## Distribution Agreement

Representation Theory of Finite Groups and its Applications

by

Siwei Xu

Raman Parimala
Adviser

Mathematics

Raman Parimala

Adviser

David Borthwick

Committee Member

David Zureick-Brown

Committee Member

2022

Representation Theory of Finite Groups and its Applications

By

Siwei Xu

Raman Parimala

Adviser

An abstract of
a thesis submitted to the Faculty of Emory College of Arts and Sciences
of Emory University in partial fulfillment
of the requirements of the degree of
Bachelor of Science with Honors

Mathematics

2022

Abstract

Representation Theory of Finite Groups and its Applications
By Siwei Xu

In this paper, we give an exposition of the representation theory of finite groups: character theory, and Frobenius-Schur descent of complex representations to real ones. We also give the applications of representation theory in proofs to the following three theorems: Burnside theorem, on the degree of $\alpha+\beta$, Eckmann's proof on Hurwitz's theorem.

Representation Theory of Finite Groups and its Applications

By

Siwei Xu

Raman Parimala

Adviser

A thesis submitted to the Faculty of Emory College of Arts and Sciences
of Emory University in partial fulfillment
of the requirements of the degree of
Bachelor of Science with Honors

Mathematics

2022

Acknowledgements

Great thanks to Dr. Parimala, my advisor, who were always so patient and helped me so much throughout the entire process of the honors program.

Contents

## 0. Introduction

The aim of this thesis is two fold. We give an exposition of the representation theory of finite groups: character theory, and Frobenius-Schur descent of complex representations to real ones. We give three applications of representation theory to solution of problems.

**Theorem 0.1.** *(Burnside) Let $G$ be a finite group of order $p^a q^b$, $a, b \in \mathbb{Z}^+$, $p$ and $q$ primes. Then $G$ is solvable.*

The famous Feit-Thomson theorem asserts that every finite group of odd order is solvable. The proof runs through 250 pages.

**Theorem 0.2.** *Let $F$ be a field of characteristic zero, and $L$ is a finite extension of $F$. Suppose $\alpha, \beta \in L$, $[F(\alpha) : F] = m$ and $[F(\beta) : F] = n$ with $m$ and $n$ coprime. Then $F(\alpha, \beta) = F(\alpha + \beta)$.*

In general, $F(\alpha, \beta) = F(\alpha + c\beta)$ for almost all $c \in F$. But in the coprime degree case, $\alpha + \beta$ serves as a primitive element for $F(\alpha, \beta)$ over F.

**Theorem 0.3.** *(A theorem of Hurwitz) Let $n \in \mathbb{Z}^+$, $n = u \cdot 2^{4\alpha+\beta}$, with $u$ odd, and $\beta = 0, 1, 2, 3$. There exists $z_1, ...z_n$ bilinear in $x_1, ...x_p$ and $y_1, ...y_n$ with complex coefficients satisfying*

$$(x_1^2 + x_2^2 + ... + x_p^2)(y_1^2 + y_2^2 + ... + y_n^2) = (z_1^2 + z_2^2 + ... + z_p^2) \tag{1}$$

*if and only if $p \leq 8\alpha + 2^\beta$. Further, we can choose the solutions to be real.*

An algebra structure on $\mathbb{R}^n$ is called a composition algebra if $||v \cdot w|| = ||v|| \cdot ||w||$ where $||z|| = z_1^2 + ... + z_n^2$ for $z = (z_1, .., z_n)$.

**Corollary 0.4.** *The only composite algebras over $\mathbb{R}$ occur in dimension 1,2,4, or 8 and they are $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ (quaternions algebra), and $\mathbb{O}$ (Octonion algebra).*

We present complete proofs of the above results using results from representation theory of finite groups which we give an exposition in the thesis. The proof of theorem 2 is due to Isaacs ([5]). The proof of theorem 3 presented here is due to Eckmann ([4]).

Here is a brief description of the contents of the the thesis. In section 1, we recall some standard results from algebra, concerning Sylow theorems, algebraic integers, Galois theory, and linear algebra. In section 2, we recall results from representation theory of finite groups required for the proofs in later sections. Sections 3, 4, and 5 are devoted to the proof of the three theorems listed earlier.

## 1. Preliminaries

### 1.1. **Sylow Theorems.**

**Lemma 1.1.** *Let $p$ be a prime dividing $|G|$, then $G$ has an element of order $p$.*

**Theorem 1.2.** *Let $G$ be a group of order $p^k m$, $k \geq 1$, and $p \nmid m$, then $G$ has a subgroup of order $p^k$ (which is called the $p$-Sylow subgroup of $G$).*

*Proof.* The proof is by induction on the order of G.
(case 1) p divides $|Z(G)|$. By 1.1, $\exists x \in Z(G)$ such that $order(x) = p$. The group generated by x: <x> has order p, and is a normal subgroup of G, so $G/<x>$ is a quotient group. Observe that $|G/<x>| = p^{k-1}m$. If k=1, $<x>$ is the p-Sylow subgroup we are looking for. By induction, $G/<x>$ has a subgroup $\bar{P}$ of order $p^{k-1}$. We look at the quotient map $\phi : G \to G/<x>$. Then, $ker(\phi) =<x>$, and it is onto. $P' = \phi^{-1}(\bar{P})$ is a subgroup of G. Now, map $P'$ to $\bar{P}$ by restricting $\phi$ to $P'$. The kernel is $<x>$, and $\exists$ a isomorphism $\widetilde{\phi}$ from $P'/<x>$ to $\bar{P}$. Thus, $|P'| = pp^{k-1} = p^k$. Thus, $P'$ is the p-Sylow subgroup of G.
(case 2) p does not divide $|Z(G)|$. By class equation, $p \nmid [G : C_G(x)]$ for some $x$ not in $Z(G)$. Then, $p^k \mid |C_G(x)|$, and $|C_G(x)| < |G|$. By induction, $C_G(x)$ has a subgroup P of order $p^k$. Therefore, P is the p-Sylow subgroup of G. $\square$

### 1.2. **p-groups.**

**Lemma 1.3.** *The center of a p-group is nontrivial*

*Proof.* Suppose $G = p^m$, $m \geq 1$. We have the class equation,

$$p^m = |Z(G)| + \sum_{[x_i]\ noncentral} [G : C_G(x)]$$

where $C_G(x) = \{g \in G | gx = xg\}$. We know that $p$ divides $[G : C_G(x)]$ for all noncentral x. Hence, p divides $|Z(G)|$. Thus, $|Z(G)| \geq 1$, and it is nontrivial. $\square$

### 1.3. **Nilpotent and Solvable Groups.**

**Definition 1.4.** A group $G$ is **solvable** if there is a chain of subgroups

$$1 = G_0 \subseteq G_1 \subseteq G_2 \subseteq ... \subseteq G_s = G$$

such that $G_i$ is normal in $G_{i+1}$ for all i, and $G_{i+1}/G_i$ is abelian for $i = 0, 1, ., s-1$

**Theorem 1.5.** *Suppose $G$ has a normal subgroup $H$. If $H$ and $G/H$ are both solvable, $G$ is solvable*

*Proof.* Let $\phi : G \to G/H$ be the quotient map. Since $G/H$ is solvable, there is a chain of subgroups: $G/H = G_0' \supseteq G_1' \supseteq ...G_n' = e$, such that $G_{i+1}'$ is normal in $G_i'$ and $G_i'/G_{i+1}'$ is abelian. Now, take $\phi^{-1}$ of every term in the chain, and we get the following new chain:

$$G \supseteq G_1 \supseteq G_2 \supseteq ... \supseteq H$$

with $G_{i+1}$ normal in $G_i$ and $G_i/G_{i+1} \simeq G_i'/G_{i+1}'$ is abelian. Since H is also solvable, we have $H \supseteq H_1 \supseteq ... \supseteq H_m = e$, such that $H_{i+1}$ is normal in $H_i$ and $H_i/H_{i+1}$ is abelian. Combining the two chains, we conclude that G is solvable. $\square$

We recall the following standard facts on p-groups. (cf. [1])

**Lemma 1.6.** *Let $G$ be a p-group and $H$ be a normal subgroup of $G$. Then $H \cap Z(G) \neq \{1\}$*

**Definition 1.7.** A subgroup H of G is maximal if $H \neq G$, and if $H \subsetneq H'$, $H' = G$

**Lemma 1.8.** *Let $|G| = p^n$, then there is a maximal subgroup in G, and all maximal subgroups of G are normal and have order $p^{n-1}$*

**Lemma 1.9.** *$|G| = p^n$, and H is a normal subgroup of G. Suppose $p^b \mid |H|$, then H has a subgroup K of order $p^b$ that is normal in G.*

**Theorem 1.10.** *p-groups are solvable*

*Proof.* Suppose $|G| = p^n$. By 1.8, $\exists G_1$ such that $G_1$ is of order $p^{n-1}$, and it is normal in G. By 1.9, since $p^{n-2}$ divides $|G_1|$, $G_1$ has a subgroup $G_2$ of order $p^{n-2}$ that is normal in G. We can repeat this process, and get a chain of subgroups:

$$G \supseteq G_1 \supseteq G_2 \supseteq ... \supseteq G_n = \{1\}$$

Each $G_i/G_{i+1}$ is abelian since it is a prime order group. Therefore, G is solvable. □

1.4. **Algebraic Integer.**

**Definition 1.11.** $\alpha \in \mathbb{C}$ is an **algebraic integer** if it is the root of a monic polynomial with coefficients in $\mathbb{Z}$

**Theorem 1.12.** *$\alpha$ is an algebraic integer if and only if $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module*

*Proof.* ($\Rightarrow$) Let $\alpha$ be an algebraic integer. $\mathbb{Z}[\alpha]$ is a $\mathbb{Z}$-module generated by $\{1, \alpha, \alpha^2, ...\}$. There $\exists$ a monic polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$, which means $\alpha^n$ can be expressed as a linear combination of $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$. Therefore, $\mathbb{Z}[\alpha]$ is finitely generated $\mathbb{Z}$-module.
($\Leftarrow$) Suppose $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module and it is generated by $\{\beta_1, ..., \beta_k\}$. Since $\alpha\beta_i \in \mathbb{Z}[\alpha]$ for all i, there exists $a_{ij} \in \mathbb{Z}$ such that

$$\alpha\beta_i = \sum_{j=1}^{k} a_{ij}\beta_j$$

Let $A = (a_{ij})$, then we have the following equation:

$$(\alpha I_k - A)\begin{pmatrix}\beta_1 \\ \vdots \\ \beta_k\end{pmatrix} = \begin{pmatrix}0 \\ \vdots \\ 0\end{pmatrix}$$

Let $(\alpha I_k - A)^*$ be the adjoint matrix so that

$$(\alpha I_k - A)^*(\alpha I_k - A) = det(\alpha I_k - A) = f(\alpha)$$

Hence, $f(\alpha) \cdot \beta_i = 0$ for $1 \leq i \leq k$. Since 1 is a linear combination of $\{\beta_1, ...\beta_k\}$, $f(\alpha) \cdot 1 = 0$. Since $f(x)$ is a monic polynomial with coefficients in $\mathbb{Z}$, we conclude that $\alpha$ is an algebraic integer. □

**Theorem 1.13.** *Let $R \subseteq \mathbb{C}$ be a subring containing $\mathbb{Z}$ which is finitely generated $\mathbb{Z}$-module. Then every $\alpha \in R$ is an algebraic integer.*

*Proof.* Since $\mathbb{Z}$ is Noetherian, and $R$ is finitely generated $\mathbb{Z}$-module, given $\alpha \in R$, $\mathbb{Z}[\alpha] \subset R$ is also a finitely generated $\mathbb{Z}$-module. By 1.12, $\alpha$ is an algebraic integer. □

