G.

Lemma 6.2 *Let H be a subgroup of G and let Ω be the set of all conjugates of H in G. Then we have*

(i) $G_H = N_G(H)$ and $\chi(G|\Omega) = \chi(G|N_G(H)$.

(ii) For any g in G, the number of conjugates of H in G containing g is given by

$$\chi(G|\Omega)(g) = \sum_{i=1}^{m} \frac{|C_G(g)|}{|C_{N_G(H)}(x_i)|} = [N_G(H) : H]^{-1} \sum_{i=1}^{k} \frac{|C_G(g)|}{|C_H(h_i)|},$$

where x_i's and h_i's are representatives of the conjugacy classes of $N_G(H)$ and H that fuse to $[g] = C_g$ in G, respectively.

Proof:

(i)

$$G_H = \{x \in G | H^x = H\} = \{x \in G | x \in N_G(H)\} = N_G(H).$$

Now the results follows from Lemma 6.1 part (i).

(ii) The proof follows from part (i) and Corollary 3.1.3 of Ganief [11] which uses a result of Finkelstien [9]. ■

Remark 6.1 *Note that*

$$\chi(G|\Omega)(g) = |\{H^x : (H^x)^g = H^x\}| = |\{H^x | H^{x^{-1}gx} = H\} =$$

$$|\{H^x | x^{-1}gx \in N_G(H)\}| = |\{H^x | g \in xN_G(H)x^{-1}\}| = |\{H^x | g \in (N_G(H))^x\}|.$$

Corollary 6.3 *If G is a finite simple group and M is a maximal subgroup of G, then number λ of conjugates of M in G containing g is given by*

$$\chi(G|M)(g) = \sum_{i=1}^{k} \frac{|C_G(g)|}{|C_M(x_i)|},$$

where $x_1, x_2, ..., x_k$ are representatives of the conjugacy classes of M that fuse to the class $[g] = C_g$ in G.

Proof: It follows from Lemma 6.2 and the fact that $N_G(M) = M$. It is also a direct application of Remark 1, since

$$\chi(G|\Omega)(g) = |\{M^x | g \in (N_G(M))^x\}| = |\{M^x | g \in M^x\}|. \blacksquare$$

Let B be a subset of Ω. If $B^g = B$ or $B^g \cap B = \varnothing$ for all $g \in G$, we say B is a **block** for G. Clearly $\varnothing, \Omega$ and $\{\alpha\}$ for all $\alpha \in \Omega$ are blocks, called **trivial blocks**. Any other block is called **non-trivial**. If G is transitive on Ω such that G has no non-trivial block on Ω, then we say G is **primitive**. Otherwise we say G is **imprimitive**.

Remark 6.2 *Classification of Finite Simple Groups (CFSG) implies that no 6-transitive finite groups exist other than S_n $(n \geq 6)$ and A_n $(n \geq 8)$, and that the Mathieu groups are the only faithful permutation groups other than S_n and A_n providing examples for 4- and 5-transitive groups.*

Remark 6.3 *It is well-known that every 2-transitive group is primitive. By using CFSG, all finite 2-transitive groups are known.*

The following is a well-known theorem that gives a characterisation of primitive permutation groups. Since by Lemma 6.1 the permutation action of a group G on a set Ω is equivalent to the action of G on the set of the left cosets G/G_α, determination of the primitive actions of G reduces to the classification of its maximal subgroups.

Theorem 6.4 *Let G be transitive permutation group on a set Ω. Then G is primitive if and only if G_α is a maximal subgroup of G for every $\alpha \in \Omega$.*

Proof: See Rotman [37]. ■

7 Designs

An incidence structure $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ consists of two disjoint sets $\mathcal{P}$ (called points) and $\mathcal{B}$ (called blocks), and $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$. If $(p, B) \in \mathcal{I}$, then we say that the point p is incident with the block B. The pair (p, B) is called a **flag**. If $(p, B) \notin \mathcal{I}$, then it is an **anti-flag**.

Example 7.1 Let $\mathcal{P}$ be any set and $\mathcal{B} \subseteq 2^{\mathcal{P}}$, where $2^{\mathcal{P}}$ is the set of all subsets of $\mathcal{P}$ (power set). Let $\mathcal{I} = \{(p, B) : p \in \mathcal{P}, B \in \mathcal{B}, p \in B\}$. Then we have an incidence structure $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$.

For example let $\mathcal{P} = \{1, 2, 3\}, \mathcal{B} = \{\{1\}, \{1, 2\}, \{2, 3\}\}$. Then

$$\mathcal{I} = \{(1, \{1\}), (1, \{1, 2\}), (2, \{1, 2\}), (2, \{2, 3\}), (3, \{2, 3\})\}.$$

We have three points and three blocks. Note that in this case $\mathcal{I} \subsetneqq \mathcal{P} \times \mathcal{B}$.

Definition 7.1 (t-Design) *An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{I}$ is a t-(v, k, λ) design, if $|\mathcal{P}| = v$, every block $B \in \mathcal{B}$ is incident with precisely k points, and every t distinct points are together incident with precisely λ blocks.*

We will say that a design $\mathcal{D}$ is **symmetric** if it has the same number of points and blocks. A $t - (v, k, 1)$ design is called a **Steiner System**. A $2 - (v, 3, 1)$ Steiner system is called a **Steiner Triple System**.

A $t - (v, 2, \lambda)$ design $\mathcal{D}$ can be regarded as a graph with $\mathcal{P}$ as points and $\mathcal{B}$ as edges.

Example 7.2 . Consider Example 7.1, where $\mathcal{P} = \{1, 2, 3\}, \mathcal{B} = \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$, and $(p, B) \in \mathcal{I}$ if and only if $p \in B$. Then the design $\mathcal{D}$ is a $1 - (3, 2, 2)$ design, which is also a $2 - (3, 2, 1)$ design. It is also symmetric.

Exercise 7.1 Let $\mathcal{P} = \{1, 2, 3\}$. Consider Example 7.1 and find two more t-designs.

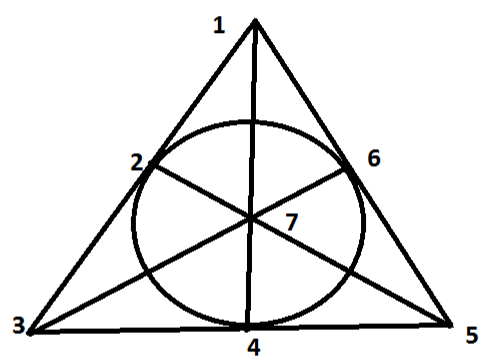
Remark 7.1 A Steiner system $2-(n^2+n+1, n+1, 1)$ is called a **Projective Plane** of order n. A Steiner system $2-(n^2, n, 1)$ is called an **Affine Plane** of order n. Projective and affine planes of order $n = p^k$, where p is a prime, exist. But the question is: **Is there a finte plane of order n when n is not a prime?** The conjecture is that the answer is NO, but so far has not been proven. It can be shown that a projective plane of order n exist if and only if there exits an affine plane of order n.

Bruck-Ryser Theorem (1949)[6] states that: if $n = 4k+1$ or $4k+2$ and n is not equal to the sum of two squares of integers, then there is no projective plane of order n.

Note that 10 is not a prime, $10 = 4 \times 2 + 2$, but $10 = 3^2 + 1^2$. So we cannot use Bruck-Ryser Theorem to show the nonexistence of a finite plane of order 10. The non-existence was proved (using computers) by Lam in 1991 (see [27]) after two decades of search for a solution to the problem.

The next smallest number to look at is 12. We do not yet know whether there exists a finite plane of order 12.

Figure 1: Fano Plane



Example 7.3 *Fano Plane .* The **Fano plane** is a projective plane of order 2, which is a $2-(7,3,1)$ design (a Stiener triple system on 7 points).

In the Figure 1 we have $\mathcal{P} = \{1,2,3,4,5,6,7\}$, $\mathcal{B} = \{B_1, B_2, B_3, B_4, B_5, B_6, B_7\}$, where $B_1 = \{1,2,3\}$,$B_2 = \{1,5,6\}$, $B_3 = \{1,4,7\}$, $B_4 = \{2,4,6\}$, $B_5 = \{2,5,7\}$, $B_6 = \{3,6,7\}$ and $B_7 = \{3,4,5\}$.

We can see that the Fano plane is a symmetric 2-design. Also note that it is a $1-(7,3,3)$ design.

Remark 7.2 (Counting Principles) *In combinatorics often we need to count the number of elements of a set S in two different ways and then equate our* *answers. So in general assume that X and Y are two finite sets and $S \subseteq X \times Y$. We define*

$$S(a,\ ) = \{(x,y) : (x,y) \in S, x = a\},\ \ S(\ ,b) = \{(x,y) : (x,y) \in S, y = b\}.$$

Then

$$S = \dot{\bigcup} S(a,\ ) = \dot{\bigcup} S(\ ,b).$$

Hence we have

$$|S| = \sum_{a \in X} |S(a,\ )| = \sum_{b \in Y} |S(\ ,b)|,$$

and if $|S(a,\ )| = l$ and $|S(\ ,b)| = m$ are independent of a and b respectively, then we have

$$l|X| = m|Y|.$$

We use the Counting Priciple described above (see Remark 7.2 to prove the following theorem on t-designs.

Theorem 7.1 *If $\mathcal{D}$ is a $t-(v,k,\lambda)$ design and $1 \leq s \leq t$, then $\mathcal{D}$ is also a $s-(v,k,\lambda_s)$ design where*

$$\lambda_s = \frac{(v-s)(v-s-1)\cdots(v-t+1)}{(k-s)(k-s-1)\cdots(k-t+1)}.$$

Proof: Let S be a set of s points and let m be the number of blocks that contain S. Let

$$\mathcal{T} = \{(T,B) : S \subset T \subset B, |T| = t, B \in \mathcal{B}\}.$$

Now count the number of elements of $\mathcal{T}$ in two different way, we have

$$\lambda\left(\begin{array}{c} v-s \\ t-s \end{array}\right) = m\left(\begin{array}{c} k-s \\ t-s \end{array}\right).$$

We can see that m is independet of S and hence

$$\lambda_s = m = \lambda\left(\begin{array}{c} v-s \\ t-s \end{array}\right)/\left(\begin{array}{c} k-s \\ t-s \end{array}\right),$$

which gives the formula. ■

Note that Fano Plane is a 2-(7,3,1) design. Here $\lambda = \lambda_t = \lambda_2 = 1$, and hence $\lambda_1 = 1 \times \frac{7-1}{3-1} = 3$. We deduce that Fano plane is also a $1-(7,3,3)$ design.

Remark 7.3

1. *$\lambda_t = \lambda$ and $\lambda_s = \frac{v-s}{k-s} \times \lambda_{s+1}$.*
2. *If the number of blocks in a $t-$design $\mathcal{D}$ is denoted by b, then we have*

$$b = \lambda_0 = \frac{v(v-1)\cdots(v-t+1)}{k(k-1)\cdots(k-t+1)}.$$

If we denote λ_1 (replication number) by r, then we have

$$r = \lambda_1 = \frac{(v-1)(v-2)\cdots(v-t+1)}{(k-1)(k-2)\cdots(k-t+1)}.$$

Thus we get

$$b = \frac{v}{k} r$$

and hence we deduce that

$$bk = vr.$$

3. *In a 2-design* $2-(v,k,\lambda)$*, we have* $\lambda_2 = \lambda$ *and by part (1) we get*

$$\lambda_1 = \frac{v-1}{k-1} \times \lambda_2,$$

and hence

$$\lambda_1(k-1) = \lambda(v-1)$$

so that

$$r(k-1) = \lambda(v-1).$$

Definition 7.2 (Incidence Matrix) *Let* $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ *be a design in which* $\mathcal{P} = \{p_1, p_2, \cdots, p_v\}$ *and* $\mathcal{B} = \{B_1, B_2, \cdots, B_b\}$*. Then the* incidence matrix *of* $\mathcal{D}$ *is defined to be a* $b \times v$ *matrix* $A = (a_{ij})$ *such that*

$$a_{ij} = \begin{cases} 1 & if\ (p_j, B_i) \in \mathcal{I} \\ 0 & if\ (p_j, B_i) \notin \mathcal{I} \end{cases}$$

Theorem 7.2 *Let* $\mathcal{D}$ *is a* $2-(v,k,\lambda)$ *design with* A *as its incidence matrix. If* I_v *is the* $v \times v$ *identity matrix and* J_v *is the* $v \times v$ *matrix with all entries equal to 1, then we have*

$$A^t A = (r-\lambda) I_v + \lambda J_v,$$

and

$$det(A^t A) = (r-\lambda)^{v-1}(v\lambda - \lambda + r) = (r-v)^{v-1} rk.$$

Proof: Easy to see that $(A^t A)_{ij} = \sum a_{ki} a_{kj}$, which is equal to the inner product of ith column of A with jth column of A. If $i = j$ then this number is r and if $i \neq j$ it is λ. Hence

$$A^t A = \begin{pmatrix} r & \lambda & \cdots & \lambda \\ \lambda & r & \cdots & \lambda \\ \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \cdots & r \end{pmatrix} = (r-\lambda) I_v + \lambda J_v.$$

Subtract the first column from each other column, and then add each row to the first row. We get a lower triangular matrix with diagonal entries $r + (v-1)\lambda, r - \lambda, r - \lambda, \cdots, r - \lambda$. Thus

$$det(A^t A) = (r-\lambda)^{v-1}(v\lambda - \lambda + r)$$

and since by Remark 3 (3) $v\lambda - \lambda = r(k-1)$, we have

$$det(A^t A) = (r-\lambda)^{v-1}(r(k-1) + r) = (r-\lambda)^{v-1} rk.$$

■

In a t-design $\mathcal{D}$, where $t \geq 2$, the **order** of $\mathcal{D}$ is defined to be $n = \lambda_1 - \lambda_2$. So if $t = 2$, then $n = r - \lambda$ and

$$det(A^t A) = (r - \lambda)^{v-1} rk = n^{v-1} rk.$$

Since by Theorem 7.1 any t-design with $t \geq 2$ is also a 2-design, Theorem 7.2 is true for any t-design with $t \geq 2$.