**Theorem 1.14.** *The algebraic integers in $\mathbb{C}$ form a ring*

*Proof.* Let $\alpha, \beta$ be two algebraic integers, then $\mathbb{Z}[\alpha, \beta]$ is a finitely generated $\mathbb{Z}$-module and $\alpha - \beta \in \mathbb{Z}[\alpha, \beta]$ is an algebraic integer by 1.12. Similarly, $\alpha \cdot \beta \in \mathbb{Z}[\alpha, \beta]$ is also an algebraic integer. The set of algebraic integers is closed under multiplication and addition. Thus, it forms a ring. □

**Theorem 1.15.** *The algebraic integers in $\mathbb{Q}$ are the elements of $\mathbb{Z}$*

*Proof.* Suppose $\alpha \in Q$,we can write it as $\frac{c}{d}$. Since it is an algebraic integer, $\exists f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ such that $f(\alpha) = 0$. Plug it in and get

$$a_0 + a_1 \frac{c}{d} + a_2 (\frac{c}{d})^2 + ... + (\frac{c}{d})^n = 0$$

Multiply both side by $d^n$, and get

$$a_0 d^n + a_1 c d^{n-1} + ... + c^n = 0$$

This is equivalent to

$$d(a_0 d^{n-1} + ... + a_{n-1} c^{n-1}) = -c^n$$

By the equality of rational numbers, c and d are coprime. Since $d \mid c^n$, d=1. Hence, $\alpha$ is an integer. □

1.5. **Field Extensions and Galois Theory.**

**Theorem 1.16.** *Let $p(x) \in F[x]$ be irreducible. Let $E$ be a field extension of $F$ and $a$ be a zero of $p(x)$ in $E$. Then, there is an $F$-isomorphism:*

$$\phi : \frac{F[x]}{< p(x) >} \to F(a)$$

*which maps $x + < p(x) >$ to $\alpha$.*

**Corollary 1.17.** *Let $p(x) \in F[x]$ be irreducible. Let $E$ be a field extension of $F$ and $a, b$ be distinct zeros of $p(x)$ in $E$. Then, there is an $F$-isomophism:*

$$\phi : F(a) \to F(b)$$

*such that $\phi(a) = b$.*

**Theorem 1.18.** *If $K$ is a field extension of $F$ and $\alpha, \beta \in K$, with $\alpha, \beta$ algebraic over $F$ and $deg(\alpha) = m$, $deg(\beta) = n$, such that m,n are coprime, then $[F(\alpha, \beta) : F] = mn$.*

*Proof.* By the multiplicativity of degree in a tower of field extensions, we get the following two equations:

$$[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)][F(\alpha) : F] = t_1 \cdot m$$
$$[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\beta)][F(\beta) : F] = t_2 \cdot n$$

Since m, and n are coprime, $[F(\alpha, \beta) : F] \geq mn$. We also know that $[F(\alpha, \beta) : F] \leq mn$. Therefore, $[F(\alpha, \beta) : F] = mn$. □

## 1.6. Linear Algebra/Spectral Theorem.

We recall spectral theorem (cf. [2]).

**Theorem 1.19.** *Given a real symmetric matrix $A$, $\exists C \in GL_n(\mathbb{R})$, $CC^T = I_n$ and* $CAC^{-1} = \begin{pmatrix} \lambda_1 & \dots & 0 \\ \vdots & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$

**Theorem 1.20.** *Given a hermitian symmetric matrix $A$, i.e. $\bar{A}^T = A$, $\exists$ unitary matrix $V \in GL_n(\mathbb{C})$ such that* $VAV^{-1} = \begin{pmatrix} \lambda_1 & \dots & 0 \\ \vdots & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$

**Remark 1.21.** *Given a hermitian symmetric positive definite matrix $A$ over $\mathbb{C}$, by 1.20, $\exists$ unitary matrix $V$ such that* $VAV^{-1} = \begin{pmatrix} \lambda_1 & \dots & 0 \\ \vdots & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$

*Hence,* $A = V^{-1} \begin{pmatrix} \lambda_1 & \dots & 0 \\ \vdots & \ddots & \\ 0 & & \lambda_n \end{pmatrix} V$. *Let* $B = V^{-1} \begin{pmatrix} \sqrt{\lambda_1} & \dots & 0 \\ \vdots & \ddots & \\ 0 & & \sqrt{\lambda_n} \end{pmatrix} V$

*In this case, $A = B^2$, and $B$ is a hermitian symmetric positive definite matrix. Further, $B$ is a real polynomial in $A$ ($\exists P \in \mathbb{R}[x]$ such that $P(\lambda_i) = \sqrt{\lambda_i}$ for $1 \le i \le n$ and hence P(A)=B). Suppose $A = T^2$. Since $P(T^2) = B$, $T$ commutes with $B$.*

# 2. Representation Theory of Finite Groups

In this section, we recall the following facts of representation theory of finite groups. (cf. [3])

## 2.1. Introduction.

Let V be a vector space over the field $\mathbb{C}$ of complex numbers and let GL(V) be the group of isomorphisms of V onto itself. The group GL(V) is identifiable with the group of invertible square matrices of order n. Let G be a finite group.

**Definition 2.1.** A **linear representation** of G in V is a homomorphism $\rho$ from the group $G$ into the group $GL(V)$.

**Definition 2.2.** Let $\rho$ and $\rho^{'}$ be two representations of group G in vector spaces $V$ and $V^{'}$. Then, we say $\rho$ and $\rho^{'}$ are **isomorphic** if $\exists$ a linear isomorphism $\phi : V \to V^{'}$ such that

$$\phi \circ \rho_s = \rho^{'}_s \circ \phi \ \forall s \in G$$

**Definition 2.3.** Let g be the order of G and let V be a vector space of dimension g, with a basis $(e_t)_{t \in G}$ indexed by the elements t of G. For $s \in G$, let $\rho_s$ be the linear map of V into V which sends $e_t$ to $e_{st}$; this defines a linear representation, which is called the **regular representation** of G.

**Lemma 2.4.** *Given a representation $\rho : G \to GL(V)$. For every $s \in G$, the absolute value of eigenvalue of $\rho_s$ is 1.*

*Proof.* Since G is a finite group, element $s$ has order k, and $\rho_s^k = id$. Suppose $\lambda$ is an eigenvalue of $\rho_s$. We have $\lambda^k = 1$. Taking the absolute value of both side, we get that $|\lambda| = 1$. □

**Theorem 2.5.** *Let $\rho : G \to GL(V)$ be a linear representation of $G$ in $V$ and let $W$ be a vector subspace of $V$ stable under $G$. Then there exists a complement $W_0$ of $W$ in $V$ which is stable under $G$, i.e. $V = W \oplus W_0$.*

*Proof.* Let $W'$ be an arbitrary complement of $W$ in V, and let $p$ be the corresponding projection of V onto W. Define

$$p^0 = \frac{1}{|G|} \sum_{t \in G} \rho_t \cdot p \cdot \rho_t^{-1}$$

Since $\rho_t$ preserves W, we have $p^0$ maps V into W. For $x \in W$, we have $\rho_t^{-1} x \in W$. Since $p$ is a projection onto W, $p\rho_t^{-1}x = \rho_t^{-1}x$. This implies $p^0 x = x$. Hence, $p^0$ is a projection onto W. Let $W_0 = ker(p^0)$. Claim that $W_0$ is stable under G: We have $\rho_s \cdot p^0 = p^0 \cdot \rho_s$ for all $s \in G$. Suppose $x \in W_0$, $p^0 x = 0$, and $p^0 \cdot \rho_s(x) = \rho_s \cdot p^0(x) = 0$. This implies that $\rho_s(x) \in W_0$. Hence, $W_0$ is stable under G. □

**Definition 2.6.** Let $\rho$ be a linear representation of G. We say that it is **irreducible** if V is not 0 and if no vector subspace of V is stable under G, except for course 0 and V

**Theorem 2.7.** *Every representation is a direct sum of irreducible representations.*

*Proof.* Let $V$ be a linear representation of $G$. We perform induction on $dim(V)$ If $dim(V) = 0$, the theorem is obviously true. For $V$ of degree larger than 0, if $V$ is irreducible, we are done. If $V$ is not irreducible, there is a nonzero G-invariant subspace W and $W \neq V$. By 2.5, we have $V = W \oplus W_0$ with $dim(W) < dim(V)$, $dim(W_0) < dim(V)$, and $W, W_0$ both stable under G. By induction hypothesis, both $W$ and $W_0$ can be written as a direct sum of irreducible representations. Therefore, $V$ can be written as a direct sum of irreducible representations. □

**Definition 2.8.** Let $\rho_1 : G \to GL(V_1)$ and $\rho_2 : G \to GL(V_2)$ be two linear representations of a group G. For $s \in G$, define an element $\rho_s$ of $GL(V_1 \otimes V_2)$ by the condition:

$$\rho_s(v_1 \otimes v_2) = \rho_s^1(v_1) \otimes \rho_s^2(v_2)$$

We write $\rho_s = \rho_s^1 \otimes \rho_s^2$. Then $\rho_s$ defines a linear representation of G in $V_1 \otimes V_2$ which is called the **tensor product** of the given representations.

Let V be a representation of group G, and let $\theta$ be an automorphism of $V \otimes V$ such that $\theta(x \otimes y) = y \otimes x$ for all $x, y \in V$. Then, $\theta^2 = id$ and $\theta$ has $\{1, -1\}$ as eigenvalues.

**Theorem 2.9.** *The space $V \otimes V$ decomposes into a direct sum:*

$$V \otimes V = Sym^2(V) \oplus Alt^2(V)$$

*where*

$$Sym^2(V) = \{w \in V \otimes V | \theta(w) = w\}$$
$$Alt^2(V) = \{w \in V \otimes V | \theta(w) = -w\}$$

*Both $Sym^2(V)$ and $Alt^2(V)$ are G-invariant subspace of $V \otimes V$.*

2.2. **Character.**

**Definition 2.10.** Let $\rho : G \to GL(V)$ be a linear representation of a finite group G in the vector space V. For each $s \in G$,

$$\chi_\rho(s) = Tr(\rho_s) = \sum_i A_{ii} = \sum_i \lambda_i$$

where $\lambda_i$ is the eigenvalues of the matrix representation A of $\rho_s$. The complex valued function $\chi_\rho$ is called the **character** of the representation $\rho$.

**Theorem 2.11.** *If X is the character of a representation $\rho$ of degree n, we have:*
*(i) $\chi(1) = n$*
*(ii)$\chi(s^{-1}) = \chi(s)^*$ for $s \in G$*
*(iii) $\chi(tst^{-1}) = \chi(s)$ for all s,t $\in G$*
*Property (iii) implies $\chi$ is constant on elements in the same conjugacy class.*

**Theorem 2.12.** *(Schur's Lemma) Let $\rho^1 : G \to GL(V_1)$, $\rho^2 : G \to GL(V_2)$ be two irreducible representations of G and let f be a linear mapping of $V_1$ into $V_2$ such that $\rho_s^2 \circ f = f \circ \rho_s^1$ for all $s \in G$. Then:*
*1) If $\rho^1$ and $\rho^2$ are not isomorphic, we have $f = 0$.*
*2) If $V^1 = V^2$ and $\rho^1 = \rho^2$, f is scalar multiple of the identity map.*

*Proof.* Suppose $\rho^1$ and $\rho^2$ are not isomorphic. Now, suppose $f \neq 0$. Let $W_1 = ker(f)$. For $x \in W_1$, $f\rho_s^1 x = \rho_s^2 f x = 0$. Hence, $\rho_s^1 x \in W_1$, and $W_1$ is stable under $\rho^1$. Since $\rho^1$ is irreducible, $W_1 = 0$ or $V_1$. If $W_1 = V_1$, $ker(f) = V_1$ and $f = 0$. That is not the case, so $W_1 = 0$. Let $W_2 = Img(f)$. For $y \in W_2$, $\exists x \in W_1$ such that $f(x) = y$. We have $\rho_s^2 f x = f\rho_s^1 x \in W_2$, so $\rho_s^2 y \in W_2$ and $W_2$ is stable under $\rho^2$. Since $\rho^2$ is irreducible, $W_2 = 0$ or $V_2$. Since $f \neq 0$, $W_2 = V_2$. Hence, $f$ is bijective. This contradicts the assumption that $\rho^1$ and $\rho^2$ are not isomorphic (2.2). Therefore, $f = 0$.