Corollary 7.3 *If $\mathcal{D}$ is a none-trivial 2-design with an incedence matrix A, then $rank(A)$ over $\mathbb{Q}$ is v.*

Proof: $A^t A$ is an square $v \times v$ matrix and since $\mathcal{D}$ is non-trivial, $v - k \neq 0$ so that $r - \lambda \neq 0$, (because in a 2-design we have $r(k-1) = \lambda(v-1)$). Thus $0 \neq det(A^t A) = (det(A))^2$, which implies that $det(A) \neq 0$. Therefore $rank_{\mathbb{Q}}(A) = v$. ■

Example 7.4 (Incidence Matrix of Fano Plane) Consider the Example 7.3. If we let M be the incidence matrix of the Fano plane, then we have that

$$M = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}.$$

Since Fano plane is a non-trivial 2-design, by Theorem 7.2 we have that $rank_{\mathbb{Q}}(M) = 7$ and $det_{\mathbb{Q}}(M) = 24$. Why?

Exercise 7.2 If M is the incidence matrix of the Fano plane show that

i. $rank_F(M) = 7$, where F is a field of characteristic p with $p \notin \{2, 3\}$.

ii. $rank_F(M) = 4$, where $char(F) = 2$;

iii. $rank_F(M) = 6$, where $char(F) = 3$.

Corollary 7.4 *If $\mathcal{D}$ is a $t-design$ with $t \geq 2$, then $b \geq v$, that is the number of blocks is at least same as the number of points.*

Proof: Since $\mathcal{D}$ is a non-trivial 2-design, $rank_{\mathbb{Q}}(A) = v$. Now since A is a $b \times v$ matrix, its rank must be less than or equal to number of its row, that is we have $v = rank_{\mathbb{Q}}(A) \leq b$. ■

Definition 7.3 *An **isomorphim** between two designs $\mathcal{D}_1$ and $\mathcal{D}_2$ is a bijection ϕ between sets of points $\mathcal{P}_1$ and $\mathcal{P}_2$ and between sets of blocks $\mathcal{B}_1$ and $\mathcal{B}_2$ such that for any $p \in \mathcal{P}_1$ and $B \in \mathcal{B}_1$, $p\mathcal{I}_1 B$ implies that $\phi(p)\mathcal{I}_2\phi(B)$. If $\mathcal{D}_1 = \mathcal{D}_2$, then ϕ is called an **automorphism** (or a collineation). The group of automorphisms of a design $\mathcal{D}$ is denoted by $Aut(\mathcal{D})$.*

Example 7.5 If $\mathcal{D}$ is the 2-design describing the Fano plane (see Example 7.3), then

$$G = Aut(\mathcal{D}) =< (5\ \ 6)(7\ \ 4), (1\ \ 2)(6\ \ 7), (5\ \ 7)(1\ \ 3), (1\ \ 4\ \ 5\ \ 7\ \ 3\ \ 2\ \ 6) > .$$

The group G is 2-transitive on points with

$$|G| = 7 \times 6 \times |G_{12}| = 168,$$

where

$$G_{12} = \{e, (5\ \ 6)(7\ \ 4), (5\ \ 7)(4\ \ 6), (5\ \ 4)(6\ \ 7)\} \cong V_4$$

Also note that $G_1 \cong S_4$ and $G \cong PSL(2,7) \cong PSL(3,2)$.

Definition 7.4 *i. The* **complement** *of $\mathcal{D}$ is the structure $\tilde{\mathcal{D}} = (\mathcal{P}, \mathcal{B}, \tilde{\mathcal{I}})$, where $\tilde{\mathcal{I}} = \mathcal{P} \times \mathcal{B} - \mathcal{I}$. If $\mathcal{D}$ is a $t-(v,k,\lambda)$ design, then $\tilde{\mathcal{D}}$ is a $t-(v, v-k, \tilde{\lambda})$ design.*

ii. The **dual** *structure of $\mathcal{D}$ is $\mathcal{D}^t = (\mathcal{B}, \mathcal{P}, \mathcal{I}^t)$, where $(B,P) \in \mathcal{I}^t$ if and only if $(P,B) \in \mathcal{I}$. Thus the transpose of an incidence matrix for $\mathcal{D}$ is an incidence matrix for $\mathcal{D}^t$. We say $\mathcal{D}$ is* **self dual** *if it is isomorphic to its dual.*

iii. A t-(v,k,λ) design is called **self-orthogonal** *if the block intersection numbers have the same parity as the block size.*

Exercise 7.3 Show that the complement of the Fano plane is a $2-(7,4,2)$ design. If $\tilde{M}$ *is the incedence matrix of this complement, show that* $det(\tilde{M}) = 2^{10}$. *If F is a field of characteristic 2, show that* $rank_F(\tilde{M}) = 3$.

8 Codes

Definition 8.1 *Let F be a finite set of q elements. A* ***q-ary code*** *C is a set of code words $(x_1, x_2, \ldots, x_n), x_i \in F, n \in \mathbb{N}$. If all code words have same length n, then we say that C is a block code of length n. In this case $C \subseteq F^n$.*

Definition 8.2 (Hamming distance) *If $w = (w_1, w_2, \ldots, w_n)$ and $v = (v_1, v_2, \ldots, v_n)$ are in F^n, we define the Hamming distance $d(v,w)$ by*

$$d(v,w) = |\{i : v_i \neq w_i\}\|.$$

For example in F^4, where $F = GF(3)$, if $v = (1,1,2,0)$ and $w = (0,1,2,3)$. then $d(v,w) = 2$. The following properties of Hamming distance are easy to prove:

1. $d(v,w)$= 0 if and only if $v = w$;
2. $d(v,w) = d(w,v)$, for all $v, w \in F$;
3. $d(u,w) \leq d(u,v) + d(v,w)$, for all $u, v, w \in F$.

Definition 8.3 (Minimum Distance) *If C is a code we define the* ***minimum distance*** *$d(C)$ by*

$$d(C) = min\{d(v,w) : v, w \in C, v \neq w\}.$$

The following results plays an important role in detecting and correcting errors when codes are transmitted via **symmetric q-ary channels**.

Theorem 8.1 *Let C be a code with minimum distance d.*

i. If $d \geq s+1 \geq 2$, then C can be used to detect up to s errors.

ii. if $d \geq 2t+1$, then C can be used to correct up to t errors.

Proof: i. Suppose v is transmitted and w received with less than or equal s errors. Then $d(v,w) \leq s \leq d-1 < d$ and hence $w \notin C$ or $w = v$. Thus if we had errors, it would be detected.

ii. Suppose v is transmitted and w received with less than or equal t errors. Then we have $d(v,w) \leq t$. Now suppose that $u \in C$ such that $u \neq v$, then we have

$$d(u,w) + d(w,v) \geq d(u,v) \geq d \geq 2t+1,$$

and hence

$$d(u,w) \geq 2t+1-d(v,w) \geq 2t+1-t = t+1.$$

Thus v is the closest codeword to w in C and it could be picked. ■

Corollary 8.2 *If $d = d(C)$, then C can detect at most $d-1$ errors and correct at most $\lfloor \frac{d-1}{2} \rfloor$ errors.*

Proof: Folows from Theorem 8.1. ■

Theorem 8.3 (Singleton Bound) *Let C be a q-ary code of length n and mininmum distance d. Then $|C| \leq q^{n-d+1}$.*

Proof: We know that $C \subseteq F^n$ and hence clearly $|C| \leq q^n$. Let C' be the set of all code words of C that their last $d-1$ co-ordinates are removed. Then clearly $|C| = |C'|$, since all elements of C' are distinct due to the fact that no two code words of C differed in less than d places. Now each cowords in C' has length $n-d+1$ and hence

$$|C| = |C'| \leq q^{n-d+1},$$

and thus the result. ■

8.1 Linear Codes

From now on we regard F as a finite field $F_q = GF(q)$ and our codes C to be subspaces of $V = F^n$. If $dim(C) = k$ and $d(C) = d$, then the code C is denoted by $[n,k,d]_q$ to represent this information.

Definition 8.4 (Support and Minimum Weight) *Let $V = F^n$, $v = (x_1, x_2, x_3 \ldots, x_n) \in V$ and $S = \{i : v_i \neq 0\}$. Then S is called the* **support** *of v (denoted by supp (v)), the $|S|$ is said to be the* **weight** *of v (denoted by wt (v)) If C is a linear code, the* **minimum weight** *of C is $min\{wt(c) : c \in C\}$.*

Proposition 8.4 *Let $C = [n,k,d]$. Then we have* *i.* $d = d(C)$ *is the minimum weight of* C,

ii. $d \leq n - k + 1$.

Proof:

i. Clearly in $V = F^n$ we have $d(v, w) = wt(v - w)$. Now since C is a subspace of V, for any $v, w \in C$ we have $v - w \in C$ and hence the result.

ii. Since C is a subspace of V with $dim(C) = k$, we have $|C| = q^k$ and now by Theorem 8.3 we have $q^k \leq q^{n-d+1}$. Hence $k \leq n-d+1$, so that $d \leq n-k+1$.

■

A **constant word** in a code is a codeword that is a scalar multiple of vector all of whose coordinate entries are either 0 or 1.

The all-one vector will be denoted by $\jmath$, and is the constant vector of weight the length of the code.

Two linear codes of the same length and over the same field are **equivalent** if each can be obtained from the other by permuting the coordinate positions and multiplying each coordinate position by a non-zero field element.

They are **isomorphic** if they can be obtained from one another by permuting the coordinate positions.

An **automorphism** of a code is any permutation of the coordinate positions that maps codewords to codewords. An automorphism thus preserves each weight class of C.

A binary code with all weights divisible by 4 is said to be a **doubly-even** binary code.

Definition 8.5 (Dual of a Code) *For any code* C*, the* **dual** *code* $C^{\perp}$ *is the orthogonal subspace under the standard inner product. That is*

$$C^{\perp} = \{v \in F^n : < v, c >= 0 \text{ for all } c \in C\}.$$

If $C \subseteq C^{\perp}$*, then we say* C *is* **self-orthogonal**. *If* $C = C^{\perp}$*, then we say that* C *is* **self-dual**. *The* **hull** *of* C *is given by* $Hull(C) = C \cap C^{\perp}$.

Definition 8.6 (Generating Matrix) . *If* C *is a* q*-ary code of dimension* k *and of length* n*, then a generating matrix* G *for* C *is a* $k \times n$ *matrix obtained from any basis of* C.

By performing elementary row operations on G, we can reduce it into a row echelon form $G' = [I_k|A]$ (**standard form**), where A is a $k \times (n - k)$ matrix. Clearly G' is a generating matrix for a code which is equivalent (and isomorphic) to C.

Proposition 8.5 *If* C *is a* $[n, k]$ *code, then* $C^{\perp}$ *is a* $[n, n - k]$ *code.*

Proof: Let G be a generating matrix for C. Then $(v)G^t \in F^k$ for all $v \in F^n$ and G^t can be regarded as a linear transformation from F^n onto F^k. Clearly $ker(G^t) = C^{\perp}$ and hence $F^n/C^{\perp} \cong F^k$, that is $dim(F^n) - dim(C^{\perp}) = dim(F^k)$. Hence $n = dim(C) + dim(C^{\perp})$. ■

Exercise 8.1 Let $C =< \jmath >$ be the code generated by all one vector $\jmath$ inside F^n.

1. What is the standard form for C?
2. Show that $C^{\perp}$ is a $[n, n-1, 2]$ code.
3. Show that $C^{\perp}$ is generated by the vectors with exactly 2 non-zero entries 1 and -1.
4. Show that the standard form for $C^{\perp}$ is $[I_{n-1}|B]$, where B is the column matrix with -1 entries.

Definition 8.7 (Parity Check Matrix) *If C is a code, then any generating matrix for $C^{\perp}$ is said to be a* **parity-check** *matrix for C.*

Proposition 8.6 *If G and H are generating and parity-check matrices of a code C, then we have $GH^t = 0_{k\times(n-k)}$ and $c \in C$ if and only if cH^t=0 if and only if $Hc^t = 0$.*
Proof: *Follows from the fact that C and $C^{\perp}$ are orthogonal and H is a generating matrix for $C^{\perp}$.* ■

Note that if $G = [I_k|A]$ is a generating matrix for a code C of dimension k in F^n, then $H = [-A^t|I_{n-k}]$ is a parity-check matrix for C. A generating matrix in its standard form simplifies the encoding. For example if we encode $u \in F^k$ by $G = [I_k|A]$, we compute uG and we will get $v = (u_1, u_2, \dots, u_k, x_{k+1}, x_{k+2} \dots, x_n)$, where $u = (u_1, u_2, \dots, u_k)$.

Exercise 8.2 The smallest Hamming code is a binary code $[7, 4, 3]$, which is a single error correcting code. It has the following generating matrix (in standard form): $G = [I_4|A]$ where

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

Find a parity-check matrix for it.

8.2 Codes from Designs

The code C_F of the design $\mathcal{D}$ over the finite field F is the space spanned by the incidence vectors of the blocks over F. If we take F to be a prime field $F_p = GF(p)$, in which case we write also C_p for C_F, and refer to the dimension of C_p as the **p-rank** of $\mathcal{D}$. If the point set of $\mathcal{D}$ is denoted by $\mathcal{P}$ and the block set by $\mathcal{B}$, and if $\mathcal{Q}$ is any subset of $\mathcal{P}$, then we will denote the incidence vector of $\mathcal{Q}$ by $v^{\mathcal{Q}}$. Thus $C_F = \langle v^B \,|\, B \in \mathcal{B} \rangle$, and is a subspace of $F^{\mathcal{P}}$, the full vector space of functions from $\mathcal{P}$ to F.