Suppose now that $V = V_1 = V_2$, and $\rho = \rho^1 = \rho^2$. Let $\lambda$ be an eigenvalue of f, and $f' = f - \lambda$. Let W be the kernel of $f'$. For all $x \in W$ and $s \in G$, we have $f'\rho_s(x) = \rho_s f'(x) = 0$. So $\rho_s(x) \in W$, and W is stable under G. Since $\rho$ is irreducible, $W$ is either equal to $V$ or 0. It is not zero, since there exists at least one eigenvector in $ker(f')$. Thus, $W = V$ and $f' = 0$. Thus, f is equal to $\lambda I$. ∎

**Remark 2.13.** *Let h be a linear mapping of $V_1$ into $V_2$ and $g = |G|$. Let*

$$h^0 = \frac{1}{g} \sum_{t \in G} (\rho_t^2)^{-1} h \rho_t^1$$

*It's easy to verify that* $\rho_s^2 h^0 = h^0 \rho_s^1$.
*(case 1) Suppose* $\rho^1$ *and* $\rho^2$ *are not isomorphic. Then, by (1) in Schur's lemma,* $h^0 = 0$.
*(case 2) Suppose* $V = V_1 = V_2$ *and* $\rho = \rho^1 = \rho^2$. *Let* $n = dim(V)$. *Then, by (2) in Schur's lemma,* $h^0 = \lambda I$. *Furthermore,*

$$Tr(h^0) = \frac{1}{g}\sum_{t\in G} Tr(\rho_t^{-1})Tr(h)Tr(\rho_t) = Tr(h)$$

*We know that* $Tr(h) = Tr(h^0) = n\lambda$, *so* $\lambda = \frac{Tr(h)}{n}$. *Hence,* $h^0 = \frac{Tr(h)}{n} I$.

Now we rewrite the remark assuming that $\rho^1, \rho^2, h, h^0$ are given in matrix form:

$$\rho_t^1 = r(t), \rho_t^2 = d(t), h = x, h^0 = y$$

Then, for arbitrary $i_1, i_2$, we have:

$$y_{i_2 i_1} = \frac{1}{g}\sum_{t,j_1,j_2} d_{i_2 j_2}(t^{-1}) x_{j_2 j_1} r_{j_1 i_1}(t)$$

We plug in case 1 and case 2 to the equation above and get the following corollary:

**Corollary 2.14.** *For arbitrary* $i_1, j_1, i_2, j_2$,
*1) If* $\rho^1, \rho^2$ *are not isomorphic,*

$$\frac{1}{g}\sum_{t\in G} d_{i_2 j_2}(t^{-1}) r_{j_1 i_1}(t) = 0$$

*2) If* $\rho^1 = \rho^2$ *of degree* $n$,

$$\frac{1}{g}\sum_{t\in G} r_{i_2 j_2}(t^{-1}) r_{j_1 i_1}(t) = \begin{cases} \frac{1}{n}, & \text{if } i_1 = i_2 \text{ and } j_1 = j_2. \\ 0, & \text{otherwise.} \end{cases}$$

**Definition 2.15.** Let $\phi$ and $\psi$ be complex valued functions on G. Define

$$(\phi|\psi) = \frac{1}{g}\sum_{t\in G}\phi(t)\psi(t)^*$$

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

**Remark 2.16.** *If $\chi$ is the character of a representation of G, $(\phi|\chi) =< \phi, \chi >$ for all function $\phi$ on $G$ by (ii) in 2.11: $\chi(t^{-1}) = \chi(t)^*$ $\forall t \in G$*

With this new notation, corollary 2.14 can be written as:

**Corollary 2.17.** *Let $\rho^1, \rho^2$ be two irreducible representations. Writing $\rho^1, \rho^2$ in matrix form:*

$$\rho^1_t = r(t), \rho^2_t = d(t)$$

*For arbitary $i_1, j_1, i_2, j_2$,*
*1) If $\rho^1, \rho^2$ are not isomorphic, $< r_{i_1j_1}, d_{i_2j_2} >= 0$*
*2) If $\rho^1 = \rho^2$ of degree $n$,*

$$< r_{i_1j_1}, r_{i_2j_2} >= \begin{cases} \frac{1}{n}, & \text{if } i_1 = i_2 \text{ and } j_1 = j_2. \\ 0, & \text{otherwise.} \end{cases}$$

**Theorem 2.18.** *(i) Let $\chi$ be the character of an irreducible representation $\rho$ of degree $n$, we have $(\chi|\chi) = 1$*
*(ii) If $\chi$ and $\chi'$ are the characters of two nonisomorphic irreducible representations, we have $(\chi|\chi') = 0$*

*Proof.* (i) Let $\rho$ be an irreducible representation with character $\chi$, given in matrix form $\rho_t = (r_{ij}(t))$. We have $\chi(t) = \sum_i r_{ii}(t)$. Hence, by case 2 in 2.17

$$(\chi|\chi) =< \chi|\chi >= \sum_{i,j} < r_{ii}, r_{jj} >= \frac{n}{n} = 1$$

(ii) is proved in the same way, by applying case 1 in 2.17. $\square$

**Theorem 2.19.** *Let $V$ be a linear representation of $G$ with character $\phi$, and suppose $V$ decomposes into a direct sum of irreducible representations:*

$$V = W_1 \oplus W_2 \oplus .... \oplus W_k$$

*Then, if $W$ is an irreducible representation with character $\chi$, the number of $W_i$ isomorphic to $W$ is equal to $(\phi|\chi) =< \phi, \chi >$*

*Proof.* Let $\chi_i$ be the character of $W_i$, we have $\phi = \chi_1 + ... + \chi_k$, and

$$(\phi|\chi) = (\chi_1 + ... + \chi_k|\chi) = (\chi_1|\chi) + ... + (\chi_k|\chi)$$

By 2.18, $(\chi_i|\chi) = 0$ for $W_i$ not isomorphic to $W$, and $(\chi_i|\chi) = 1$ for $W_i$ isomorphic to $W$. Therefore, $(\phi|\chi)$ is equal to the number of $W_i$ isomorphic to $W$. $\square$

Let $W_1, ..., W_h$ be all non-isomorphic irreducible representations of group G. Let $\chi_1, ..., \chi_h$ be its corresponding character function, and $n_1, n_2, ..., n_h$ be the degree of the representations. Let R be the regular representation of G, $r_G$ be its character function, and let $g = dim(R) = |G|$. Hence, $r_G(1) = g$, and $r_G(s) = 0$ for $s \neq 1$.

**Theorem 2.20.** *Every irreducible representation $W_i$ is contained in the regular representation with multiplicity equal to its degree $n_i$.*

*Proof.* By 2.19, number of irreducible representations that are isomorphic to W in regular representation is equal to

$$< r_G, \chi_i >= \frac{1}{g} \sum_{t \in G} r_G(t) \chi_i(t^{-1}) = \frac{g}{g} \cdot \chi_i(1) = n_i$$

□

**Corollary 2.21.** *The degree $n_i$ satisfy the relation: $\sum_{i=1}^{h} n_i^2 = g$*

*Proof.* By 2.20, for $s \in G$, $r_G(s) = \sum_i \chi_i(s) n_i$. Plugging in $s = 1$ to the equation, we get

$$\sum_{i=1}^{h} n_i^2 = r_G(1) = g$$

□

**Corollary 2.22.** *If $s \in G$ is different from 1, we have $\sum_{i=1}^{r} n_i \chi_i(s) = 0$*

*Proof.* Plugging in $s \neq 1$ to the equation in the last proof, we get

$$\sum_{i=1}^{r} n_i \chi_i(s) = r_G(s) = 0$$

□

**Lemma 2.23.** *Let $f$ be a class function on $G$, and $\rho : G \to GL(V)$ be a linear representation of $G$. Define $\rho_f : V \to V$ as*

$$\rho_f = \sum_{t \in G} f(t) \rho_t$$

*If $\rho$ is irreducible of degree $n$ and character $\chi$, $\rho_f = \lambda I$, where $\lambda = \frac{g}{n}(f|\chi^*)$.*

*Proof.* Suppose $\rho : G \to GL(V)$ is irreducible representation of degree n with character $\chi$. It is easy to verify that $\forall s \in G$, $\rho_s \rho_f = \rho_f \rho_s$. By Schur's lemma, $\rho_f = \lambda I$. By construction of $\rho_f$, we have

$$n\lambda = Tr(\rho_f) = \sum_{t \in G} f(t) \chi(t) = g(f|\chi^*)$$

Hence, $\lambda = \frac{g}{n}(f|\chi^*)$. □

**Theorem 2.24.** *Let $H$ be the space of class functions on $G$. Then, $\{\chi_1, \chi_2, .., \chi_h\}$ form an orthonormal basis of $H$.*

*Proof.* Theorem 2.18 shows that $\chi_i$ is orthonormal and linearly independent in $H$. It remains to prove that they generate $H$. Since $\chi_i^*$ is spanned by $\chi_i$, it is enough to show that for every $f \in H$ orthogonal to $\chi_i^*$ for all i, $f = 0$. Let $f \in H$ and $(f|\chi_i^*) = 0$ for all i. Let $\rho$ be a representation of $G$, and $\rho_f = \sum_{t \in G} f(t)\rho_t$. By 2.23, $\rho_f = 0$ if $\rho$ is irreducible. From direct sum composition, we conclude that $\rho_f$ is always zero. Now, suppose $\rho : G \to GL(V)$ is the regular representation of degree n. Let $(e_t)_{t \in G}$ be the basis of V that is indexd by $t \in G$ and $e_1$ corresponds to $1 \in G$. We have

$$\rho_f e_1 = \sum_{t \in G} f(t)\rho_t e_1 = \sum_{t \in G} f(t)e_t$$

Since $\rho_f = 0$, we have $f(t) = 0$ for all $t \in G$. Hence, $f = 0$. $\square$

**Theorem 2.25.** *Number of irreducible representations (up to isomorphism) of $G$ is equal to number of conjugacy classes in $G$.*

*Proof.* Let $C_1, ..., C_k$ be the conjugacy classes in G. Let $f_i$ be the class function on G such that $f_i(x) = 1\ \forall x \in C_i$, and 0 for all other elements. It is easy to verify that $f_1, ...f_k$ forms a basis of the space $H$. By 2.24, $\chi_1, ...\chi_h$ also forms a basis of $H$, we have $h = k$. Hence, the number of irreducible representations of G is equal to number of conjugacy classes in G. $\square$

## 2.3. **Real Representation.**

**Definition 2.26.** Let $\rho : G \to GL(V)$ be a representation of G over $\mathbb{C}$. We say $\rho$ is **realizable** over $\mathbb{R}$ if there is a G-invariant $\mathbb{R}-$subspace $V_0$ of $V$ such that $V = V_0 \oplus iV_0$. We say $(V, \rho)$ descends to $(V_0, \rho_0)$ where $\rho_0 = \rho/V_0$.

**Definition 2.27.** A **Hermitian scalar product** on V is a map: $V \times V \to \mathbb{C}$ denoted as $(x|y)$ satisfying, for $a, b \in \mathbb{C}, x, y \in V$,
1) $(ax|y) = a(x|y)$
2) $(x|by) = \overline{b}(x|y)$
3) $(x|y) = \overline{(y|x)}$
4) $(x|y)$ is biaddictive
$(x|y)$ is positive definite if $(x|x) > 0$ for all $x \in V, x \neq 0$.
$(x|y)$ is G-invariant if given a representation $\rho$, $(x|y) = (\rho_s x|\rho_s y)\ \forall s \in G$.

**Remark 2.28.** *Let $\rho : G \to GL(V)$ be a representation of $G$ over $\mathbb{C}$. Then $V$ admits a Hermitian positive definite scalar product that is G-invariant: Define a map $A : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$ by $A((x_1, ...x_n), (y_1, ..., y_n)) = x_1\overline{y_1} + ... + x_n\overline{y_n}$. Then, $A$ is a positive definite hermitian product on $\mathbb{C}^n$. Let $\phi : V \to \mathbb{C}^n$ be an isomorphism of $\mathbb{C}$-vector spaces. We can construct a positive definite hermitian product $(x|y)$ on $V$ by*

$$(x|y) = A(\phi(x), \phi(y))$$

*Since $(x|y)$ is a positive definite hermitian product on V, we define*

$$(x,y) = \frac{1}{|G|}\sum_{g\in G}(\rho_g x|\rho_g y)$$

*which is a G-invariant positive definite hermitian scalar product on $V$.*

**Remark 2.29.** *Let $\rho : G \to GL(V)$ be a representation of $G$ over $\mathbb{C}$. Let $V^{'} = Hom(V,\mathbb{C})$ be the dual vector space. Define a linear representation $\rho^{'} : G \to GL(V^{'})$, for every $f \in V^{'}, v \in V$:*

$$\rho^{'}(s)(f)(v) = f(\rho^{-1}v)$$

*Let $B : V \times V \to \mathbb{C}$ be a G-invariant symmetric bilinear form. It induces a map:*

$$\tilde{B} : V \to V^{'} \text{ by } \tilde{B}(x)(y) = B(x,y)$$

*which is G-module homomorphism. For $g \in G, x, y \in V$,*

$$\tilde{B}(\rho_g x)(y) = B(\rho_g x, y) = B(x, \rho_g^{-1}y) = \tilde{B}(x)(\rho_g^{-1}y) = \tilde{\rho}_g\tilde{B}(x)(y)$$

*Hence, $\tilde{B}(\rho x) = \tilde{\rho}\tilde{B}(x)$.*

**Theorem 2.30.** *(Frobenius-Schur Theorem) Let $\rho : G \to GL(V)$ be a representation of $G$ over $\mathbb{C}$. Then, $\rho$ is realizable over $\mathbb{R}$ (2.26) if and only if there is a nonzero G-invariant symmetric bilinear form on V.*

*Proof.* Let $\rho : G \to GL(V)$ be a representation of G over $\mathbb{C}$.
We first prove the forward direction. Suppose $\rho$ is realizable over $\mathbb{R}$. By definition, there $\exists$ a $G$-invariant $\mathbb{R}$-subspace $V_0 \subseteq V$ such that $V = V_0 \oplus iV_0$. This implies every vector in $V$ can be written as $v_0 + v_1 i$, $v_0, v_1 \in V_0$
Suppose $\{v_1, ..., v_n\}$ is basis of the $\mathbb{R}$-subspace $V_0$. Let $\phi : V_0 \to \mathbb{R}^n$ map $\sum_i c_i v_i$ to $(c_1, c_2, ..., c_n)$. We have the scalar product on $\mathbb{R}^n$:

$$(x_1, ..., x_n) \cdot (y_1, ..., y_n) = \sum x_i y_i$$

Define $B_0^{'} : V_0 \times V_0 \to R$ by $B_0^{'}(x,y) = \phi(x)\cdot\phi(y)$. Since we are taking the inner product of two vectors, $B_0^{'}$ is a symmetric and bilinear form on $V_0$. We set $B_0 : V_0 \times V_0 \to R$ to be

$$B_0(x,y) = \frac{1}{|G|}\sum_{g\in G} B_0^{'}(\rho_g x, \rho_g y)$$

Then, we know that $B_0$ is a G-invariant symmetric bilinear form. We can extend $B_0$ to $B : V \times V \to R$ by

$$B(v_0 + v_1 i, w_0 + w_1 i) = B_0(v_0, w_0) - B_0(v_1, w_1) + i(B_0(v_0, w_1) + B_0(v_1, w_0))$$

We verify that $B$ is a nonzero symmetric bilinear G-invariant form on $V$ by the fact that $B_0$ is a nonzero symmetric bilinear G-invariant form on $V_0$.

Now, we prove the opposite direction. Suppose there is a symmetric bilinear G-invariant form $B : V \times V \to \mathbb{C}$. Then $B$ induces a $G$-isomorphism $\tilde{B} : V \to V'$ (2.29) by

$$\tilde{B}(x)(y) = B(x, y)$$

Step 1: Let $(x|y)$ be the G-invariant positive definite hermitian scalar product on V defined in 2.28. For $x \in V$, let $f_x : V \to \mathbb{C}$ be the map $f_x(y) = \overline{(x|y)}$. Check that $f$ is linear: for $\lambda \in \mathbb{C}$

$$f_x(\lambda y) = \overline{(x|\lambda y)} = (\lambda y|x) = \lambda(y|x) = \lambda\overline{(x|y)} = \lambda f_x(y)$$

Therefore, $f_x \in V'$, and we can define a map from $V \to V'$ by mapping x to $f_x$. We claim that this map is an isomorphism by proving the kernel is zero. Suppose $x \in V$ and $f_x(y) = 0 \ \forall y \in V$. This means $\overline{(x|y)} = (y|x) = 0 \ \forall y \in V$. Hence $(x|x) = 0$. Since the hermitian product is positive definite, we have $x = 0$. Therefore, $x \to f_x$ is an isomorphism.

Step 2: For $x \in V$, $\tilde{B}(x) \in V'$. Then, $\exists y \in V$ such that $f_y = \tilde{B}(x)$. We call this transform $y = \phi(x)$. Then the map $\phi : V \to V$ satisfies the following relationship:

$$B(x, y) = \tilde{B}(x)(y) = f_{\phi(x)}(y) = \overline{(\phi(x)|y)} \ \forall x, y \in V$$

First, we claim that $\phi$ is semilinear. For all $x, y \in V$,

$$B(\lambda x, y) = \overline{(\phi(\lambda x)|y)} = (y|\phi(\lambda x))$$

$$\lambda B(x, y) = \lambda\overline{(\phi(x)|y)} = \lambda(y|\phi(x)) = (y|\overline{\lambda}\phi(x))$$

Since B is bilinear, $B(\lambda x, y) = \lambda B(x, y)$. Hence, $(y|\phi(\lambda x)) - (y|\overline{\lambda}\phi(x)) = (y|\phi(\lambda x) - \overline{\lambda}\phi(x)) = 0$ implies that $\phi(\lambda x) = \overline{\lambda}\phi(x)$.
Second, we claim that $\phi$ and $\phi^2$ are both G-invariant. Since $(x|y)$ is G-invariant, we have:

$$B(x, y) = \overline{(\phi(x)|y)} = (y|\phi(x))$$

$$B(\rho_g x, \rho_g y) = \overline{(\phi(\rho_g x)|\rho_g y)} = (\rho_g y|\phi(\rho_g x)) = (y|\rho_g^{-1}\phi(gx))$$

Since $B$ is G-invariant, $B(x, y) = B(\rho_g x, \rho_g y)$. Hence, $\rho_g^{-1}\phi(\rho_g x) = \phi(x)$, and $\phi(\rho_g x) = \rho_g\phi(x)$. With the same deduction and the fact that $\phi$ is G-invariant, we get that $\phi^2$ is also G-invariant.
Third, we claim that $\phi^2$ is Hermitian symmetric. Since $B$ is symmetric, we have:

$$(y|\phi^2(x)) = \overline{(\phi^2(x)|y)} = B(\phi(x), y) = B(y, \phi(x)) = \overline{(\phi(y)|\phi(x))} = (\phi(x)|\phi(y))$$

For similar reasons,

$$(\phi^2(y)|x) = (\phi(x)|\phi(y))$$

Hence, $(y|\phi^2(x)) = (\phi^2(y)|x)$.
Last, we claim that $\phi^2$ is positive definite:

$$(\phi^2(x)|x) = (\phi(x)|\phi(x)) > 0 \text{ if } x \neq 0$$

Therefore, $\phi^2 : V \to V$ is a $\mathbb{C}$-linear, hermitian symmetric, positive definite, and G-invariant map.

Step 3: By 1.21, there $\exists$ $\mathbb{C}$-linear, hermitian symmetric, positive definite map $u : V \to V$, which is a polynomial in $\phi^2$ such that $\phi^2 = u^2$. Then, $u$ is G-invariant and commutes with $\phi$. Define $\sigma : V \to V$ by $\sigma = \phi u^{-1}$. Since $\phi$ and $u$ are both G-invariant, $\sigma$ is also G-invariant. Since $\phi$ is semilinear, and $u$ is linear, we get that $\sigma$ is semilinear. Because $u$ commutes with $\phi$, we have:

$$\sigma^2 = \phi u^{-1} \phi u^{-1} = \phi^2 u^{-2} = id$$

Therefore, $\sigma : V \to V$ is a semilinear automorphism G-invariant map with $\sigma^2 = id$. Considering $\sigma$ as an R-isomorphism, $\sigma$ is R-linear, and $\sigma^2 = id$. Hence, $\{1, -1\}$ are the only eigenvalues of $\phi$. The corresponding eigenspaces are:

$$V_0 = \{v \in V | \sigma(v) = v\}$$
$$V_1 = \{v \in V | \sigma(v) = -v\}$$

We have $V = V_0 \oplus V_1$. Further, $V_1 = iV_0$, so $V = V_0 \oplus iV_0$. Since $\sigma$ is G-invariant, $V_0$ is G-invariant, Therefore, $(V, \rho)$ is realizable over R from $(V_0, \rho_0)$ where $\rho_0 = \rho / V_0$. □

**Theorem 2.31.** *Let $\rho : G \to GL(V)$ be a representation of $G$ over $\mathbb{C}$, and $B$ be a symmetric bilinear form on $V$. Then, $B$ is G-invariant if and only if $\rho_g$ is orthogonal for every $g \in G$.*

**Remark 2.32.** *By Frobenius-Schur's theorem, and 2.31, those orthogonal representations are equivalent to real representations.*

**Theorem 2.33.** *Let $\rho : G \to GL(V)$ be an irreducible representation of $G$ over $\mathbb{C}$ of degree $n$, and let $X$ be its character. Define*

$$S = \frac{1}{g} \sum_{s \in G} \chi(s^2)$$

*Then, $S$ is equal to 1, -1, or 0.*

*Proof.*
Step 1: By theorem 2.9,

$$V \otimes V = Sym^2(V) \oplus Alt^2(V)$$

Let $\chi_\tau^2$, $\chi_\lambda^2$ be the character of $Sym^2(V)$ and $Alt^2(t)$ respectively. Then, for every $s \in G$

$$\chi_\tau^2(s) = \frac{1}{2}[\chi(s)^2 + \chi(s^2)]$$
$$\chi_\lambda^2(s) = \frac{1}{2}[\chi(s)^2 - \chi(s^2)]$$

Subtracting the bottom equation from the upper one, and summing it over every s, we get

$$\sum_s \chi(s^2) = \sum_s (\chi_\tau^2(s) - \chi_\lambda^2(s))$$

By definition,

$$S = \frac{1}{g}\sum_{s\in G}\chi(s^2) = < 1, \chi_\tau^2 > - < 1, \chi_\lambda^2 >$$

By 2.19, $< 1, \chi_\tau^2 >$ is the number of times the irreducible trivial representation occurs in $Sym^2(V)$, and $< 1, \chi_\lambda^2 >$ is that of $Alt^2(V)$.