Example 8.1 Let $\mathcal{D}$ be the 2-design representing the Fano plane. Then using the Exercise 7.2 we can easily see that

i. If F is a field of characteristic p with $p \notin \{2, 3\}$, then $C_F(\mathcal{D}) = F^7$ with $Aut(C) \cong S_7$.

ii. $C_2(\mathcal{D}) = [7,4,3]_2$ (the smallest hamming code) with $Aut(C) \cong PGL(3,2) \cong PSL(2,7) \cong PSL(3,2)$, the simple group of order 168.

iii. $C_3(\mathcal{D}) =< \jmath >^{\perp} = [7,6,2]_3$, with $Aut(C) \cong S_7$.

Terminology for graphs is standard: our graphs are undirected, the **valency** of a vertex is the number of edges containing the vertex. A graph is **regular** if all the vertices have the same valence, and a regular graph is **strongly regular** of type (n,k,λ,μ) if it has n vertices, valence k, and if any two adjacent vertices are together adjacent to λ vertices, while any two non-adjacent vertices are together adjacent to μ vertices.

9 Method 1

Construction of 1-Designs and Codes from Maximal Subgroups: In this section we consider primitive representations of a finite group G. Let G be a finite primitive permutation group acting on the set Ω of size n. We can consider the action of G on $\Omega \times \Omega$ given by $(\alpha,\beta)^g = (\alpha^g,\beta^g)$ for all $\alpha,\beta \in \Omega$ and all $g \in G$. An orbit of G on $\Omega \times \Omega$ is called an **orbital**. If $\bar{\Delta}$ is an orbital, then $\bar{\Delta}^* = \{(\alpha,\beta) : (\beta,\alpha) \in \bar{\Delta}\}$ is also an orbital of G on $\Omega \times \Omega$, which is called the **paired orbital** of $\bar{\Delta}$. We say that $\bar{\Delta}$ is **self-paired** if $\bar{\Delta} = \bar{\Delta}^*$.

Now Let $\alpha \in \Omega$, and let $\Delta \neq \{\alpha\}$ be an orbit of the stabilizer $M = G_\alpha$ of α. It is not difficult to see that $\bar{\Delta}$ given by $\bar{\Delta} = \{(\alpha,\delta)^g : \delta \in \Delta, g \in G\}$ is an orbital. We say that Δ is self-paired if and only if $\bar{\Delta}$ is a self paired orbital. Also note that the primitivity of G on Ω implies that M is a maximal subgroup of G.

If $M = G_\alpha$ has only three orbits $\{\alpha\}$, Δ and Δ' on Ω, then we say that G is a rank-3 permutation group.

Our construction for the symmetric 1-designs is based on the following results, mainly Theorem 9.1 below, which is the Proposition 1 of [18] with its corrected version in [19]:

Theorem 9.1 *Let G be a finite primitive permutation group acting on the set Ω of size n. Let $\alpha \in \Omega$, and let $\Delta \neq \{\alpha\}$ be an orbit of the stabilizer G_α of α. If*

$$\mathcal{B} = \{\Delta^g : \ g \in G\}$$

and, given $\delta \in \Delta$,

$$\mathcal{E} = \{\{\alpha,\delta\}^g \ : \ g \in G\},$$

then $\mathcal{D} = (\Omega,\mathcal{B})$ forms a 1-$(n,|\Delta|,|\Delta|)$ design with n blocks. Further, if Δ is a self-paired orbit of G_α, then $\Gamma = (\Omega,\mathcal{E})$ is a regular connected graph of valency $|\Delta|$, $\mathcal{D}$ is self-dual, and G acts as an automorphism group on each of these structures, primitive on vertices of the graph, and on points and blocks of the design.

Proof: We have $|G| = |\Delta^G||G_\Delta|$, and clearly $G_\Delta \supseteq G_\alpha$. Since G is primitive on Ω, G_α is maximal in G, and thus $G_\Delta = G_\alpha$, and $|\Delta^G| = |\mathcal{B}| = n$. This proves that we have a 1-$(n,|\Delta|,|\Delta|)$ design.

Since Δ is self-paired, Γ is a graph rather than only a digraph. In Γ we notice that the vertices adjacent to α are the vertices in Δ. Now as we orbit these pairs under G, we get the nk ordered pairs, and thus $nk/2$ edges, where $k = \Delta$. Since the graph has G acting, it is clearly regular, and thus the valency is k as required, i.e. the only vertices adjacent to α are those in the orbit Δ. The graph must be connected, as a maximal connected component will form a block of imprimitivity, contradicting the group's primitive action.

Now notice that an adjacency matrix for the graph is simply an incidence matrix for the 1-design, so that the 1-design is necessarily self-dual. This proves all our assertions. ■

Note that if we form any union of orbits of the stabilizer of a point, including the orbit consisting of the single point, and orbit this under the full group, we will still get a self-dual symmetric 1-design with the group operating. Thus the orbits of the stabilizer can be regarded as "building blocks". Since the complementary design (i.e. taking the complements of the blocks to be the new blocks) will have exactly the same properties, we will assume that our block size is at most $v/2$.

In fact this will give us all possible designs on which the group acts primitively on points and blocks:

Lemma 9.2 *If the group G acts primitively on the points and the blocks of a symmetric 1-design $\mathcal{D}$, then the design can be obtained by orbiting a union of orbits of a point-stabilizer, as described in Theorem 9.1.*

Proof: Suppose that G acts primitively on points and blocks of the 1-(v, k, k) design $\mathcal{D}$. Let $\mathcal{B}$ be the block set of $\mathcal{D}$; then if B is any block of $\mathcal{D}$, $\mathcal{B} = B^G$. Thus $|G| = |\mathcal{B}||G_B|$, and since G is primitive, G_B is maximal and thus $G_B = G_\alpha$ for some point. Thus G_α fixes B, so this must be a union of orbits of G_α. ■

Lemma 9.3 *If G is a primitive simple group acting on Ω, then for any $\alpha \in \Omega$, the point stabilizer G_α has only one orbit of length 1.*

Proof: Suppose that G_α fixes also β. Then $G_\alpha = G_\beta$. Since G is transitive, there exists $g \in G$ such that $\alpha^g = \beta$. Then $(G_\alpha)^g = G_{\alpha^g} = G_\beta = G_\alpha$, and thus $g \in N_G(G_\alpha) = N$, the normalizer of G_α in G. Since G_α is maximal in G, we have $N = G$ or $N = G_\alpha$. But G is simple, so we must have $N = G_\alpha$, so that $g \in G_\alpha$ and so $\beta = \alpha$. ■

We have considered various finite simple groups, for example J_1; J_2; M^cL; $PSp_{2m}(q)$, where q is a power of an odd prime, and $m \geq 2$; Co_2; HS and Ru. For each group, using Magma [4], we construct designs and graphs that have the group acting primitively on points as automorphism group, and, for a selection of small primes, codes over that prime field derived from the designs or graphs that also have the group acting as automorphism group. For each code, the code automorphism group at least contains the associated group G.

To aid in the classification, if possible, the dimension of the hull of the design for each of these primes were found. Then we took a closer look at some of the more interesting codes that arose, asking what the basic coding properties were, and if the full automorphism group could be established.

It is well known, and easy to see, that if the group is rank-3, then the graph formed as described in Theorem 9.1 will be strongly regular. In case the group is not of rank 3, this might still happen, and we examined this question also for some of the groups we studied.

A sample of our results for example for J_1 and J_2 is given below, but the full set can be obtained at Jenny Key's web site under the file "Janko groups and designs":

`http://www.ces.clemson.edu/~keyj`

Clearly the automorphism group of any of the codes will contain the automorphism group of the design from which it is formed. We looked at some of the codes that were computationally feasible to find out if the groups J_1 and $\bar{J}_2$ formed the full automorphism group in any of the cases when the code was not the full vector space. We first mention the following lemma:

Lemma 9.4 *Let C be the linear code of length n of an incidence structure $\mathcal{I}$ over a field F. Then the automorphism group of C is the full symmetric group if and only if $C = F^n$ or $C = F\boldsymbol{\jmath}^{\perp}$.*

Proof: Suppose $\mathrm{Aut}(C)$ is S_n. C is spanned by the incidence vectors of the blocks of $\mathcal{I}$; let B be such a block and suppose it has k points, and so it gives a vector of weight k in C. Clearly C contains the incidence vector of any set of k points, and thus, by taking the difference of two such vectors that differ in just two places, we see that C contains all the vectors of weight 2 having as non-zero entries 1 and -1. Thus $C = F\boldsymbol{\jmath}^{\perp}$ or F^n. The converse is clear.■

Huffman [15] has more on codes and groups, and in particular, on the possibility of the use of permutation decoding for codes with large groups acting. See also Knapp and Schmid [26] for more on codes with prescribed groups acting.

Most of the codes we looked at were too large to find the automorphism group, but we did find some of, through computation with Magma. Note that we could in some cases look for the full group of the hull, and from that deduce the group of the code, since $\mathrm{Aut}(C) = \mathrm{Aut}(C^{\perp}) \subseteq \mathrm{Aut}(C \cap C^{\perp})$.

9.1 J_1, J_2 and Co_2

In this subsection we give a brief discussion on the application of Method 1 (discussed in Section 9) to the sporadic simple groups J_1, J_2 and Co_2. For full details the readers are referred to [18], [19], [20] and [32].

9.1.1 Computations for J_1 and J_2

The first Janko sporadic simple group J_1 has order $175560 = 2^3 \times 3 \times 5 \times 7 \times 11 \times 19$ and it has seven distinct primitive representations, of degree 266, 1045, 1463, 1540, 1596, 2926, and 4180, respectively (see Table 1 and [5, 10]). For each of the seven primitive representations, using Magma, we constructed the permutation group and formed the orbits of the stabilizer of a point. For each of the non-trivial orbits, we formed the symmetric 1-design as described in Theorem 9.1. We took set of the $\{2, 3, 5, 7, 11\}$ of primes and found the dimension of the code and its hull for each of these primes. Note also that since 19 is a divisor of the order of J_1, in some of the smaller cases it is worthwhile also to look at codes over the field of order 19. We also found the automorphism group of each design, which will be the same as the automorphism group of the regular graph. Where computationally possible we also found the automorphism group of the code.

Conclusions from our results are summarized below. In brief, we found that there are 245 designs formed in this manner from single orbits and that none of them is isomorphic to any other of the designs in this set. In every case the full automorphism group of the design or graph is J_1.

No.	Order	Index	Structure
Max[1]	660	266	$PSL(2,11)$
Max[2]	168	1045	2^3:7:3
Max[3]	120	1463	$2 \times A_5$
Max[4]	114	1540	19:6
Max[5]	110	1596	11:10
Max[6]	60	2926	$D_6 \times D_{10}$
Max[7]	42	4180	7:6

Table 1: Maximal subgroups of J_1

In Table 2, the first column gives the degree, the second the number of orbits, and the remaining columns give the length of the orbits of length greater than 1, with the number of that length in parenthesis behind the length in case there is more than one of that length. The pairs that had the same code dimensions occurred as follows: for degrees 266, 1045 and 1596, there were no such pairs; for degree 1463 there were two pairs, both for orbit size 60; for degree 1540, there were two pairs, for orbit size 57 and 114 respectively; for degree 2926 there was one pair for orbit size 60; for degree 4180 there were 12 pairs, for orbit size 42.

In summary then, we have the following:

Proposition 9.5 *If G is the first Janko group J_1, there are precisely* 245 *non-isomorphic self-dual* 1*-designs obtained by taking all the images under G of the non-trivial orbits of the point stabilizer in any of G's primitive representations, and on which G acts primitively on points and blocks. In each case the full automorphism group is J_1. Every primitive action on symmetric 1-designs can be*

Degree	#	length				
266	5	132	110	12	11	
1045	11	168(5)	56(3)	28	8	
1463	22	120(7)	60(9)	20(2)	15(2)	12
1540	21	114(9)	57(6)	38(4)	19	
1596	19	110(13)	55(2)	22(2)	11	
2926	67	60(34)	30(27)	15(5)		
4180	107	42(95)	21(6)	14(4)	7	

Table 2: Orbits of a point-stabilizer of J_1

obtained by taking the union of such orbits and orbiting under G.

We tested the graphs for strong regularity in the cases of the smaller degree, and did not find any that were strongly regular. We also found the designs and their codes for some of the unions of orbits in some cases. We found that some of the codes were the same for some primes, but not for all.

The second Janko sporadic simple group J_2 has order has order $604800 = 2^7 \times 3^3 \times 5^2 \times 7$, and it has nine primitive permutation representations (see Table 3), but we did not compute with the largest degree. Thus our results cover only the first eight. Our results for J_2 are different from those for J_1, due to the existence of an outer automorphism. The main difference is that usually the full automorphism group is $\bar{J}_2$, and that in the cases where it was only J_2, there would be another orbit of that length that would give an isomorphic design, and which, if the two orbits were joined, would give a design of double the block size and automorphism group $\bar{J}_2$. A similar conclusion held if some union of orbits was taken as a base block.

No.	Order	Index	Structure
Max[1]	6048	100	$PSU(3,3)$
Max[2]	2160	280	$3{\cdot}PGL(2,9)$
Max[3]	1920	315	$2^{1+4}{:}A_5$
Max[4]	1152	525	$2^{2+4}{:}(3 \times S_3)$
Max[5]	720	840	$A_4 \times A_5$
Max[6]	600	1008	$A_5 \times D_{10}$
Max[7]	336	1800	$PSL(2,7){:}2$
Max[8]	300	2016	$5^2{:}D_{12}$
Max[9]	60	10080	A_5

Table 3: Maximal subgroups of J_2

From these eight primitive representations, we obtained in all 51 non-isomorphic symmetric designs on which J_2 acts primitively. Table 4 gives the same information for J_2 that Table 2 gives for J_1. The automorphism group of the design in

Degree	#	length						
100	3	63	36					
280	4	135	108	36				
315	6	160	80	32(2)	10			
525	6	192(2)	96	32	12			
840	7	360	240	180	24	20	15	
1008	11	300	150(2)	100(2)	60(2)	50	25	12
1800	18	336	168(6)	84(3)	42(3)	28	21	14(2)
2016	18	300(2)	150(6)	75(5)	50(2)	25	15	

Table 4: Orbits of a point-stabilizer of J_2 (of degree ≤ 2016)

each case was J_2 or $\bar{J}_2$. Where J_2 was the full group, there is another copy of the design for another orbit of the same length. This occurred in the following cases: degree 315, orbit length 32; degree 1008, orbit lengths 60, 100 and 150; degree 1800, orbit lengths 42, 42, 84 and 168; degree 2016, orbit lengths 50, 75, 75, 150, 150, and 300. We note again that the p-ranks of the design and their hulls gave an initial indication of possible isomorphisms and clear non-isomorphisms, so that only the few mentioned needed be tested. This reduced the computations tremendously.

We also found three strongly regular graphs (all of which are known: see Brouwer [7]): that of degree 100 from the rank-3 action, of course, and two more of degree 280 from the orbits of length 135 and 36, giving strongly regular graphs with parameters (280,135,70,60) and (280,36,8,4) respectively. The full automorphism group is $\bar{J}_2$ in each case. We have not checked all the other representations but note that this is the only one with point stabilizer having exactly four orbits. Note that Bagchi [3] found a strongly regular graph with J_2 acting.

In each of the following we consider the primitive action of J_2 on a design formed as described in Method 1 from an orbit or a union of orbits, and the codes are the codes of the associated 1-design.

1. For J_2 of degree 100, $\bar{J}_2$ is the full automorphism group of the design with parameters 1-$(100, 36, 36)$, and it is the automorphism group of the self-orthogonal doubly-even $[100, 36, 16]_2$ binary code of this design.

2. For J_2 of degree 280, $\bar{J}_2$ is the full automorphism group of the design with parameters 1-$(280, 108, 108)$, and it is the automorphism group of the self-orthogonal doubly-even $[280, 14, 108]_2$ binary code of this design. The weight distribution of this code is

```
 <0, 1>, <108, 280>, <128, 1575>, <136, 2520>, <140, 7632>,
<144, 2520>, <152, 1575>, <172, 280>, <280, 1>
```

   Thus the words of minimum weight (i.e. 108) are the incidence vectors of the design.

3. For J_2 of degree 315, $\bar{J}_2$ is the full automorphism group of the design with parameters 1-$(315, 64, 64)$ (by taking the union of the two orbits of length 32), and it is the automorphism group of the self orthogonal doubly-even $[315, 28, 64]_2$ binary code of this design. The weight distribution of the code is as follows:

```
<0, 1>,<64, 315>,<96, 6300>,<104, 25200>,<112, 53280>, <120,
242760>,<124, 201600>,<128, 875700>,<132, 1733760>, <136,
4158000>,<140, 5973120>,<144, 12626880>,<148, 24232320>, <152,
35151480>,<156, 44392320>,<160, 53040582>, <164, 41731200>,<168,
28065120>,<172, 13023360>,<176, 2129400>, <180, 685440>,<184,
75600>,<192, 10710>,<200, 1008>
```

   Thus the words of minimum weight (i.e. 64) are the incidence vectors of the blocks of the design.

Furthermore, the designs from the two orbits of length 32 in this case, i.e. 1-$(315, 32, 32)$ designs, each have J_2 as their automorphism group. Their binary codes are equal, and are $[315, 188]_2$ codes, with hull the 28-dimensional code described above. The automorphism group of this 188-dimensional code is again $\bar{J}_2$. The minimum weight is at most 32. This is also the binary code of the design from the orbit of length 160.

4. For J_2 of degree 315, $\bar{J}_2$ is the full automorphism group of the design with parameters 1-$(315, 160, 160)$ and it is the automorphism group of the $[315, 265]_5$ 5-ary code of this design. This code is also the 5-ary code of the design obtained from the orbit of length 10, and from that of the orbit of length 80, so we can deduce that the minimum weight is at most 10. The hull is a $[315, 15, 155]_5$ code and again with $\bar{J}_2$ as full automorphism group.

5. For J_2 of degree 315, $\bar{J}_2$ is the full automorphism group of the design with parameters 1-$(315, 80, 80)$ from the orbit of length 80, and it is the automorphism group of the self-orthogonal doubly-even $[315, 36, 80]_2$ binary code of this design. The minimum words of this code are precisely the 315 incidence vectors of the blocks of the design.

In [20] we used the construction described in Method 1 to obtain all irreducible modules of J_1 (as codes) over the prime fields $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5$. We also showed that most of those of J_2 can be represented in this way as the code, the dual code or the hull of the code of a design, or of codimension 1 in one of these. For J_2, if no such code was found for a particular irreducible module, then we checked that it could not be so represented for the relevant degrees of the primitive permutation representations up to and including 1008. In summary, we obtained:

Proposition 9.6 *Using the construction described in Method 1 above (see Theorem 9.1 and Lemma 9.2), taking unions of orbits, the following constructions of the irreducible modules of the Janko groups J_1 and J_2 as the code, the dual code or the hull of the code of a design, or of codimension 1 in one of these, over $\mathbb{F}_p$ where $p = 2, 3, 5$, were found to be possible:*

1. *J_1: all the seven irreducible modules for $p = 2, 3, 5$;*

2. *J_2: all for $p = 2$ apart from dimensions $12, 128$; all for $p = 3$ apart from dimensions $26, 42, 114, 378$; all for $p = 5$ apart from dimensions $21, 70, 189, 300$. For these exclusions, none exist of degree ≤ 1008.*

Note: 1. We do not claim that we have all the constructions of the modular representations as codes; we were seeking mainly existence.

We give below three self-orthogonal binary codes of dimension 20 invariant under J_1 of lengths 1045, 1463, and 1540. These are irreducible by [16] or Magma data. In all cases the Magma *simgps* library is used for J_1 and J_2.

1. **J_1 of Degree 1045**
   $[1045, 20, 456]_2$ code; dual code: $[1045, 1025, 4]_2$

```
\\Orbit lengths of stabilizer of a point:
[ 1, 8, 28, 56, 56, 56, 168, 168, 168, 168, 168 ];
\\Orbits chosen: ##1,3,5,10,11
\\Defining block is the union of these, length 421
1-(1045, 421, 421) Design with 1045 blocks
\\C is the code of the design, of dimension 21
\\The 20-dimensional code is Ch:= C meet Dual(C) =Hull(C)
> WeightDistribution(Ch);
[ <0, 1>, <456, 3080>, <488, 29260>, <496, 87780>, <504, 87780>,
<512, 36575>, <520, 299706>, <528, 234080>, <536, 175560>, <544,
58520>, <552, 14630>, <560, 19019>, <608, 1540>, <624, 1045> ].
Those of weight 456, 504, 544, 552, 624, 608 are single orbits; the
others split.
>WeightDistribution(C);
 [ <0, 1>, <421,1405>, <437, 1540>, <456, 3080>, <485,19019>,
 <488, 29260>, <493, 14630>, < 496, 87780>, <501, 58520>,
<504, 87780>, <509, 175560>, <512, 36575>, <517, 234080>, <520,
299706>, <525, 299706>, <528, 234080>, <533, 36575>, <536, 175560>,
<541, 87780>, <544, 58520>, <549, 87780>, <552, 14630>, <557,29260>,
<560, 19019>, <589, 3080>, <608, 1540>, <624, 1045>, <1045, 1> ].
```

2. **J_1 of Degree 1463**
$[1463, 20, 608]_2$ code; dual code: $[1463, 1443, 3]_2$

```
\\Orbit lengths of stabilizer of a point:
[ 1, 12, 15, 15, 20, 20, 60, 60, 60, 60, 60, 60, 60, 60, 120,
120, 120, 120, 120, 120, 120 ]
\\Orbits chosen ##18,21
\\Defining block is union of these, of length 240
1-(1463, 240, 240) Design with 1463 blocks
\\C is the code of the design, of dimension 492
\\The 20-dimensional code is Ch:= C meet Dual(C) =Hull(C)
 WD(Ch);
[ <0, 1>, <608, 1540>, <632, 2926>, <640, 7315>, <688, 29260>, <696,
29260>, <712, 87780>, <720, 89243>, <728, 311410>, <736, 87780>,
<744, 175560>, <752, 222376>, <760, 3080>, <784, 1045> ]
```

3. **J_1 of Degree 1540**
$[1540, 20, 640]_2$ code; dual code: $[1540, 1520, 4]_2$

```
\\Orbit lengths of stabilizer of a point:
[ 1, 19, 38, 38, 38, 38, 57, 57, 57, 57, 57, 57, 114, 114, 114, 114,
114, 114, 114, 114, 114 ]
\\Orbits chosen ##7,13
\\Defining block is the union of these, length 171
1-(1540, 171, 171) Design with 1540 blocks
\\C is the code of the design, of dimension 592
\\The code of dimension 20 is Ch:=C meet Dual(C)
WD(Ch); [ <0, 1>, <640, 1463>, <728, 33440>, <736, 58520>, <760,
311696>, <768, 358435>, <792, 175560>, <800, 105336>, <856, 3080>,
<896, 1045> ]
```

We now look at the smallest representations for J_2. We have not been able to find any of dimension 12, and none can exist for degree ≤ 1008, as we have verified computationally by examining the permutation modules. We give below four representations of J_2 acting on self-orthogonal binary codes of small degree that are irreducible or indecomposable codes over J_2. The full automorphism group of each of these codes is $\bar{J}_2$.

1. **J_2 of Degree 100, dimension 36**
   $[100, 36, 16]_2$ code; dual code: $[100, 64, 8]_2$

```
\\Orbit lengths of stabilizer of a point:
[1, 36, 63] 1-(100, 36, 36) Design with 100 blocks
\\ Orbit #2 gave a block of the design
[ <0, 1>, <16, 1575>, <24, 105000>, <28, 1213400>, <32, 29115450>,
<36, 429677200>, <40, 2994639480>, <44, 10672216200>, <48,
20240374350>, <52, 20217640800>, <56, 10675819800>, <60,
3004193640>, <64, 422248725>, <68, 30819600>, <72, 1398600>, <76,
12600>, <80, 315> ]
```

   This code $C = C_{36}$ of dimension 36 is irreducible, by Magma. The dual code $C_{64} = C^{\perp}$ has an invariant subcode C_{63} of dimension 63 that is spanned by the weight-8 vectors and that contains $\jmath$ and C_{36}. All these codes are indecomposable, by Magma. The full automorphism group of this code is $\bar{J}_2$.

2. **J_2 of Degree 280, dimension 13**
   $[280, 13, 128]_2$ code; dual code: $[280, 267, 4]_2$

```
\\Orbit lengths of stabilizer of a point:
[1, 36, 108, 135]
\\Orbit #3 gave a block of the design
1-(280,108,108) Design with 280 blocks
\\Weight distribution of its 14-dimensional binary code
[ <0, 1>, <108, 280>, <128, 1575>, <136, 2520>, <140, 7632>, <144,
2520>, <152, 1575>, <172, 280>, <280, 1> ] Dual code: [280,266,4]
\\Weight distribution of reducible but indecomposable 13-dimensional code
[ <0, 1>, <128, 1575>, <136, 2520>, <144, 2520>, <152, 1575>, <280,
1> ]
```

   This code has the invariant subcode of dimension 1 generated by the all-one vector, so it is reducible. However, we checked the orbits of all the other words and found that there are no other invariant subcodes. It is thus indecomposable. The full automorphism group of these codes is $\bar{J}_2$.

3. **J_2 of Degree 315, dimension 28**
   $[315, 28, 64]_2$ code; dual code: $[315, 287, 3]_2$

```
\\Orbit lengths of stabilizer of a point:
[ 1, 10, 32, 32, 80, 160 ]
```

```
\\Orbits ## 3 and 4 chosen
1-(315, 64, 64) Design with 315 blocks
\\Weight distribution of its 28-dimensional binary code
[ <0, 1>, <64, 315>, <96, 6300>, <104, 25200>, <112, 53280>, <120,
242760>, <124, 201600>, <128, 875700>, <132, 1733760>, <136,
4158000>, <140, 5973120>, <144, 12626880>, <148, 24232320>, <152,
35151480>, <156, 44392320>, <160, 53040582>, <164, 41731200>, <168,
28065120>, <172, 13023360>, <176, 2129400>, <180, 685440>, <184,
75600>, <192, 10710>, <200, 1008> ]
```

The code is an irreducible module over J_2, by Magma. The full automorphism group of this code is $\bar{J}_2$.

4. **J_2 of Degree 315, dimension 36**
$[315, 36, 80]_2$ code; dual code: $[315, 279, 5]_2$

```
\\Orbit lengths of stabilizer of a point:
[ 1, 10, 32, 32, 80, 160 ]
\\chose the orbit of length 80
1-(315, 80, 80) Design with 315 blocks 36 =Dim(C) dim hull 36
//Weight distribution of the 36-dimensional code
[ <0, 1>, <80, 315>, <84, 1800>, <96, 9450>, <100, 50400>, <108,
126000>, <112, 84150>, <116, 466200>, <120, 4798920>, <124,
10987200>, <128, 54432000>, <132, 180736920>, <136, 606475800>,
<140, 1792977480>, <144, 3988438335>, <148, 6923044800>, <152,
10151396640>, <156, 12278475300>, <160, 11844516600>, <164,
9314451720>, <168, 6136980600>, <172, 3360636720>, <176,
1436425200>, <180, 459183200>, <184, 132924960>, <188, 32715900>,
<192, 7006125>, <196, 1800000>, <200, 126000>, <204, 113400>, <208,
75600>, <216, 12600>, <220, 6300>, <252, 100> ]
```

The code is an irreducible module over J_2, by Magma. The full automorphism group of this code is $\bar{J}_2$.