Step 2: Suppose $\phi$ is a G-invariant bilinear form on $V$, then $\phi$ is either symmetric or alternating.

*Proof.* The G-invariant bilinear form $\phi$ induces G-homomorphism $\tilde{\phi} : V \to V'$ by $\tilde{\phi}(x)(y) = \phi(x, y)$. Suppose $\exists$ another G-invariant bilinear form $\psi$, it induces $\tilde{\psi} : V \to V'$, which is also a G-isomorphism. Hence, $\tilde{\psi}^{-1}\tilde{\phi} : V \to V$ is an G-automorphism, which implies it commutes with $\rho_s$ for all $s \in G$. By Schur's Lemma, $\tilde{\psi}^{-1}\tilde{\phi} = \lambda I$ and $\tilde{\phi} = \lambda\tilde{\psi}$. Therefore, $\phi$ is unique upto homothety.

Since $\phi$ is bilinear on $V$, it induces a homomorphism $V \otimes V \to \mathbb{C}$. Hence, we can consider $\phi$ as living in the vector space $V' \otimes V'$. By 2.29 and 2.9, we can define a representation on the vector space with the following decomposition:

$$V' \otimes V' = Sym^2(V') \oplus Alt^2(V')$$

We can write $\phi = \phi_+ + \phi_-$ with $\phi_+$ symmetric and $\phi_-$ alternating, then $\phi_+$ and $\phi_-$ are also G-invariant bilinear forms. Since $\phi$ is unique upto scalar, we have either $\phi_+ = 0$ ($\phi$ is alternating) or $\phi_- = 0$ ($\phi$ is symmetric).

□

Step 3: There exists a G-invariant symmetric (alternating) bilinear form $\phi$ on $V$ if and only if there is an irreducible trivial representation in symmetric (alternating) square of $V'$.

*Proof.* If $\phi$ is symmetric, $\phi \in Sym^2(V')$. Since $\phi$ is G-invariant, $\rho_s(\phi) = \phi$ for all $s \in G$. Therefore, we find a irreducible trivial representation W spanned by $\{\phi\}$ in $Sym^2(V')$. We omit the other way around since it is similar. □

Suppose there is a G-isomorphism $\tilde{\phi} : V \to V'$, the number of trivial representations in symmetric square of $V'$ is the same as that of $V$. Combining Step 2, and Step 3, we exhaust all possibilities with the following three cases:
case 1: G does not have a nonzero invariant bilinear form on V. In this case, there is no irreducible trivial representation in symmetric or alternating square of V. Hence, $S = 0 - 0 = 0$
case 2: G has a symmetric nonzero invariant bilinear form on V. In this case, there is a trivial representation in $Sym^2(V)$, and it is unique. Hence, $S = 1 - 0 = 1$
case 3: G has an alternating nonzero invariant bilinear form on V. In this case, there is a trivial representation in $Atl^2(V)$, and it is unique. Hence, $S = 0 - 1 = -1$. □

**Corollary 2.34.** *An irreducible representation $V$ comes from a real representation if and only if $S = 1$.*

*Proof.* First, suppose $V$ comes from a real representation, then by the Frobenius-Schur theorem (2.30), $\exists$ G-invariant symmetric bilinear form on V over $\mathbb{C}$. By 2.33, this is in according to case 2, and $S = 1$. Now, we prove the other way around. Suppose $S = 1$, there is an irreducible trivial representation in symmetric square of V, and $\exists$ G-invariant symmetric bilinear form on V. Hence, $V$ comes from a real representation. $\square$

**Corollary 2.35.** *When $S = 0$ or -1, there exists an irreducible representation of $G$ over $\mathbb{R}$ of degree 2n.*

*Proof.* Let $\rho : G \to GL_n(\mathbb{C})$ be a irreducible representation of G with $S = 0$ or $-1$. It induces $\tilde{\rho} : G \to GL_{2n}(\mathbb{R})$ by mapping $\rho(g) = A + iB$ to $\tilde{\rho}(g) = \begin{pmatrix} A & -B \\ B & A \end{pmatrix}$. Claim that $\tilde{\rho}$ is an irreducible real representation. Suppose $\tilde{\rho}$ is not irreducible, then $\exists V_0 \subseteq \mathbb{R}^{2n}$, $V_0 \neq 0$, $V_0 \neq \mathbb{R}^{2n}$ that is G-invariant, i.e. $\tilde{\rho}(g)(V_0) \subseteq V_0$. We know that $\mathbb{C}^n = \mathbb{R}^{2n}$. Hence, $\rho(g)(V_0) \subseteq V_0$, and $\rho(g)(iV_0) = i\rho(g)(V_0) \subseteq iV_0$. Thus, $V_0 \oplus iV_0 \neq 0$ is a G-invariant $\mathbb{C}$-subspace of $\mathbb{C}^n$. Since $\mathbb{C}^n$ is irreducible, we have $V_0 \oplus iV_0 = \mathbb{C}^n$. This contradicts to the fact that $\rho$ does not come from a real representation. Therefore, $\tilde{\rho}$ is a real irreducible representation of G with degree 2n. $\square$

**Theorem 2.36.** *Given a group G. Every real irreducible representation of G occurs as one of the following:*
*1) $\rho : G \to GL_n(\mathbb{C})$: a complex irreducible representation which comes from a real representation. The dimension of the real representation is n.*
*2) $\rho : G \to GL_n(\mathbb{C})$: a complex irreducible representation which does not come from a real representation. Then $\tilde{\rho} : G \to GL_{2n}(\mathbb{R})$ is a real irreducible representation and $dim(\tilde{\rho}) = 2n$.*

This theorem uses the decomposition of the semisimple algebra $\mathbb{R}[G]$ as a product of simple algebra of the form $M_n(\mathbb{R})$, $M_n(\mathbb{C})$, or $M_n(\mathbb{H})$, where $\mathbb{H}$ is the quaternion algebra, and every irreducible representation of $G$ corresponds to one of these simple algebras. We do not give a proof here of these results.

## 3. Burnside's Theorem

**Theorem 3.1.** *(Burnside) Let $G$ be a finite group of order $p^a q^b$, $a, b \in \mathbb{Z}^+$, $p$ and $q$ primes. Then $G$ is solvable. (1.4).*

The rest of the section is devoted to the proof of the theorem.

**Lemma 3.2.** *For every character $\psi$ of the finite group $G$, $\psi(x)$ is an algebraic integer for all $x \in G$*

*Proof.* Given $x \in G$, let its matrix representation be $\rho_x$. Since $G$ is finite, we can assume the order of $x$ is $k$, then $(\rho_x)^k = I$. $\rho_x$ can be written as $AJA^{-1}$, where J is in Jordan canonical form, thus, a lower triangular. $\psi(x) = Tr(\rho_x) = Tr(J)$. Since $(\rho_x)^k = I$, $J^k = I$, and $J_{ii}^k = 1$ for $i = 1, .., n$, implying that $J_{ii}$ is a root of $x^k - 1$. Thus, $J_{ii}$ is an algebraic integer, and $Tr(J) = \sum_1^n J_{ii}$ is also an algebraic integer by 1.14. Therefore, $\psi(x)$ is an algebraic integer. $\square$

Given a group G, let $\chi_1$,$\chi_2$, ..., $\chi_r$ be all the characters of the distinct irreducible representations of G. Let $K_1$, $K_2$, ..., $K_r$ be the conjugacy classes of G. Let $\phi_i$ be the matrix representation of irreducible representations with character $\chi_i$.

**Theorem 3.3.** *Define a complex valued function $\omega_i$ on $\{K_1, K_2, .., K_r\}$ for each $i$ by*

$$\omega_i(K_j) = \frac{|K_j|\chi_i(g)}{\chi_i(1)}$$

*where $g$ is any element of $K_j$. Then $\omega_i(K_j)$ is an algebraic integer for all $i$ and $j$.*

*Proof.* Let $X = \sum_{g\in K_j} \phi_i(g)$. For any element p in G,

$$\phi_i(p)^{-1}X\phi_i(p) = \sum_{g\in K_j} \phi_i(p^{-1})\phi_i(g)\phi_i(p) = X$$

since every element of form $p^{-1}gp$ is in the conjugacy class $K_j$. Thus, X commutes with $\phi_i(p)$ for all p. Since $X$ is a linear mapping from a vector space to itself, by Schur's lemma 2.12, $X = \alpha I$ for some $\alpha \in \mathbb{C}$.

$$\alpha \cdot \chi_i(1) = tr(X) = \sum_{g\in Kj} tr(\phi_i(g)) = |K_j|\chi_i(g)$$

From this equality, we conclude that $\alpha = \frac{|K_j|\chi_i(g)}{\chi_i(1)}$ and $X = \omega_i(K_j)I$.
Substituting $\omega_i(K_j)$ with $X$, we get, for all $i, j, t$ in 1,2,..,r:

$$\omega_t(K_i)\omega_t(K_j)I = (\sum_{g\in K_i} \phi_t(g))(\sum_{g\in K_j} \phi_t(g)) = \sum_{g_i\in K_i}\sum_{g_j\in K_j} \phi_t(g_ig_j) = \sum_{s=1}^{r}\sum_{g\in K_s} a_{ijs}\phi_t(g)$$

where $a_{ijs}$ is the the number of pairs of $(g_i, g_j)$ such that $g_ig_j = g$, g in $K_s$. This value is independent of choice of g because for other elements in $K_s$ of form $xgx^{-1}$, $xg_ix^{-1}$, and $xg_jx^{-1}$ will pair up and return such an element (vice versa). We apply this property to the equation above,

$$\omega_t(K_i)\omega_t(K_j)I = \sum_{s=1}^{r} a_{ijs} \sum_{g\in K_s} \phi_t(g) = \sum_{s=1}^{r} a_{ijs}\omega_t(K_s)I$$

Hence, $\omega_t(K_i)\omega_t(K_j) = \sum_{s=1}^{r} a_{ijs}\omega_t(K_s)$.
Thus, the ring $M = \mathbb{Z}[\omega_t(K_1), \omega_t(K_2), ..., \omega_t(K_r)]$ is a finitely generated $\mathbb{Z}$-module, generated by $1, \omega_t(K_1), ..., \omega_t(K_r)$. Since $\mathbb{Z}$ is Noetherian, and $\mathbb{Z}[\omega_t(K_i)]$ is a submodule of M, it is also finitely generated. By 1.12, $\omega_t(K_i)$ is an algebraic integer for all t and i.