For F one of the fields $\mathbb{F}_p$ for $p = 2, 3, 5$ and n the degree of the permutation representation, in [20] we demonstrated some cases where the full space F^n can be completely decomposed into G-modules, where $G = J_1, J_2$, using codes obtained by our construction. In all cases C_m denotes an indecomposable linear code of dimension m over the relevant field and group. If the codes were irreducible they were obtained according to our method and were listed in [20]. For example

- For J_1 of degree 1045 over F_2, the full space can be completely decomposed into J_1-modules, that is:

$$\mathbb{F}_2^{1045} = C_{76} \oplus C_{112} \oplus C_{360} \oplus C_{496} \oplus \mathbb{F}_2\boldsymbol{\jmath},$$

  where all but C_{496} are irreducible. C_{496} has composition factors of dimensions 20, 112, 1, 76, 20, 1, 112, 20, 1, 1, 112, 20. Also

$$S = Socle(\mathbb{F}_2^{1045}) = \mathbb{F}_2\boldsymbol{\jmath} \oplus C_{20} \oplus C_{76} \oplus C_{112} \oplus C_{360},$$

  with $dim(S) = 569$.

- For J_2 of degree 315 over $\mathbb{F}_2$ we have:

$$F_2^{315} = C_{160} \oplus C_{154} \oplus \mathbb{F}_2\boldsymbol{\jmath},$$

where C_{160} is irreducible and $C_{154} \oplus \mathbb{F}_2\boldsymbol{\jmath} = C_{160}^{\perp}$ is the binary code of the 1-$(315, 33, 33)$ design from orbits #1 and #4. (Note that $\mathbb{F}_2^{100}$ and $\mathbb{F}_2^{280}$ are indecomposable as J_2 modules.)

- For J_2 of degree 100 over $\mathbb{F}_3$ we have:

$$F_3^{100} = C_{36} \oplus C_{63} \oplus \mathbb{F}_3\boldsymbol{\jmath}.$$

- For J_2 of degree 280 over $\mathbb{F}_3$ we have:

$$F_3^{280} = C_{63} \oplus C_{216} \oplus \mathbb{F}_3\boldsymbol{\jmath},$$

where C_{216} is the code of the 1-$(280, 135, 135)$ design obtained from the orbit # 4.

- for J_2 of degree 525 over $\mathbb{F}_5$ we have:

$$F_5^{525} = C_{175} \oplus C_{100} \oplus C_{250},$$

where C_{175} is irreducible and C_{100} is the dual of the code C of the 1-$(525, 140, 140)$ design obtained from the orbits #2, #3 , #4, and $C_{250} = C \cap C_{175}^{\perp}$.

9.1.2 The Conway group Co_2

The Leech lattice is a certain 24-dimensional $\mathbb{Z}$ submodule of the Euclidean space $\mathbb{R}^{24}$ whose automorphism group is the double cover $2{}^{\cdot}\mathrm{Co}_1$ of the Conway group Co_1. The Conway groups Co_2 and Co_3 are stabilizers of sublattices of the Leech lattice.

The subgroup structure of Co_2 is discussed in Wilson [40] and [39] using the following information. The group Co_2 admits a 23-dimensional *indecomposable* representation over $GF(2)$ obtained from the 24-dimensional Leech lattice by reducing modulo 2 and factoring out a fixed vector. The action of Co_2 on the vectors of this 23-dimensional indecomposable $GF(2)$ module (say M) produces eight orbits, with stabilizers isomorphic to Co_2, $U_6(2){:}2$, $2^{10}{:}M_{22}{:}2$, M^cL, $HS{:}2$, $U_4(3).D_8$, $2_+^{1+8}{:}S_8$ and M_{23}, respectively. The 23-dimensional indecomposable $GF(2)$ module M contains an irreducible $GF(2)$-submodule N of dimension 22. We use TABLE III(a) given by Wilson in [39] to produce Table 5, which gives the orbit lengths and stabilizers for the actions of Co_2 on M and N respectively.

On the other hand, reduction modulo 2 of the 23-dimensional ordinary irreducible representation results in a *decomposable* 23-dimensional $GF(2)$ representation. In [40] Wilson showed that Co_2 has exactly eleven conjugacy classes of maximal subgroups. One of these subgroups is the group $U_6(2){:}2$ of index 2300. In Proposition 9.7, using this maximal subgroup, we construct the decomposable 23-dimensional $GF(2)$-representation as the binary code C_{892} of dimension 23 invariant under the action of Co_2. The action of Co_2 on C_{892} produces 12 orbits

M-Stabilizer	M-Orbit length	N-Stabilizer	N-Orbit length
Co_2	1	Co_2	1
$U_6(2):2$	2300	$U_6(2):2$	2300
M^cL	47104		
2^{10}:M_{22}:2	46575	2^{10}:M_{22}:2	46575
HS:2	476928	HS:2	476928
$U_4(3).D_8$	1619200	$U_4(3).D_8$	1619200
M_{23}	4147200		
2_+^{1+8}:S_8	2049300	2_+^{1+8}:S_8	2049300

Table 5: Action of Co_2 on M and N

with stabilizers isomorphic to Co$_2$ (2 copies), $U_6(2)$:2 (2 copies), 2^{10}:M_{22}:2 (2 copies), HS:2 (2 copies), $U_4(3).D_8$ (2 copies), 2_+^{1+8} : S_8 (2 copies) respectively. Furthermore, C_{892} contains a binary code C_{1408} of dimension 22 invariant and irreducible under the action of Co$_2$. Notice that the 2-modular character table of Co$_2$ is completely known (see [36]) and follows from it that the irreducible 22-dimensional $GF(2)$ representation is unique and 22 is the smallest dimension for any non-trivial irreducible $GF(2)$ module.

Here we examine some designs $\mathcal{D}_i$ and associated binary codes C_i constructed from a primitive permutation representation of degree 2300 of the sporadic simple group Co$_2$. For the full detail the readers are encouraged to see [32].

We used Method 1 and constructed self-dual symmetric 1-designs $\mathcal{D}_i$ and binary codes C_i, where i is an element of the set $\{891, 892, 1408, 1409, 2299\}$, from the rank-3 primitive permutation representation of degree 2300 of the sporadic simple group Co$_2$ of Conway. The stabilizer of a point α in this representation is a maximal subgroup isomorphic to $U_6(2)$:2, producing orbits $\{\alpha\}$, Δ_1, Δ_2 of lengths 1, 891 and 1408 respectively.

The self-dual symmetric 1-designs $\mathcal{D}_i$ are constructed from the sets Δ_1, $\{\alpha\} \cup \Delta_1$, Δ_2, $\{\alpha\} \cup \Delta_2$, and $\Delta_1 \cup \Delta_2$, respectively. We let $\Omega = \{\alpha\} \cup \Delta_1 \cup \Delta_2$.

We proved the following result:

Proposition 9.7 *Let G be the Conway group* Co$_2$ *and $\mathcal{D}_i$ and C_i where i is in the set* $\{891, 892, 1408, 1409, 2299\}$ *be the designs and binary codes constructed from the primitive rank-3 permutation action of G on the cosets of* $U_6(2)$:2. *Then the following holds:*

(i) $\mathrm{Aut}(\mathcal{D}_{891}) = \mathrm{Aut}(\mathcal{D}_{892}) = \mathrm{Aut}(\mathcal{D}_{1408}) = \mathrm{Aut}(\mathcal{D}_{1409}) = \mathrm{Aut}(C_{892}) = \mathrm{Aut}(C_{1408}) = \mathrm{Co}_2$.

(ii) $dim(C_{892}) = 23$, $dim(C_{1408}) = 22$, $C_{892} \supset C_{1408}$ and Co$_2$ *acts irreducibly on C_{1408}.*

(iii) $C_{891} = C_{1409} = C_{2299} = V_{2300}(GF(2))$.

(iv) $\mathrm{Aut}(\mathcal{D}_{2299}) = \mathrm{Aut}(C_{891}) = \mathrm{Aut}(C_{1049}) = \mathrm{Aut}(C_{2299}) = S_{2300}$.

The proof of the proposition follows from a series of lemmas. In fact we showed that the codes C_{892} and C_{1408} are of types $[2300, 23, 892]_2$ and $[2300, 22, 1024]_2$ respectively. Furthermore

$$C_{892} = \langle C_{1408}, \jmath \rangle = C_{1408} \cup \{w + \jmath : w \in C_{1408}\}$$
$$= C_{1408} \oplus \langle \jmath \rangle,$$

where $\jmath$ denotes the all-one vector. Let W_l denote the set of all codewords of C_{892} of weight l and let A_l be the size of W_l. Then clearly $W_l + \{\jmath\} = W_{2300-l} \subset C_{892}$ and $|W_l| = A_l = |W_{2300-l}| = A_{2300-l}$. We found the weight distribution of C_{892} and then the weight distribution of C_{1408} follows. We also determined the structures of the stabilizers $(\mathrm{Co}_2)_{w_l}$, for all nonzero weight l, where $w_l \in C_{1408}$ is a codeword of weight l. The structures of the stabilizers $(\mathrm{Co}_2)_{w_l}$ for C_{892} follows clearly from those of C_{1408}.

We also showed that the code C_{1408} is the 22 dimensional irreducible representation of Co_2 over $GF(2)$ contained in the 23-dimensional decomposable C_{892}. It is also contained in the 23-dimensional indecomposable representation of Co_2 over $GF(2)$ discussed in 𝔸𝕋𝕃𝔸𝕊 [5] and Wilson [39].

We should also mention that computation with Magma shows the codes over some other primes, in particular, $p = 3$ are of some interest. In a separate paper we plan to deal with the ternary codes invariant under Co_2 [35].

10 Method 2

Construction of 1-Designs and Codes from Maximal Subgroups and Conjugacy Classes of Elements: In this section we assume G is a finite simple group, M is a maximal subgroup of G, nX is a conjugacy class of elements of order n in G and $g \in nX$. Thus $C_g = [g] = nX$ and $|nX| = |G : C_G(g)|$.

As in Section 6 let $\chi_M = \chi(G|M)$ be the permutation character afforded by the action of G on Ω, the set of all conjugates of M in G. Clearly if g is not conjugate to any element in M, then $\chi_M(g) = 0$.

The construction of our 1-designs is based on the following theorem.

Theorem 10.1 *Let G be a finite simple group, M a maximal subgroup of G and nX a conjugacy class of elements of order n in G such that $M \cap nX \neq \emptyset$. Let $\mathcal{B} = \{(M \cap nX)^y | y \in G\}$ and $\mathcal{P} = nX$. Then we have a $1-(|nX|, |M \cap nX|, \chi_M(g))$ design $\mathcal{D}$, where $g \in nX$. The group G acts as an automorphism group on $\mathcal{D}$, primitive on blocks and transitive (not necessarily primitive) on points of $\mathcal{D}$.*

Proof: First note that

$$\mathcal{B} = \{M^y \cap nX | y \in G\}.$$

We claim that $M^y \cap nX = M \cap nX$ if and only if $y \in M$ or $nX = \{1_G\}$. Clearly if $y \in M$ or $nX = \{1_G\}$, then $M^y \cap nX = M \cap nX$. Conversely suppose there exits $y \notin M$ such that $M^y \cap nX = M \cap nX$. Then maximality of M in G implies that $G =< M, y >$ and hence $M^z \cap nX = M \cap nX$ for all $z \in G$. We can deduce that $nX \subseteq M$ and hence $< nX > \leq M$. Since $< nX >$ is a normal subgroup of G and G is simple, we must have $< nX >= \{1_G\}$. Note that maximality of M and the fact $< nX > \leq M$, excludes the case $< nX >= G$.

From above we deduce that

$$b = |\mathcal{B}| = |\Omega| = [G : M].$$

If $B \in \mathcal{B}$, then

$$k = |B| = |M \cap nX| = \sum_{i=1}^{k} |[x_i]_M| = |M| \sum_{i=1}^{k} \frac{1}{|C_M(x_i)|},$$

where $x_1, x_2, ..., x_k$ are the representatives of the conjugacy classes of M that fuse to g.

Let $v = |\mathcal{P}| = |nX| = [G : C_G(g)]$. Form the design $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{I}$ given by $x\mathcal{I}B$ if and only if $x \in B$. Since the number of blocks containing an element x in $\mathcal{P}$ is $\lambda = \chi_M(x) = \chi_M(g)$, we have produced a $1-(v, k, \lambda)$ design $\mathcal{D}$, where $v = |nX|$, $k = |M \cap nX|$ and $\lambda = \chi_m(g)$.

The action of G on blocks arises from the action of G on Ω and hence the maximality of M in G implies the primitivity. The action of G on nX, that is on points, is equivalent to the action of G on the cosets of $C_G(g)$. So the action on points is primitive if and only if $C_G(g)$ is a maximal subgroup of G. ■

Remark 10.1 *Since in a $1-(v, k, \lambda)$ design $\mathcal{D}$ we have $kb = \lambda v$, we deduce that*

$$k = |M \cap nX| = \frac{\chi_M(g) \times |nX|}{[G : M]}.$$

Also note that $\tilde{\mathcal{D}}$, the complement of $\mathcal{D}$, is $1-(v, v-k, \tilde{\lambda})$ design, where $\tilde{\lambda} = \lambda \times \frac{v-k}{k}$.