□

**Corollary 3.4.** $\chi_i(1)$ *divides* $|G|$ *for all* $i = 1, 2, .., r$

*Proof.* Since $\chi_i(g_j)$ and $\chi_i(g_j)^*$ is the same for every element $g_j \in K_j$, we have

$$\begin{aligned}\frac{|G|}{\chi_i(1)} &= \frac{|G|}{\chi_i(1)}(\chi_i|\chi_i)\\ &= \sum_{j=1}^{r} \frac{|K_j|\chi_i(g_j)\chi_i(g_j)^*}{\chi_i(1)}\\ &= \sum_{j=1}^{r} \omega_i(K_j)\chi_i(g_j)^* = \sum_{j=1}^{r} \omega_i(K_j)\chi_i(g_j^{-1})\end{aligned}$$

By 3.2, $\chi_i(g_j^{-1})$ is an algebraic integer, and by 3.3, $\omega_i(K_j)$ is also an algebraic integer. Thus, the right hand side is an algebraic integer (1.14). Since the left hand is rational, it is an integer (1.15). □

**Lemma 3.5.** *If $G$ is any group with conjugacy class $K$ and an irreducible matrix representation $\phi$ with character $\chi$ such that $gcd(|K|, \chi(1)) = 1$, then for $g \in K$, either $\chi(g) = 0$ or $\phi(g)$ is a scalar matrix.*

*Proof.* By hypothesis, $\exists s, t \in \mathbb{Z}$ such that $s|K| + t\chi(1) = 1$. Pick $g \in K$, and multiplying both sides by $\chi(g)$, and dividing both sides by $\chi(1)$, we get

$$s\omega(K) + t\chi(g) = \frac{\chi(g)}{\chi(1)}$$

We know that the left side is an algebraic integer. Thus, $a_1 = \frac{\chi(g)}{\chi(1)}$ is also an algebraic integer. Let $p(x)$ be the minimal polynomial of $a_1$ over $Q$. Let $a_1, a_2, .., a_m$ be roots of $p(x)$. Let $n = \chi(1)$, then $a_1 = \frac{\lambda_1+\lambda_2+...+\lambda_n}{\chi(1)}$, where $\lambda_i$ is an eigenvalue of $\phi(g)$ for each i from 1 to n, and $|\lambda_i| = 1$ by 2.4. Thus, $|a_1| \leq 1$, and so are $a_i$ for all i. Now, we go back and find $minipoly_Q(a_1) = (x - a_1)(x - a_2)...(x - a_m) \in \mathbb{Q}[x]$, which means the constant term of the polynomial is a rational number. Thus, $b = \Pi_{i=1}^{m} a_i$ is rational, and by 1.15, an integer as well. Further, $|b| \leq 1$ since $|a_i| \leq 1$ for all i.
(case 1) $b = 0 \Rightarrow a_1 = 0 \Rightarrow \chi(g) = 0$
(case 2) $b = \pm 1 \Rightarrow |a_i| = 1$ for all i $\Rightarrow |\chi(g)| = \chi(1)$. Since $\phi(g)^l = id$ for some l, $\phi(g)$ is a diagonalizable matrix. Let $C =< \epsilon_1, \epsilon_2, ..., \epsilon_n >$ be a diagonal matrix conjugate to $\phi(g)$. If there exists $i, j$ such that $\epsilon_i \neq \epsilon_j$, then $|\chi(g)| = |\epsilon_1 + ... + \epsilon_n| < n$ by triangle inequality, which contradicts to $|\chi(g)| = \chi(1)$. Thus, $C = \epsilon I$. Since $\phi(g)$ is similar to C, $\phi(g) = \epsilon I$.

□

**Lemma 3.6.** *If $|K|$ is a power of a prime for some nonidentity conjugacy class $K$ of $G$, then $G$ is not a non-abelian simple group.*

*Proof.* Suppose G is a non-abelian simple group and $|K| = p^c$ Let $g \in K$, $g \neq 1$
case 1: $c = 0 \Rightarrow |K| = 1 \Rightarrow \exists g \in Z(G), g \neq 1$. This contradicts to the fact that non-abelian simple group has a trivial center.
case 2: $c \neq 0$. Recall that $\chi_1, \chi_2, ..., \chi_r$ are the character functions of irreducible

representations of G. Assign $\chi_1$ to be the character of trivial representation. Pick $g \in G$, and $g \neq 1$. Then, by 2.22

$$0 = \sum_{i=1}^{r} \chi_i(1)\chi_i(g)$$
$$= 1 + \sum_{i=2}^{r} \chi_i(1)\chi_i(g)$$

Suppose $p$ divides $\chi_j(1)$ for all j such that $\chi_j(g) \neq 0$, then

$$0 = 1 + p \sum_j d_j \chi_j(g)$$

$$\sum_j d_j \chi_j(g) = -\frac{1}{p}$$

Left hand side of the equation is an algebraic integer. Thus, $-\frac{1}{p}$ is an algebraic integer, and an integer as well. Since $p$ is a prime number, this leads to a contradiction. The hypothesis is wrong: $\exists j$ such that p does not divide $\chi_j(1)$ and $\chi_j(g) \neq 0$. Thus, $gcd(p^c, \chi_j(1)) = 1 \Rightarrow$. By 3.5, $\phi_j(g)$ is a scalar matrix. Since G is a simple group, the normal subgroup of G, $ker(\phi_j) = \{1\}$, and $\phi_j$ is injective. For any $a \in G$

$$\phi_j(ag) = \phi_j(a)\phi_j(g) = \phi_j(g)\phi_j(a) = \phi_j(ga)$$

Then $ag = ga$, and $g \in Z(G)$, which contradicts to the fact that non-abelian simple group has a trivial center. Thus, we conclude that G is not a non-abelian simple group.

□

Proof of Burnside Theorem: Let G be a group of order $p^a q^b$. We prove the theorem by induction on $|G|$. If $p = q$ or if $a$ or $b$ is zero, then G is solvable (1.10). Otherwise, let G be a counterexample with minimal order, i.e. $G$ is a non solvable group of form $|G| = p^a q^b$, where $p, q$ are distinct primes and $a > 0, b > 0$, and $|G|$ is the least. Suppose G has a proper, nontrivial normal subgroup $N$. Thus, both $N$ and $G/N$ are solvable by induction hypothesis, and by (1.5), $G$ is solvable, which is not true. Hence, G is a non-abelian simple group. Let P be a p-Sylow group in G (1.2). $\exists g \in Z(P)$ such that $g \neq 1$ (1.3). By definition, $P \subseteq C_G(g)$. If $C_G(g) = G$, then $g \in Z(G)$. Since $g \neq 1$, G has a nontrivial normal subgroup $Z(G)$, which contradicts to G is simple. Hence, $C_G(g) \subsetneq G$, and $|C_G(g)| = p^a q^x$ with $x < b$. Thus, $|Cl(g)| = [G : C_G(g)] = q^{b-x}$, which means in $G$, there $\exists$ a nonidentity conjugacy class K, whose order is a power of a prime. By 3.6, $G$ is not a non-abelian simple group, and this leads to contradiction. This completes the proof of Burnside's Theorem.

## 4. On the Degree of $\alpha + \beta$

**Theorem 4.1.** *Let $F$ be a field of characteristic zero, and $L$ is a finite extension of $F$. Suppose $\alpha, \beta \in L$, $[F(\alpha) : F] = m$, and $[F(\beta) : F] = n$. Suppose that $m$, $n$ are coprime, then $F(\alpha, \beta) = F(\alpha + \beta)$.*

The rest of the section is devoted to the proof of the theorem.

Let $f(x) = minipoly_F(\alpha)$, $g(x) = minipoly_F(\beta)$. Then $deg(f(x)) = m$, and $deg(g(x)) = n$. Since $char(F) = 0$, $f$ and $g$ has no multiple zero. Let $A$, $B$ be the set of zeros of $f(x)$, $g(x)$ respectively. i.e. $A = \{\alpha = \alpha_1, ..., \alpha_m\}$, $B = \{\beta = \beta_1, ..., \beta_n\}$. Let $\overline{F}$ be the algebraic closure of F. Let $F(A), F(B), F(A, B)$ be the subfields of $\overline{F}$ generated by $A$, $B$, and $A \cup B$ respectively.

**Lemma 4.2.** *Let $H$ be $Aut(F(A)/F)$. Then $H$ acts transitively on $A$, i.e. given $(i, j)$, $\exists \sigma \in H$ such that $\sigma(\alpha_i) = \alpha_j$.*

*Proof.* Suppose $\alpha_i, \alpha_j$ are two distinct zeros in set A. Since $\alpha_i$, and $\alpha_j$ are zeros of the same irreducible polynomial $f(x) \in F[x]$, there is an F-isomorphism:

$$\phi : F(\alpha_i) \to F(\alpha_j)$$

such that $\phi(\alpha_i) = \alpha_j$ (1.17). Since $F(A)$ is a splitting field of $f(x)$ over $F$, we can extend $\phi$ to $\sigma : F(A) \to F(A)$, such that $\sigma|_{F(\alpha_i)} = \phi$. Hence, $\exists \sigma \in H$ such that $\sigma(\alpha_i) = \alpha_j$. And H acts transitively on A. ☐

**Lemma 4.3.** *Let $G$ be $Aut(F(A, B)/F)$. Then $G$ acts transitively on $A \times B$.*

*Proof.* First, show that $g(x)$ is irreducible in $F(\alpha)[x]$. Suppose $g = g_1 g_2$, where $g_1, g_2 \in F(\alpha)[x]$. Given that m, and n are coprime, by 1.18, we show that

$$[F(\alpha, \beta) : F(\alpha)] = \frac{[F(\alpha, \beta) : F]}{[F(\alpha) : F]} = \frac{mn}{m} = n$$

Since $\beta$ is a root of $g(x)$, $\beta$ is also a root of either $g_1(x)$ or $g_2(x)$. Suppose $\beta$ is a root of $g_1(x)$. Then $deg(g_1(x)) \geq$ degree of $minipoly_{F(\alpha)}(\beta) = [F(\alpha, \beta) : F(\alpha)] = n$. Thus, $deg(g(x)) = deg(g_1(x))$, and $g(x)$ is irreducible in $F(\alpha)[x]$. There is an F-isomorphism:

$$\phi : F(\alpha_i) \to F(\alpha_j)$$

such that $\phi(\alpha_i) = \alpha_j$ (1.17). Since $g(x)$ is irreducible in $F(\alpha_i)[x]$, and $\beta_r$, $\beta_t$ are zeros of $g(x)$, $\exists$ an isomorphism:

$$\psi : F(\alpha_i, \beta_r) \to F(\alpha_j, \beta_t)$$

such that $\psi(\beta_r) = \beta_t$, and $\psi|_{F(\alpha_i)} = \phi$ implying that $\psi(\alpha_i) = \alpha_j$. Since $F(A, B)$ is a splitting field of $f \cdot g$ over $F$, we can extend $\psi$ to $\sigma : F(A, B) \to F(A, B)$. Then, $\exists \sigma \in G$ such that $\sigma(\alpha_1) = \sigma(\alpha_2)$, and $\sigma(\beta_1) = \beta_2$ for arbitrary $\alpha_1, \alpha_2, \beta_1, \beta_2$. Thus, G acts transitively on $A \times B$. ☐

Let $V_A, V_B$ denote the F-subspace of $F(A, B)$ generated by A and B respectively. Let $G$ be $Aut(F(A, B)/F)$. Since $A$ is the set of zeros of an irreducible polynomial $f(x) \in F[x]$, $G$ permutes elements of $A$, and $V_A$ is a G-invariant subspace of $F(A,B)$, For the same reason, $V_B$ is a G-invariant subspace of $F(A,B)$. Hence, we can define the following representation

$$\rho_A : G \to GL(V_A)$$

$$\rho_B : G \to GL(V_B)$$

by $\rho_A(\sigma) = \sigma|_{V_A}$, and $\rho_B(\sigma) = \sigma|_{V_B}$.