Remark 10.2 *If $\lambda = 1$, then $\mathcal{D}$ is a $1-(|nX|, k, 1)$ design. Since nX is the disjoint union of b blocks each of size k, we have $Aut(\mathcal{D}) = S_k \wr S_b = (S_k)^b : S_b$. Clearly In this case for all p, we have $C = C_p(\mathcal{D}) = [|nX|, b, k]_p$, with* $\mathrm{Aut}(C) = \mathrm{Aut}(\mathcal{D})$.

Remark 10.3 *The designs $\mathcal{D}$ constructed by using Theorem 12 are not symmetric in general. In fact $\mathcal{D}$ is symmetric if and only if*

$$b = |\mathcal{B}| = v = |\mathcal{P}| \Leftrightarrow [G : M] = |nX| \Leftrightarrow [G : M] = [G : C_G(g)] \Leftrightarrow |M| = |C_G(g)|.$$

10.1 Some 1-designs and Codes from A_7

A_7 has five conjugacy classes of maximal subgroups, which are listed in Table 6. It has also 9 conjugacy classes of elements, some of which are listed in Table 7.

We apply the Theorem 10.1 to the above maximal subgroups and few conjugacy classes of elements of A_7 to construct several non-symmetric 1- designs. The corresponding binary codes are also constructed.

No.	Structure	Index	Order
Max[1]	A_6	7	360
Max[2]	$PSL_2(7)$	15	168
Max[3]	$PSL_2(7)$	15	168
Max[4]	S_5	21	120
Max[5]	$(A_4 \times 3)$:2	35	72

Table 6: Maximal subgroups of A_7

nX	$\|nX\|$	$C_G(g)$	Maximal Centralizer
$2A$	105	D_8: 3	No
$3A$	70	$A_4 \times 3 \cong (2^2 \times 3)$: 3	No
$3B$	280	3×3	No

Table 7: Some of the conjugacy classes of A_7

10.1.1 $G = A_7$, $M = A_6$ and $nX = 3A$

Let $G = A_7$, $M = A_6$ and $nX = 3A$. Then

$$b = [G : M] = 7, v = |3A| = 70, k = |M \cap 3A| = 40.$$

Also using the character table of A_7, we have $\chi_M = \chi_1 + \chi_2 = \underline{1a} + \underline{6a}$ and hence $\chi_M(g) = 1+3 = 4 = \lambda$, where $g \in 3A$. We produce a non-symmetric $1-(70, 40, 4)$ design $\mathcal{D}$. A_7 acts primitively on the 7 blocks. Since $C_{A_7}(g) = A_4 \times 3$ is not maximal in A_7 (sits in the maximal subgroup $(A_4 \times 3)$:2 with index two), A_7 acts imprimitively on the 70 points. The complement of $\mathcal{D}$, $\tilde{\mathcal{D}}$, is a $1-(70, 30, 3)$ design.

Computations with MAGMA [4] shows that the full automorphism group of $\mathcal{D}$ is

$$Aut(\mathcal{D}) \cong 2^{35}{:}S_7 \cong 2^5 \wr S_7,$$

with $|Aut(\mathcal{D})| = 2^{39}.3^2.5.7$. Construction using MAGMA shows that the binary code C of this design is a $[70, 6, 32]_2$ code. The code C is self-orthogonal with the weight distribution

$$< 0, 1 >, < 32, 35 >, < 40, 28 > .$$

Our group A_7 acts irreducibility on C.

If W_i denote the set of all words in C of weight i, then

$$C =< W_{32} >=< W_{40} >,$$

so C is generated by its minimum-weight codewords. The full automorphism group of C is $Aut(C) \cong 2^{35}{:}S_8$ with $|Aut(C)| = 2^{42}.3^2.5.7$, and we note that $Aut(C) \geq Aut(\mathcal{D})$ and that $Aut(\mathcal{D})$ is not a normal subgroup of $Aut(C)$.

Furthermore $C^{\perp}$ is a $[70, 64, 2]_2$ code and its weight distribution has been determined. Since the blocks of $\mathcal{D}$ are of even size 40, we have that $\jmath$ meets

l	$\lvert W_l\rvert$	$Aut(\mathcal{D})_{w_l}$
32	35	2^{35}:$(A_4 \times 3)$:2
40(1)	7	2^{35}:S_6
40(2)	21	2^{35}:$(S_5$:2)

Table 8: Stabilizer of a word w_l in $Aut(\mathcal{D})$

l	$\lvert W_l\rvert$	$Aut(\mathcal{D})_{w_l}$
32	35	2^{35}:$(S_4 \times S_4)$:2
40	28	2^{35}:$(S_6 \times 2)$

Table 9: Stabilizer of a word w_l in $Aut(C)$

evenly every vector of C and hence $\jmath \in C^{\perp}$. If $\bar{W}_i$ denote the set of all codewords in $C^{\perp}$ of weight i, then $|\bar{W}_2| = 35,$, $|\bar{W}_3| = 840$, $|\bar{W}_4| = 14035$ and

$$C^{\perp} =< \bar{W}_3 >, dim(< \bar{W}_2 >= 35, dim(< \bar{W}_4 >= 63.$$

Let e_{ij} denote the 2-cycle (i,j) in S_7, where $\{i,j\} = s(\bar{w}_2)$ is the support of a codeword $\bar{w}_2 \in \bar{W}_2$. Then $e_{ij}(\bar{w}_2) = \bar{w}_2$, and $< e_{ij} | \{i,j\} = s(\bar{w}_2), \bar{w}_2 \in \bar{W}_2 >= 2^{35}$.

Using MAGMA we can easily show that $V = F_2^{70}$ is decomposable into indecomposable G-modules of dimension 40 and 30. We also have $dim(\mathrm{Soc}(V) = 21$ and

$$\mathrm{Soc}(V) =< \jmath > \oplus C \oplus C_{14},$$

where C is our 6-dimensional code and C_{14} is an irreducible code of dimension 14.

The structures the stabilizers $Aut(\mathcal{D})_{w_l}$ and $Aut(C)_{w_l}$, where $l \in \{32, 40\}$ are listed in Table 8 and 9.

10.1.2 $G = A_7$, $M = A_6$ and $nX = 2A$

Let $G = A_7$, $M = A_6$ and $nX = 2A$. Then

$$b = [G : M] = 7, v = |2A| = 105, k = |M \cap 2A| = 45.$$

Also using the character table of A_7, we have $\chi_M = \chi_1 + \chi_2 = \underline{1a} + \underline{6a}$ and hence $\chi_M(g) = 1+2 = 3 = \lambda$, where $g \in 2A$. We produce a non-symmetric $1-(105, 45, 3)$ design $\mathcal{D}$. A_7 acts primitively on the 7 blocks. Since $C_{A_7}(g) = D_8 : 3$ is not maximal in A_7 (sits in the maximal subgroup $(A_4 \times 3)$:2 with index three), A_7 acts imprimitively on the 105 points. The complement of $\mathcal{D}$, $\tilde{\mathcal{D}}$, is a $1-(105, 60, 4)$ design.

The full automorphism group of $\mathcal{D}$ is

$$Aut(\mathcal{D}) \cong {S_3}^{35}{:}S_7 \cong {S_3}^5 \wr S_7,$$

with $|Aut(\mathcal{D})| = 2^{42}.3^{37}.5.7$.

Construction using MAGMA shows that the binary code C of this design is a $[105, 7, 45]_2$ code. The weight distribution of C is

$$< 0, 1 >, < 45, 28 >, < 48, 35 >, < 57, 35 >, < 60, 28 >, < 105, 1 > .$$

We also have that $Hull(C)$ is a $[105, 6, 48]$ code and has the following weight distribution:

$$< 0, 1 >, < 48, 35 >, < 60, 28 > .$$

Note that $C = Hull(C) \oplus < \boldsymbol{\jmath} >$, and that our group A_7 acts irreducibility on $Hull(C)$. Also note that this result together with the result obtained in 5.1.2 imply that the 6-dimensional irreducible representation of A_7 over $GF(2)$ could be represented by two non-isomorphic codes, namely $[105, 6, 48]_2$ and $[70, 6, 32]_2$ codes.

We also have

$$C =< W_{45} >=< W_{57} >,$$

so C is generated by its minimum-weight codewords. The full automorphism group of C is $Aut(C) = Aut(\mathcal{D})$ and its structure was given above in 5.2.1.

Using MAGMA we can easily show that $V = F_2^{105}$ is decomposable into indecomposable G-modules of dimension 1, 14, 20 and 70 (the first three are irreducible). We also have $dim(\text{Soc}(V) = 55$ and that

$$\text{Soc}(V) =< \boldsymbol{\jmath} > \oplus C_{14} \oplus C_{14} \oplus C_{20} \oplus Hull(C),$$

where $C = Hull(C) \oplus < \boldsymbol{\jmath} >$ is our 7-dimensional code and C_{14} and C_{20} are irreducible codes of dimension 14 and 20 respectively.

10.1.3 $G = A_7$, $M = S_5$ and $nX = 2A$: $1-(105, 25, 5)$ Design

Let $G = A_7$, $M = S_5$ and $nX = 2A$. Then

$$b = [G : M] = 21, v = |2A| = 105, k = |M \cap 2A| = 25.$$

Note that both conjugacy classes of involutions of S_5 fuses to $2A$. Also using the character table of A_7, we have $\chi_M = \chi_1 + \chi_2 + \chi_5 = \underline{1a} + \underline{6a} + \underline{14a}$ and hence $\chi_M(g) = 1 + 2 + 2 = 5 = \lambda$, where $g \in 2A$. We produce a non-symmetric $1-(105, 25, 5)$ design $\mathcal{D}$. A_7 acts primitively on the 21 blocks. Since $C_{A_7}(g) = D_8{:}3$ is not maximal in A_7 (sits in the maximal subgroup $(A_4 \times 3){:}2$ with index three), A_7 acts imprimitively on the 105 points. The complement of $\mathcal{D}$, $\tilde{\mathcal{D}}$, is a $1-(105, 80, 16)$ design.

10.1.4 $G = A_7$, $M = PSL_2(7)$ and $nX = 2A$: $1-(105, 21, 3)$ Design

Let $G = A_7$, $M = PSL_2(7)$ and $nX = 2A$. Then

$$b = [G : M] = 15, v = |2A| = 105, k = |M \cap 2A| = 21.$$

Also using the character table of A_7, we have $\chi_M = \chi_1 + \chi_6 = \underline{1a} + \underline{14b}$ and hence $\chi_M(g) = 1+2 = 3 = \lambda$, where $g \in 2A$. We produce a non-symmetric $1-(105, 21, 3)$

design $\mathcal{D}$. A_7 acts primitively on the 15 blocks. Since $C_{A_7}(g) = D_8 : 3$ is not maximal in A_7 (sits in the maximal subgroup $(A_4 \times 3)$:2 with index three), A_7 acts imprimitively on the 105 points. The complement of $\mathcal{D}$, $\tilde{\mathcal{D}}$, is a $1-(105, 84, 12)$ design.

10.1.5 $G = A_7$, $M = PSL_2(7)$ and $nX = 3B$: $1-(280, 56, 3)$ Design

Let $G = A_7$, $M = PSL_2(7)$ and $nX = 3B$. Then

$$b = [G : M] = 15, v = |3B| = 280, k = |M \cap 2A| = 56.$$

Also using the character table of A_7, we have $\chi_M = \chi_1 + \chi_6 = \underline{1a} + \underline{14b}$ and hence $\chi_M(g) = 1+2 = 3 = \lambda$, where $g \in 3B$. We produce a non-symmetric $1-(280, 56, 3)$ design $\mathcal{D}$. A_7 acts primitively on the 15 blocks. Since $C_{A_7}(g) = 3\times 3 \in Syl_3(A_7)$ is not maximal in A_7 (sits in the maximal subgroups A_6 and $(A_4 \times 3)$:2 with indices 40 and 8 respectively), A_7 acts imprimitively on the 280 points. The complement of $\mathcal{D}$, $\tilde{\mathcal{D}}$, is a $1-(280, 224, 12)$ design.

10.2 Design and codes from $PSL_2(q)$

The main aim of this section to develop a general approach to $G = PSL_2(q)$, where M is the maximal subgroup that is the stabilizer of a point in the natural action of degree $q+1$ on the set Ω. This is fully discussed in Subsection 5.2.1. We start this section by applying the results discussed for Method 1, particularly the Theorem 10.1, to all maximal subgroups and conjugacy classes of elements of $PSL_2(11)$ to construct 1- designs and their corresponding binary codes. These are itemized bellow after Tables 5 and 6. The group $PSL_2(11)$ has order $660 = 2^2 \times 3 \times 5 \times 11$, it has four conjugacy classes of maximal subgroups, which are listed in the table 10. It has also eight conjugacy classes of elements which we list in Table 11.

No.	Order	Index	Structure
Max[1]	55	12	$F_{55} = 11 : 5$
Max[2]	60	11	A_5
Max[3]	60	11	A_5
Max[4]	12	55	D_{12}

Table 10: Maximal subgroups of $PSL_2(11)$

Max[1]

$\underline{5A}$: $\mathcal{D} = 1-(132, 22, 2), b = 12$; $C = [132, 11, 22]_2$, $C^{\perp} = [132, 121, 2]_2$; $Aut(\mathcal{D}) = Aut(C) = 2^{66} : S_{12}$.

$\underline{5B}$: As for $5A$.

$\underline{11A}$: $\mathcal{D} = 1-(60, 5, 1), b = 12$; $C = [60, 12, 5]_2$, $C^{\perp} = [60, 48, 2]_2$; $Aut(\mathcal{D}) = Aut(C) = (S_5)^{12} : S_{12}$.