**Lemma 4.4.** *Suppose $\phi : V_A \to V_B$ is a $G-homomorphism$, then it maps the entire module $V_A$ to the trivial G-module*

$$F \cdot (\beta_1 + ... + \beta_n)$$

*Proof.* Set $G_{\alpha_i} = \{\sigma \in G | \sigma(\alpha_i) = \alpha_i\}$. By 4.3, $G_{\alpha_i}$ acts transitively on $\{\alpha_i\} \times B$, i.e. given $(\alpha_i, \beta_j)$, and $(\alpha_i, \beta_k)$, there exists $\sigma \in G_{\alpha_i}$ such that

$$\sigma(\alpha_i, \beta_j) = (\alpha_i, \beta_k)$$

Suppose $\phi(\alpha_i) = c_1\beta_1 + ... + c_k\beta_k + ... + c_n\beta_n$, $c_i \in F$. Let $\sigma_k \in G_{\alpha_i}$ map $\alpha_i$ to $\alpha_i$, and $\beta_1$ to $\beta_k$. Since $\phi$ is a $F[G]-homomorphism$,

$$\begin{aligned}\phi(\alpha_i) = \phi(\sigma_k\alpha_i) = \sigma_k\phi(\alpha_i) &= c_1\sigma_k(\beta_1) + ... + c_n\sigma_k(\beta_n) \\ &= c_1\beta_k + c_2\sigma_k(\beta_2) + ... + c_n\sigma_k(\beta_n)\end{aligned}$$

Comparing the two different expressions for $\phi(\alpha_i)$, we get that $c_1 = c_k$. Varying k from 1 to n, we conclude that $c_1 = c_2 = ... = c_n$, and $\phi(\alpha_i) = c_1(\beta_1 + ... + \beta_n)$. This applies to $\alpha_i$ for $1 \le i \le m$. Therefore, $\phi(V_A) = F \cdot (\beta_1 + \beta_2 + ... + \beta_n)$, and the G action on $F \cdot (\beta_1 + \beta_2 + ... + \beta_n)$ is trivial. □

Proof of 4.1: Suppose that $F(\alpha + \beta) \subsetneq F(\alpha, \beta)$. This implies

$$|Aut(F(\alpha, \beta)/F(\alpha + \beta))| = [F(\alpha, \beta) : F(\alpha + \beta)] \ge 2$$

and we can pick $\sigma \in G$, $\sigma \ne id$ such that $\sigma(\alpha + \beta) = \alpha + \beta$, but $\sigma(\alpha) \ne \alpha$, or $\sigma(\beta) \ne \beta$. In this case, $\sigma(\alpha) \ne \alpha$ and $\sigma(\beta) \ne \beta$. Set $\delta$ to be $\sigma(\alpha) - \alpha = \beta - \sigma(\beta) \ne 0$. We claim that $\delta \notin F$. Suppose $\delta \in F$, and $\sigma$ is of order $l$ in G. Then,

$$\sigma^l(\alpha) = \sigma...\sigma(\alpha + \delta) = \sigma...\sigma(\alpha + \delta + \delta) = \alpha + l\delta = \alpha$$

Since $char(F) = 0$, $l \ne 0$, we get $\delta = 0$. But $\delta \ne 0$, so $\delta \notin F$.

Let $U$ be the F-subspace of $F(A,B)$ spanned by $\{g\delta, g \in G\}$. We have $\delta = \sigma(\alpha) - \alpha \in V_A$. For every $g \in G$, $g\delta \in V_A$ since $V_A$ is G-invariant, hence, $U \subseteq V_A$. Further, $U$ is a G-invariant subspace of $V_A$. Since $char(F) = 0$, we have a direct sum decomposition $V_A = U \oplus V_A'$ by 2.5. Since $\delta = \beta - \sigma(\beta) \in V_B$, $U \subseteq V_B$ is G-invariant, and $V_B = U \oplus V_B'$. Let $p : V_A \to U$ be the projection which is a G-homomorphism. Composing p with the inclusion mapping $q : U \to V_B$, we get a G-homomorphism $\phi : V_A \to V_B$ whose image is $U$. By 4.4, $U \subseteq F \cdot (\beta_1 + ... + \beta_n)$. Since $F \cdot (\beta_1 + ... + \beta_n)$ has trivial G-action, $U$ has trivial G-action. Hence, $g\delta = \delta$ for all $g \in G$, and $\delta \in F$ which leads to a contradiction. Therefore, $F(\alpha, \beta) = F(\alpha + \beta)$.

## 5. Eckmann's proof on Hurwitz's Theorem

We want to find n bilinear forms $z_1, ..., z_n$ in $x_1, ...x_p$, and $y_1, , , , y_n$ with complex coefficients such that the following equation holds:

$$(x_1^2 + x_2^2 + ... + x_p^2)(y_1^2 + y_2^2 + ... + y_n^2) = z_1^2 + ... + z_n^2 \tag{2}$$

**Theorem 5.1.** *Let $n = u \cdot 2^{4\alpha+\beta}$, where $u$ is odd, and $\beta = 0, 1, 2, 3$, there exists complex solutions to equation (2) if and only if $p \leq 8\alpha + 2^\beta$. Further, we can choose the solutions to be real.*

*Proof.* Step 1: Suppose the original equation has solutions. Then we can express $z_k$ as $\sum\limits_{1\leq i\leq p, 1\leq j\leq n} a_{ij}^k x_i y_j$ for $k = 1, .., n$. Now, we construct matrices with the coefficients of the solutions: $[A_k]_{ij} = a_{ki}^j$ and $A_k$ is a $n \times n$ matrix. By equation (2), for a fixed pair of $i$ and $j$, we know that $\sum\limits_{1<k<n} a_{ij}^k = 1$ since the coefficients before $(x_i y_j)^2$ is 1. On the other hand, the coefficients of every other possible term is 0, so we get that $A_k A_k^T = I$, which is equivalent to saying $A_k$ is orthogonal for $k = 1, ...p$. We also get the following equation:

$$A_k A_l^T + A_l A_k^T = 0, \quad k, l = 1, ..., p; \; k \neq l \tag{3}$$

Therefore, the original problem is equivalent to the following matrix problem: Find p complex orthogonal $n \times n$ matrices $A_1, ..., A_p$ that satisfy equation (3). The case p=1 is trivial, so we assume $p \geq 2$.

Now, we multiply all matrices with the orthogonal matrix $A_p^T$ and obtain a different solution to the problem, where the new $A_p$ is $I$, and $A_k^T + A_k = 0$ for $k = 1, ..., p-1$. Plugging $A_k^T = -A_k$ into equation (3):

$$A_k A_l + A_l A_k = 0, \quad k, l = 1, .., p-1; \; k \neq l$$

and because $A_k A_k^T = I$,

$$A_k^2 = -I, \;\; k = 1, ..., p-1$$

Therefore, it is sufficient to solve the problem in the following form: *Find p-1 complex orthogonal $n \times n$ matrices $A_1, ..., A_{p-1}$ such that the following relation is satisfied:*

$$A_k^2 = -I, \;\; A_k A_l = -A_l A_k, \quad k, l = 1, .., p-1; \; k \neq l \tag{4}$$

Step 2: We construct the group G, generated by p elements, $a_1, ..., a_{p-1}, \epsilon$ with the following relations:

$$\epsilon^2 = 1, \; a_k^2 = \epsilon, \; \epsilon a_k = a_k \epsilon, \; a_k a_l = \epsilon a_l a_k, \quad k, l = 1, ..., p-1; k \neq l$$

Then, the problem can be expressed as following: *We look for a complex orthogonal representations of G in which $\epsilon$ is mapped to -I.*

Step 3: All elements in group G can be listed as follows:

$$a_{k_1} a_{k_2} ... a_{k_r} \text{ and } \epsilon a_{k_1} a_{k_2} ... a_{k_r}, \quad r = 0, ..., p-1$$

where $k_i$ is a number from 1 to p-1 such that $k_1 < k_2 < ... < k_r$. Therefore, G is of order $2 \cdot 2^{p-1} = 2^p$.

For $p = 2$, G is the cyclic group of order 4, and there are 4 irreducible representations of G. Then, there exists real solutions to the original equation if and only if $n = 2m$. Take n=2 as an example:

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1y_1 + x_2y_2)^2 + (x_1y_2 - x_2y_1)^2$$

For bigger n, we pair up $y_i$ with $y_{i+1}$, and perform the same trick above. In conclusion, we only need to consider $p \geq 3$.

The set of commutators in G is $\{1, \epsilon\}$. The commutator subgroup K has order 2, and the abelian group G' = G/K has order $2^{p-1}$. Irreducible representations of an abelian group are in degree one. *Therefore, G has $2^{p-1}$ inequivalent representations of degree 1.*

Step 4: Let h be the number of conjugacy classes in G:

$$h = 2^{p-1} + 2 \text{ if p is even}$$

$$h = 2^{p-1} + 1 \text{ if p is odd}$$

*Proof.* case a) Let $g = a_{k_1}...a_{k_r}$, $1 \leq r \leq p-1$, in which r is even,

$$a_{k_1}^{-1} g a_{k_1} = \epsilon a_{k_1}(a_{k_1}...a_{k_r})a_{k_1} = (a_{k_2}...a_{k_r})a_{k_1} = \epsilon^{r-1} g = \epsilon g$$

There are no other elements that is conjugate to g since the $a_j$ conjugates of g do not change. Hence, the conjugacy class of an element g of such form including $a_1a_2...a_{p-1}$ (p odd) is $\{g, \epsilon g\}$.
case b) Let $g = a_{k_1}...a_{k_r}$, $1 \leq r \leq p-2$, in which r is odd, and we can choose $k$ to be a distinct number from $\{k_1, ..., k_r\}$,

$$a_k^{-1} g a_k = \epsilon a_k(a_{k_1}...a_{k_r})a_k = \epsilon\epsilon^r a_k^2 g = \epsilon^{r+2} g = \epsilon g$$

so the conjugacy class of an element g of such form is $\{g, \epsilon g\}$
Combining case a) and b), we get that when p is odd, $Z(G) = \{1, \epsilon\}$, and $g \neq 1$ or $\epsilon$ is conjugate to $\epsilon g$. Therefore,

$$h = 2 + (2^p - 2)/2 = 2^{p-1} + 1$$

Now, suppose p is even, case a) and b) do not cover the case when $g = a_1...a_{p-1}$. We show that $b^{-1}gb = g$ for all $b \in G$. It is sufficient to show that for all the generators:

$$a_k^{-1} g a_k = \epsilon a_k a_1 a_2 ... a_{p-1} a_k = \epsilon\epsilon^{p-2} a_k^2 a_1 a_2 ... a_{p-1} = \epsilon^p a_1 a_2 ... a_{p-1} = g$$

(Remark: the switch is one less since $a_k$ is the same as one of the terms in g)
So we get that $Z(G) = \{1, \epsilon, g, \epsilon g\}$, and

$$h = 4 + (2^p - 4)/2 = 2^{p-1} + 2$$

□

Step 5: By 2.25, h is the number of inequivalent irreducible representations of G. From Step 3, we know the number of degree 1 representations, so we get that when p is even, there are two inequivalent irreducible representations of

G of degree greater than 1 (degree denoted by $f, f'$), and when p is odd, there is only one such representation (degree denoted as $f$). By 2.21,
1) when p is odd,

$$f^2 + 2^{p-1} \cdot 1^2 = 2^p$$

so,

$$f = 2^{\frac{p-1}{2}}$$

2) when p is even,

$$f^2 + f'^2 + 2^{p-1} \cdot 1^2 = 2^p$$

so,

$$f^2 + f'^2 = 2^{p-1}$$

By 3.4, $f, f'$ divides $2^p$, so we let $f = 2^v$, and $f' = 2^u$. Plugging it into the equation above and get $u = v = \frac{p-1}{2}$, $f = f' = 2^{\frac{p-2}{2}}$

Step 6: Since representations of degree 1 map $\epsilon$ to the identity, we only consider irreducible representations $\rho$ of degree greater than 1. They do not map $\epsilon$ to I, because $G' = G/(1, \epsilon)$ is abelian, and representations of $G'$ are of degree 1. Since $\epsilon$ is in the center, $\rho(\epsilon)\rho(g) = \rho(g)\rho(\epsilon)$ for all $g \in G$ and $\rho(\epsilon)$ is a G-homomorphism that maps V to V. Hence, by Schur's Lemma, $\rho(\epsilon) = \lambda I$, $\lambda \in \mathbb{C}^*$. Since $\epsilon^2 = 1$, we have $\lambda^2 = 1$, and $\lambda = -1$. Therefore, irreducible representations of G of degree larger than one map $\epsilon$ to $-I$.