$\underline{11B}$: As for $11A$.

nX	$\|nX\|$	$C_G(g)$	Maximal Centralizer
$2A$	55	D_{12}	Yes
$3A$	110	$\mathbb{Z}_6$	No
$5A$	132	$\mathbb{Z}_5$	No
$5B$	132	$\mathbb{Z}_5$	No
$6A$	110	$\mathbb{Z}_6$	No
$11A$	60	$\mathbb{Z}_{11}$	No
$11B$	60	$\mathbb{Z}_{11}$	No

Table 11: Conjugacy classes of $PSL_2(11)$

Max[2]

$\underline{2A}$: $\mathcal{D} = 1-(55,15,3), b = 11$; $C = [55,11,15]_2,\ C^{\perp} = [55,44,4]_2$; $Aut(\mathcal{D}) = PSL_2(11), Aut(C) = PSL_2(11) : 2$.

$\underline{3A}$: $\mathcal{D} = 1-(110,20,2), b = 11$; $C = [110,10,20]_2,\ C^{\perp} = [110,100,2]_2$; $Aut(\mathcal{D}) = Aut(C) = 2^{55} : S_{11}$.

$\underline{5A}$: $\mathcal{D} = 1-(132,12,1), b = 11$; $C = [132,11,12]_2,\ C^{\perp} = [132,121,2]_2$; $Aut(\mathcal{D}) = Aut(C) = (S_{12})^{11} : S_{11}$.

$\underline{5B}$: As for $5A$.

Max[3]

As for Max[2].

Max[4]

$\underline{2A}$: $\mathcal{D} = 1-(55,7,7), b = 55$; $C = [55,35,4]_2,\ C^{\perp} = [55,20,10]_2$; $Aut(\mathcal{D}) = Aut(C) = PSL_2(11) : 2$.

$\underline{3A}$: $\mathcal{D} = 1-(110,2,1), b = 55$; $C = [110,55,2]_2,\ C^{\perp} = [110,55,2]_2$; $Aut(\mathcal{D}) = Aut(C) = 2^{55} : S_{55}$.

$\underline{6A}$: As for $3A$.

10.2.1 $G = PSL_2(q)$ of degree $q+1$, $M = G_1$

Let $G = PSL_2(q)$, let M be the stabilizer of a point in the natural action of degree $q+1$ on the set Ω. Let $M = G_1$. Then it is well known that G acts sharply 2-transitive on Ω and $M = F_q : F_q^* = F_q : \mathbb{Z}_{q-1}$, if q is even, and $M = F_q : \mathbb{Z}_{\frac{q-1}{2}}$, if q is odd. Since G acts 2-transitively on Ω, we have $\chi = 1 + \psi$ where χ is the permutation character of the action and ψ is an irreducible character of G of degree q. Also since the action is sharply 2-transitive, only 1_G fixes 3 distinct elements of Ω. Hence for all $1_G \neq g \in G$ we have $\lambda = \chi(g) \in \{0,1,2\}$.

Proposition 10.2 *For $G = PSL_2(q)$, let M be the stabilizer of a point in the natural action of degree $q+1$ on the set Ω. Let $M = G_1$. Suppose $g \in nX \subseteq G$ is an element fixing exactly one point, and without loss of generality, assume $g \in M$. Then the replication number for the associated design is $r = \lambda = 1$. We also have*

(i) *If q is odd then $|g^G| = \frac{1}{2}(q^2-1)$, $|M \cap g^G| = \frac{1}{2}(q-1)$, and $\mathcal{D}$ is a 1-$(\frac{1}{2}(q^2-1), \frac{1}{2}(q-1), 1)$ design with $q+1$ blocks and*

$$\mathrm{Aut}(\mathcal{D}) = S_{\frac{1}{2}(q-1)} \wr S_{q+1} = (S_{\frac{1}{2}(q-1)})^{q+1} : S_{q+1}.$$

For all p, $C = C_p(\mathcal{D}) = [\frac{1}{2}(q^2-1), q+1, \frac{1}{2}(q-1)]_p$, with $\mathrm{Aut}(C) = \mathrm{Aut}(\mathcal{D})$.

(ii) *If q is even then $|g^G| = (q^2-1)$, $|M \cap g^G| = (q-1)$, and $\mathcal{D}$ is a 1-$((q^2-1), (q-1), 1)$ design with $q+1$ blocks and*

$$\mathrm{Aut}(\mathcal{D}) = S_{(q-1)} \wr S_{q+1} = (S_{(q-1)})^{q+1} : S_{q+1}.$$

For all p, $C = C_p(\mathcal{D}) = [(q^2-1), q+1, q-1]_p$, with $\mathrm{Aut}(C) = \mathrm{Aut}(\mathcal{D})$.

Proof: Since $\chi(g) = 1$, we deduce that $\psi(g) = 0$. We now use the character table and conjugacy classes of $PSL_2(q)$ (for example see [14]):

(i) For q odd, there are two types of conjugacy classes with $\psi(g) = 0$. In both cases we have $|C_G(g)| = q$ and hence $|nX| = |g^G| = |PSL_2(q)|/q = (q^2-1)/2$. Since $b = [G : M] = q+1$ and

$$k = \frac{\chi(g) \times |nX|}{[G : M]} = \frac{1 \times (q^2-1)/2}{q+1} = (q-1)/2,$$

the results follow from Remark 10.2.

(ii) For q even, $PSL_2(q) = SL_2(q)$ and there is only one conjugacy class with $\psi(g) = 0$. A class representative is the matrix $g = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ with $|C_G(g)| = q$ and hence $|nX| = |g^G| = |PSL_2(q)|/q = (q^2-1)$. Since $b = [G : M] = q+1$ and

$$k = \frac{\chi(g) \times |nX|}{[G : M]} = \frac{1 \times (q^2-1)}{q+1} = q-1,$$

the results follow from Remark 10.2. ■

If we have $\lambda = r = 2$ then a graph (possibly with multiple edges) can be defined on b vertices, where b is the number of blocks, i.e. the index of M in G, by stipulating that the vertices labelled by the blocks b_i and b_j are adjacent if b_i and b_j meet. Then the incidence matrix for the design is an incidence matrix for the graph.

In the case where the graph is an undirected graph without multiple edges the following result from [8, Lemma] can be used.

Lemma 10.3 ([8]) *Let $\Gamma = (V, E)$ be a regular graph with $|V| = N$, $|E| = e$ and valency v. Let $\mathcal{G}$ be the 1-$(e, v, 2)$ incidence design from an incidence matrix A for Γ. Then $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(\mathcal{G})$.*

Note: If the graph Γ is also connected, then it is an easy induction to show that $\mathrm{rank}_p(A) \geq |V| - 1$ for all p with obvious equality when $p = 2$. If in addition (as happens for some classes of graphs, see [8, 25, 24]) the minimum weight is the valency and the words of this weight are the scalar multiples of the rows of the incidence matrix, then we also have $\mathrm{Aut}(C_p(\mathcal{G})) = \mathrm{Aut}(\mathcal{G})$.

Proposition 10.4 *For $G = PSL_2(q)$, let M be the stabilizer of a point in the natural action of degree $q+1$ on the set Ω. Let $M = G_1$. Suppose $g \in nX \subseteq G$ is an element fixing exactly two points, and without loss of generality, assume $g \in M = G_1$ and that $g \in G_2$. Then the replication number for the associated design is $r = \lambda = 2$. We also have*

(i) If g is an involution, so that $q \equiv 1 \pmod 4$, the design $\mathcal{D}$ is a 1-$(\frac{1}{2}q(q+1), q, 2)$ design with $q+1$ blocks and $Aut(\mathcal{D}) = S_{q+1}$. Furthermore $C_2(\mathcal{D}) = [\frac{1}{2}q(q+1), q, q]_2$, $C_p(\mathcal{D}) = [\frac{1}{2}q(q+1), q+1, q]_p$ if p is an odd prime, and $\mathrm{Aut}(C_p(\mathcal{D})) = \mathrm{Aut}(\mathcal{D}) = S_{q+1}$ for all p.

(ii) If g is not an involution, the design $\mathcal{D}$ is a 1-$(q(q+1), 2q, 2)$ design with $q+1$ blocks and $Aut(\mathcal{D}) = 2^{\frac{1}{2}q(q+1)} : S_{q+1}$. Furthermore $C_2(\mathcal{D}) = [q(q+1), q, 2q]_2$, $C_p(\mathcal{D}) = [q(q+1), q+1, 2q]_p$ if p is an odd prime, and $\mathrm{Aut}(C_p(\mathcal{D})) = \mathrm{Aut}(\mathcal{D}) = 2^{\frac{1}{2}q(q+1)} : S_{q+1}$ for all p.

Proof: A block of the design constructed will be $M \cap g^G$. Notice that from elementary considerations or using group characters we have that the only powers of g that are conjugate to g in G are g and g^{-1}. Since M is transitive on $\Omega \setminus \{1\}$, g^M and $(g^{-1})^M$ give $2q$ elements in $M \cap g^G$ if $o(g) \neq 2$, and q if $o(g) = 2$. These are all the elements in $M \cap g^G$ since M_j is cyclic so if $h_1, h_2 \in M_j$ and $h_1 = g_1^x, h_2 = g_2^x$ for some $x_1, x_2 \in G$, then h_1 is a power of h_2, so they can only be equal or inverses of one another.

(i) In this case by the above $k = |M \cap g^G| = q$ and hence

$$|nX| = \frac{k \times [G:M]}{\chi(g)} = \frac{q \times (q+1)}{2}.$$

So $\mathcal{D}$ is a 1-$(\frac{1}{2}q(q+1), q, 2)$ design with $q+1$ blocks. An incidence matrix of the design is an incidence matrix of a graph on $q+1$ points labelled by the rows of the matrix, with the vertices corresponding to rows r_i and r_j being adjacent if there is a conjugate of g that fixes both i and j, giving an edge $[i, j]$. Since G is 2-transitive, the graph we obtain is the complete graph K_{q+1}.

The automorphism group of the design is the same as that of the graph (see [8]), which is S_{q+1}. By [24], $C_2(\mathcal{D}) = [\frac{1}{2}q(q+1), q, q]_2$ and $C_p(\mathcal{D}) = [\frac{1}{2}q(q+1), q+1, q]_p$ if p is an odd prime. Further, the words of the minimum weight q are the scalar multiples of the rows of the incidence matrix, so $\mathrm{Aut}(C_p(\mathcal{D})) = \mathrm{Aut}(\mathcal{D}) = S_{q+1}$ for all p.

(ii) If g is not an involution, then $k = |M \cap g^G| = 2q$ and hence

$$|nX| = \frac{k \times [G:M]}{\chi(g)} = \frac{2q \times (q+1)}{2} = q(q+1).$$

So $\mathcal{D}$ is a 1-$(q(q+1), 2q, 2)$ design with $q+1$ blocks. In the same way we define a graph from the rows of the incidence matrix, but in this case we have the complete directed graph.

The automorphism group of the graph and of the design is $2^{\frac{1}{2}q(q+1)} : S_{q+1}$. Similarly to the previous case, $C_2(\mathcal{D}) = [q(q+1), q, 2q]_2$ and $C_p(\mathcal{D}) = [q(q+1), q+1, 2q]_p$ if p is an odd prime. Further, the words of the minimum weight $2q$ are the scalar multiples of the rows of the incidence matrix, so $\text{Aut}(C_p(\mathcal{D})) = \text{Aut}(\mathcal{D}) = 2^{\frac{1}{2}q(q+1)} : S_{q+1}$ for all p. ■

We end this subsection by giving few examples of designs and codes constructed, using Propositions 10.2 and 10.4, from $PSL_2(q)$ for $q \in \{16, 17, 19\}$, where M is the stabilizer of a point in the natural action of degree $q+1$ and $g \in nX \subseteq G$ is an element fixing exactly one or two points.

Example 10.1 ($PSL_2(16)$)

1. *g is an involution having cycle type $1^1 2^8$, $r = \lambda = 1$: $\mathcal{D}$ is a $1-(255, 15, 1)$ design with 17 blocks. For all p, $C = C_p(\mathcal{D}) = [255, 17, 15]_p$, with* $\text{Aut}(C) = \text{Aut}(\mathcal{D}) = S_{15} \wr S_{17} = (S_{15})^{17} : S_{17}$.

2. *g is an element of order 3 having cycle type $1^2 3^5$, $r = \lambda = 2$: $\mathcal{D}$ is a $1-(272, 32, 2)$ design with 17 blocks. $C_2(\mathcal{D}) = [272, 16, 32]_2$ and $C_p(\mathcal{D}) = [272, 17, 32]_p$ for odd p. Also for all p we have* $\text{Aut}(C_p(\mathcal{D})) = \text{Aut}(\mathcal{D}) = 2^{136} : S_{17}$.

Example 10.2 ($PSL_2(17)$) *Note that* $17 \equiv 1 \pmod 4$.

1. *g is an element of order 17 having cycle type $1^1 17^1$, $r = \lambda = 1$: $\mathcal{D}$ is a $1-(144, 8, 1)$ design with 18 blocks. For all p, $C = C_p(\mathcal{D}) = [144, 18, 8]_p$, with* $\text{Aut}(C) = \text{Aut}(\mathcal{D}) = S_8 \wr S_{18} = (S_8)^{18} : S_{18}$.

2. *g is an involution having cycle type $1^2 2^8$, $r = \lambda = 2$: $\mathcal{D}$ is a $1-(153, 17, 2)$ design with 18 blocks. $C_2(\mathcal{D}) = [153, 17, 17]_2$ and $C_p(\mathcal{D}) = [153, 18, 17]_p$ for odd p. Also for all p we have* $\text{Aut}(C_p(\mathcal{D})) = \text{Aut}(\mathcal{D}) = S_{18}$.

3. *g is an element of order 4 having cycle type $1^2 4^4$, $r = \lambda = 2$: $\mathcal{D}$ is a $1-(306, 34, 2)$ design with 18 blocks. $C_2(\mathcal{D}) = [306, 17, 34]_2$ and $C_p(\mathcal{D}) = [306, 18, 34]_p$ for odd p. Also for all p we have* $\text{Aut}(C_p(\mathcal{D})) = \text{Aut}(\mathcal{D}) = 2^{153} : S_{18}$.

4. *g is an element of order 8 having cycle type $1^2 8^2$, $r = \lambda = 2$: $\mathcal{D}$ is a $1-(306, 34, 2)$ design with 18 blocks. $C_2(\mathcal{D}) = [306, 17, 34]_2$ and $C_p(\mathcal{D}) = [306, 18, 34]_p$ for odd p. Also for all p we have* $\text{Aut}(C_p(\mathcal{D})) = \text{Aut}(\mathcal{D}) = 2^{153} : S_{18}$.

Example 10.3 ($PSL_2(19)$)

1. *g is an element of order 19 having cycle type $1^1 19^1$, $r = \lambda = 1$: $\mathcal{D}$ is a $1-(180, 9, 1)$ design with 20 blocks. For all p, $C = C_p(\mathcal{D}) = [180, 20, 9]_p$, with* $\text{Aut}(C) = \text{Aut}(\mathcal{D}) = S_9 \wr S_{20} = (S_9)^{20} : S_{20}$.

2. *g is an element of order 3 having cycle type $1^2 3^6$, $r = \lambda = 2$: $\mathcal{D}$ is a $1-(380, 38, 2)$ design with 20 blocks. $C_2(\mathcal{D}) = [360, 19, 38]_2$ and $C_p(\mathcal{D}) = [360, 20, 38]_p$ for odd p. Also for all p we have* $\text{Aut}(C_p(\mathcal{D})) = \text{Aut}(\mathcal{D}) = 2^{190} : S_{20}$.

10.3 Some 1-designs from the Janko group J_1

The Jako group J_1 of order $2^3 \times 3 \times 5 \times 7 \times 11 \times 19$ has seven conjugacy classes of maximal subgroups, which were listed in the table 1. It has also 15 conjugacy classes of elements some of which are listed in Table 12.

nX	$\|nX\|$	$C_G(g)$	Maximal Centralizer
$2A$	1463	$2 \times A_5$	Yes
$3A$	5852	$D_6 \times 5$	No

Table 12: Some of the conjugacy classes of J_1

We apply the Theorem 10.1 to the maximal subgroups and few conjugacy classes of elements of J_1 to construct several 1- designs.

10.3.1 $G = J_1$, $M = PSL_2(11)$ and $nX = 2A$: $1-(1463, 55, 10)$ Design

Let $G = J_1$, $M = PSL_2(11)$ and $nX = 2A$. Then

$$b = [G : M] = 266, v = |2A| = 1463, k = |M \cap 2A| = 55.$$

Also using the character table of J_1, we have

$$\chi_M = \chi_1 + \chi_2 + \chi_4 + \chi_6 = \underline{1a} + \underline{56a} + \underline{56b} + \underline{76a} + \underline{77a}$$

and hence $\chi_M(g) = 1 + 0 + 0 + 4 + 5 = 10 = \lambda$, where $g \in 2A$. We produce a non-symmetric $1-(1463, 55, 10)$ design $\mathcal{D}$. Since $C_G(g) = 2 \times A_5$ is also a maximal subgroup of J_1, J_1 acts primitively on blocks and points. The complement of $\mathcal{D}$, $\tilde{\mathcal{D}}$, is a $1-(1463, 1408, 256)$ design.

10.3.2 $G = J_1$, $M = 2 \times A_5$ and $nX = 2A$: $1-(1463, 31, 31)$ Design

Let $G = J_1$, $M = 2 \times A_5$ and $nX = 2A$. Then

$$b = [G : M] = 1463, v = |2A| = 1463.$$

It is easy to see that $M = 2 \times A_5$ has three conjugacy classes of order 2, namely $x_1 = z$, $x_2 = \alpha$ and $x_3 = z\alpha$, that fuse to $2A$ with corresponding centralizer orders 120, 8 and 8. Now by using Corollary 6.3 we have

$$\lambda = \chi_M(g) = \sum_{i=1}^{3} \frac{|C_G(g)|}{|C_M(x_i)|} = \frac{120}{120} + \frac{120}{8} + \frac{120}{8} = 31,$$

where $g \in 2A$. Alternatively we can use the character table of J_1 to find that

$$\chi_M = \chi_1 + \chi_2 + \chi_3 + 2\chi_4 + 2\chi_6 + \chi_9 + \chi_{10} + \chi_{11} + 2\chi_{12} + 2\chi_{15},$$

and

$$\chi_M(g) = 1 + 0 + 0 + 8 + 10 + 0 + 0 + 0 + 10 + 2 = 31 = \lambda.$$

In this case clearly $k = |M \cap 2A| = \lambda = 31$, and we produce a symmetric $1-(1463, 31, 31)$ design $\mathcal{D}$. Obviously J_1 acts primitively on blocks and points. The complement of $\mathcal{D}$, $\tilde{\mathcal{D}}$, is a $1-(1463, 1432, 1432)$ design.

10.3.3 $G = J_1$, $M = PSL_2(11)$ and $nX = 3A$: $1-(5852, 110, 5)$ Design

Let $G = J_1$, $M = PSL_2(11)$ and $nX = 3A$. Then

$$b = [G : M] = 266, v = |3A| = 5852, k = |M \cap 3A| = 110.$$

Also using the character table of J_1, we have

$$\chi_M = \chi_1 + \chi_2 + \chi_4 + \chi_6 = \underline{1a} + \underline{56a} + \underline{56b} + \underline{76a} + \underline{77a}$$

and hence $\chi_M(g) = 1 + 4 + 1 - 1 = 5 = \lambda$, where $g \in 3A$. We produce a non-symmetric $1-(5852, 110, 5)$ design $\mathcal{D}$. Since $C_G(g) = D_6 \times 5$ is not a maximal subgroup of J_1, J_1 acts primitively on 266 blocks but imprimitively on 5852 points. The complement of $\mathcal{D}$, $\tilde{\mathcal{D}}$, is a $1-(5852, 5742, 261)$ design.

10.3.4 $G = J_1$, $M = PSL_2(11)$ and $nX = 3A$: $1-(5852, 20, 5)$ Design

Let $G = J_1$, $M = 2 \times A_5$ and $nX = 3A$. Then

$$b = [G : M] = 1463, v = |3A| = 5852, k = |M \cap 3A| = 20.$$

It is easy to see that $M = 2 \times A_5$ has only one conjugacy class of elements of order 3, which fuses to $3A$, with the corresponding centralizer order 6. Now by using Corollary 6.3 we have

$$\lambda = \chi_M(g) = \frac{|C_G(g)|}{|C_M(x)|} = \frac{30}{6} = 5,$$

where $g \in 3A$. Alternatively we can use the character χ_M as in Subsection 10.3.2 to find that

$$\chi_M(g) = 1 + 2 + 2 + 2 - 2 + 0 + 0 + 0 + 2 - 2 = 5 = \lambda,$$

where $g \in 3A$. We produce a non-symmetric $1-(5852, 20, 5)$ design $\mathcal{D}$. Since $C_G(g) = D_6 \times 5$ is not a maximal subgroup of J_1, J_1 acts primitively on the 1463 blocks but imprimitively on the 5852 points. The complement of $\mathcal{D}$, $\tilde{\mathcal{D}}$, is a $1-(5852, 5832, 1458)$ design.

References

[1] F. Ali, *Fischer-Clifford Theory for Split and non-Split Group Extensions*, PhD Thesis, University of Natal, 2001.

[2] E. F. Assmus, Jr. and J. D. Key, *Designs and their Codes*, Cambridge University Press, 1992 (Cambridge Tracts in Mathematics, Vol. 103, Second printing with corrections, 1993).

[3] B. Bagchi, A regular two-graph admitting the Hall-Janko-Wales group, Combinatorial mathematics and applications (Calcutta, 1988),*Sankhyā, Ser. A* **54** (1992), 35–45.

[4] W. Bosma and J. Cannon, *Handbook of Magma Functions*, Department of Mathematics, University of Sydney, November 1994.

[5] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *An Atlas of Finite Groups*, Oxford University Press, 1985.

[6] R. Bruck and H. J Ryser, The non-existence of certain finite projective planes, *Canad. J. Math.* , **1** (1949), 88–93.

[7] A. E. Brouwer, Strongly regular graphs, in Charles J. Colbourn and Jeffrey H. Dinitz, editors, *The CRC Handbook of Combinatorial Designs*, pages 667–685. CRC Press, Boca Raton, 1996. VI.5.

[8] W. Fish, J. D. Key, and E. Mwambene, Codes from the incidence matrices and line graphs of Hamming graphs, submitted.

[9] L. Finkelstein, The maximal subgroups of Janko's sinple group of order $50, 232, 960$, *J. Algebra*, **30** (1974), 122–143.

[10] L. Finkelestein and A. Rudvalis, Maximal subgroups of the Hall-Janko-Wales group, *J. Algebra*, **24** (1977),486–493.

[11] M. S. Ganief, *2-Generations of the Sporadic Simple Groups*, PhD Thesis, University of Natal, 1997.

[12] I. M. Isaacs, *Character Theory of Finite Groups*, Academic Press, San Diego, 1976.

[13] The GAP Group, *GAP - Groups, Algorithms and Programming, Version 4.2* , Aachen, St Andrews, 2000, `(http://www-gap.dcs.st-and.ac.uk/~gap)`.

[14] K. E. Gehles, *Ordinary characters of finite special linear groups*, MSc Dissertaion, University of St Andrews, 2002.

[15] W. C. Huffman, Codes and groups, in V. S. Pless and W. C. Huffman, editors, *Handbook of Coding Theory*, pages 1345–1440, Amsterdam: Elsevier, 1998, Volume 2, Part 2, Chapter 17.

[16] C. Jansen, K. Lux, R. Parker, and R. Wilson. *An Atlas of Brauer Characters*. Oxford: Oxford Scientific Publications, Clarendon Press, 1995. LMS Monographs New Series 11.

[17] W. Knapp and P. Schmid, Codes with prescribed permutation group, *J. Algebra*, **67** (1980), 415–435, 1980.

[18] J. D. Key and J. Moori, Designs, codes and graphs from the Janko groups J_1 and J_2, *J. Combin. Math. and Combin. Comput.*, **40** (2002), 143–159.

[19] J. D. Key and J. Moori, Correction to: "Codes, designs and graphs from the Janko groups J_1 and J_2 [*J. Combin. Math. Combin. Comput.*, 40 (2002), 143–159], *J. Combin. Math. Combin. Comput.*, **64** (2008), 153.

[20] J. D. Key and J. Moori, Some irreducible codes invariant under the Janko group, J_1 or J_2, submitted.

[21] J. D. Key and J. Moori, Designs and codes from maximal subgroups and conjugacy classes of finite simple groups, submitted.

[22] J. D. Key, J. Moori, and B. G. Rodrigues, On some designs and codes from primitive representations of some finite simple group, *J. Combin. Math. and Combin. Comput.*, **45** (2003), 3–19.

[23] J. D. Key, J. Moori, and B. G. Rodrigues, Some binary codes from symplectic geometry of odd characteristic, *Utilitas Mathematica*, **67** (2005), 121-128.

[24] J. D. Key, J. Moori, and B. G. Rodrigues, Codes associated with triangular graphs, and permutation decoding, *Int. J. Inform. and Coding Theory*, to appear.

[25] J. D. Key and B. G. Rodrigues, Codes associated with lattice graphs, and permutation decoding, submitted.

[26] W. Knapp and P. Schmid, Codes with prescribed permutation group, *J. Algebra*, **67**(1980), 415–435, 1980.

[27] c. W. H Lam, The search for a finite projective plane of order 10, *Amer. Math. Monthly* **98** (1991), 305-318.

[28] J. Moori, Finite groups, designs and codes, *Information Security, Coding Theory and Related Combinatorics*, Nato Science for Peace and Security Series D: Information and Communication Security, **29** (2011), 202–230, IOS Press (ISSN 1874-6268).

[29] J. Moori, *Finite Groups and Representation Theory*, AIMS Lectures, 2011.

[30] J. Moori, *Finite Groups, Designs and Codes*, AIMS Lectures, 2011

[31] J. Moori and B. G. Rodrigues, A self-orthogonal doubly even code invariant under the $M^cL:2$ group, *J. Comb. Theory, Series A*, **110** (2005), 53–69.

[32] J. Moori and B. G. Rodrigues, Some designs and codes invariant under the simple group Co_2, *J. of Algerbra*, **316** (2007), 649–661.

[33] J. Moori and B. G. Rodrigues, A self-orthogonal doubly-even code invariant under $\mathrm{M^cL}$, *Ars Combinatoria*, **91** (2009), 321–332.

[34] J. Moori and B. G. Rodrigues, Some designs and codes invariant under the Higman-Sims group, *Utilitas Mathematica*, to appear.

[35] J. Moori and B. Rodrigues, Ternary codes invariant under the simple group Co_2, under prepararion.

[36] J. Müller and J. Rosenboom, Jens, Condensation of induced representations and an application: the 2-modular decomposition numbers of Co_2, Computational methods for representations of groups and algebras (Essen, 1997), 309–321, *Progr. Math.*, 173, Birkhuser, Basel, 1999.

[37] J. J. Rotman, *An Introduction to the Theory of Groups*, volume 148 of Graduate Text in Mathematics, Springer-Verlag, 1994.

[38] I. A. Suleiman and R. A. Wilson, The 2-modular characters of Conway's group Co_2, *Math. Proc. Cambridge Philos. Soc.* **116** (1994), 275–283.

[39] R. A. Wilson, Vector stabilizers and subgroups of Leech lattice groups, *J. Algebra*, **127** (1989), 387–408.

[40] , R. A. Wilson, The maximal subgroups of Conway's group Co_2, *J. Algebra,* **84** *(1983), 107–114*.