For odd p, there exists only one inequivalent irreducible representation of higher degree: $2^{\frac{p-1}{2}}$. For even p, there are two irreducible representations of higher degree: $2^{\frac{p-2}{2}}$. Since we only consider $p > 2$, $\frac{p-2}{2} > 0$, and the degree is greater than 1. For an arbitrary representation of $G$ that maps $\epsilon$ to $-I$, it can be decomposed into direct sum of irreducible representations, each of degree greater than 1, mapping $\epsilon$ to $-I$:

$$V = W_1 \oplus W_2 \oplus ... \oplus W_m$$

Let the degree of representation be n, then the following equations hold:

$$n = m \cdot 2^{\frac{p-1}{2}} \text{ when p is odd}$$

$$n = m \cdot 2^{\frac{p-2}{2}} \text{ when p is even}$$

Suppose $n = u \cdot 2^t$, where u is odd. Then $G$ has representations that maps $\epsilon$ to $-I$ if and only if $\frac{p-1}{2} \leq t$ when p is odd, and $\frac{p-2}{2} \leq t$ when p is even. After simplification, $G$ has such representations if and only if $p \leq 2t + 2$. In other words:

*Let $n = u \cdot 2^t$ with odd u, there exists p-1 complex $n \times n$ matrices $A_1, ..A_{p-1}$, that satisfy equation (4) if and only if $p \leq 2t + 2$.*

Step 7: We now look for representations of G which are equivalent to orthogonal representations. By the remark of Frobenius-Schur theorem 2.30, those orthogonal representations are equivalent to real representations. Every solution of the representation problem is thus equivalent to a real solution to the original problem.

Let $\chi$ be the character function of a complex irreducible representation D of G of degree (denoted as f) larger than 1. We define:

$$S = \frac{1}{|G|} \sum_{g \in G} \chi(g^2)$$

S can only be 1, -1, or 0. (2.33) When $S = 1$, $D$ comes from a real representation (2.34). When $S = -1$, $D$ is not equivalent to a real representation, but we can construct an irreducible real representation of degree $2f$ from $D$. If S=0, $\chi(D)$ is not real, but we can again construct an irreducible real representation of degree $2f$ from $D$ (2.35). The representations described above are all real irreducible representations of G (2.36).

For an arbitrary element g $\in$ G,

$$g = a_{k_1} a_{k_2} ... a_{k_r} \text{ or } g = \epsilon a_{k_1} a_{k_2} ... a_{k_r}$$

so,

$$g^2 = (a_{k_1} a_{k_2} ... a_{k_r})^2 = \epsilon^{r+r-1+...+2+1} = \epsilon^{\frac{r(r+1)}{2}}$$

so,

$$g^2 = 1 \text{ if } r \equiv 3, 0 \mod 4$$
$$g^2 = \epsilon \text{ if } r \equiv 1, 2 \mod 4$$

Since the irreducible representation $D$ maps $\epsilon$ to $-I$, we have:

$$\text{for } r \equiv 3, 0 \mod 4, \ \chi(g^2) = f$$

$$\text{for } r \equiv 1, 2 \mod 4, \ \chi(g^2) = -f$$

Summing over $2^p$ elements of G, we have

$$S = \frac{2}{|G|}[f - f \cdot \text{number of choices of } (a_{k_1}) - f \cdot \text{number of choices of } (a_{k_1} a_{k_2}) - f \cdot \text{number of choices of } (a_{k_1} a_{k_2} a_{k_3}) + ...]$$

We simplify the equation and get:

$$S = \frac{2f\sigma}{|G|}$$

where

$$\sigma = \binom{p-1}{0} - \binom{p-1}{1} - \binom{p-1}{2} + \binom{p-1}{3} + \binom{p-1}{4} - -... \pm \binom{p-1}{p-1}$$

To compute the sign of $\sigma$, we construct the complex number

$$z = (1-i)^{p-1} = x + iy, \text{ x,y are real}$$

Expanding the polynomial, we get that $\sigma = x + y$. Since $argz = -\frac{\pi}{4}(p-1)$, we can determine the sign of $\sigma$:

$$\sigma > 0, if -\frac{\pi}{4}(p-1) \equiv 0, \frac{\pi}{4}, \frac{2\pi}{4} (\text{mod } 2\pi)$$
$$\sigma = 0, if -\frac{\pi}{4}(p-1) \equiv \frac{3\pi}{4}, \frac{7\pi}{4} (\text{mod } 2\pi)$$
$$\sigma < 0, if -\frac{\pi}{4}(p-1) \equiv \frac{4\pi}{4}, \frac{5\pi}{4}, \frac{6\pi}{4} (\text{mod } 2\pi)$$

Therefore, $S = 1$ for p $\equiv$ 7,0,1 (mod 8), $S = -1$ for p $\equiv$ 3,4,5 (mod 8), and $S = 0$ for p $\equiv$ 2,6 (mod 8). Combining the property we said about $S$, we get:

*When p $\equiv$ 7,0,1 (mod 8), D of degree f is a real irreducible representation; otherwise, there exists a real irreducible representation of degree 2f that comes from D.*

Step 8: The degree n of an irreducible real representation that maps $\epsilon$ to $-I$ is given by:

$$(5) \quad \begin{aligned} &a) \text{ for } p \equiv 7, 1 (\text{mod } 8), \text{ p is odd, } n = f = 2^{\frac{p-1}{2}} \\ &b) \text{ for } p \equiv 0 (\text{mod } 8), \text{ p is even, } n = f = 2^{\frac{p-2}{2}} \\ &c) \text{ for } p \equiv 3, 5 (\text{mod } 8), \text{ p is odd, } n = 2f = 2 \cdot 2^{\frac{p-1}{2}} = 2^{\frac{p+1}{2}} \\ &d) \text{ for } p \equiv 2, 4, 6 (\text{mod } 8), \text{ p is even, } n = 2f = 2 \cdot 2^{\frac{p-2}{2}} = 2^{\frac{p}{2}} \end{aligned}$$

Complex orthogonal representations of G of degree $n = m \cdot 2^s$ for which $\epsilon$ is assigned to -I exists in the following cases:

$$(6) \quad \begin{aligned} &a) p \equiv 7, 1 (\text{mod } 8),\ 2^s = 2^{\frac{p-1}{2}} \rightarrow s \equiv 3, 0 \text{ (mod 4) and } p = 2s + 1 \\ &b) p \equiv 0 (\text{mod } 8),\ 2^s = 2^{\frac{p-2}{2}} \rightarrow s \equiv 3 \text{ (mod 4) and } p = 2s + 2 \\ &c) p \equiv 3, 5 (\text{mod } 8),\ 2^s = 2^{\frac{p+1}{2}} \rightarrow s \equiv 2, 3 \text{ (mod 4) and } p = 2s - 1 \\ &d) p \equiv 2, 4, 6 (\text{mod } 8),\ 2^s = 2^{\frac{p}{2}} \rightarrow s \equiv 1, 2, 3 \text{ (mod 4) and } p = 2s \end{aligned}$$

Suppose the degree of an arbitrary orthogonal complex representation that maps $\epsilon$ to $-I$ is $n = u \cdot 2^t$, with u odd. We can find the greatest possible number p by solving for $s \leq t$. Take $t = 4\alpha$ as an example. Let $s = t$, $s \equiv 0$ (mod 4), and by case a), $p = 2s+1 = 2t+1 = 8\alpha+1$. Let $s = 4\alpha - 1$, $s \equiv 3$ (mod 4), and by case b), $p = 2s + 2 = 2(4\alpha - 1) + 2 = 8\alpha$. Hence, the greatest possible p for $t = 4\alpha$ is $8\alpha + 1$. Applying the steps above to each case below and we get:

$$(7) \quad \begin{aligned} &\text{for } t = 4\alpha : p = 2t + 1 = 8\alpha + 1 \\ &\text{for } t = 4\alpha + 1 : p = 2t = 8\alpha + 2 \\ &\text{for } t = 4\alpha + 2 : p = 2t = 8\alpha + 4 \\ &\text{for } t = 4\alpha + 3 : p = 2t + 2 = 8\alpha + 8 \end{aligned}$$

We conclude:

*Suppose $n = u \cdot 2^{4\alpha+\beta}$ with $u$ odd, and $\beta = 0, 1, 2, 3$, there exists p-1 complex orthogonal matrices satisfying equation (2) if and only if $p \leq 8\alpha + 2^{\beta}$. Those matrices can be chosen to be real.*

□

**Corollary 5.2.** *When $p = n$, there exists real solutions to the original problem if and only if $n = 1, 2, 4, 8$*

*Proof.* Plugging $p = n$ into the condition we concluded, we get that

$$u \cdot 2^{4\alpha+\beta} \leq 8\alpha + 2^{\beta}$$

case 1: $\alpha = 0$, $u \cdot 2^{\beta} \leq 2^{\beta}$, then $u = 1$, $\beta$ can be 0,1,2, or 3, and the corresponding n is $2^{\beta} = 1, 2, 4, 8$
case 2: $\alpha \geq 1$, the left hand is always larger than the right hand by induction. Therefore, the original problem has real solutions if and only if $n = 1, 2, 4, 8$.

□

**Remark 5.3.** *The composition law on $\mathbb{R}^n$ for $n = 1, 2, 4, 8$ is given by*

$$(x_1, ..., x_n) \cdot (y_1, ..., y_n) = (z_1, ..., z_n)$$

*where $z_i$ is the real solution found in corollary 5.2. Hence, composition algebra structure exists on $\mathbb{R}^n$ for n=1,2,4,8 and these are all the possible composition algebra.*

*We list all the composition algebra:*
*a) n=1: $\forall x, y \in \mathbb{R}$, $x \cdot y = xy$. This satisfies the composition algebra structure since $N(x)N(y) = N(xy)$ where $N(t) = t^2$*
*b) n=2: $\mathbb{C} = \mathbb{R} \oplus \mathbb{R}i$. $\forall x, y \in \mathbb{C}$, let $x = a + bi, y = c + di$,*

$$x \cdot y = (ac - bd) + (ad + bc)i$$

*This satisfies the composition algebra structure since $N(x)N(y) = N(xy)$ where $N(t) = t_1^2 + t_2^2$. i.e. $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$*
*c) n=4: $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}ij, ij = -ij$. $\forall x, y \in \mathbb{H}$, let $x = a + bi + cj + dk, y = e + fi + gj + hk$, $x \cdot y$ again satisfies the composition algebra structure given that $N(t) = t\bar{t}$.*
*d) n=8: It is called the Octonion algebra. It is obtained by doubling $\mathbb{H} : \mathbb{O} = \mathbb{H} \oplus p\mathbb{H}$. We omit the discussion of the exact group structure here.*

## References


[1] David S. Dummit, Richard M. Foote, *Abstract Algebra*, John Wiley and Sons, 2004.
[2] S.H. Friedberg, A.J. Insel, *Linear Algebra*, Pearson 1979.
[3] J.P. Serre, *Linear Representation of finite groups*, Springer, 1977.
[4] B. Eckmann, *Gruppentheoretischer Beweis des Satzes von Hurwitz-Radon über die Komposition quadratichen Formen*, Comment. Math. Helv. 15 (1942), 358-366
[5] I.M. Isaacs, *Degree of a Sum in a Separable Field Extension*, Proc. A.M.S. **25** (1970), 638–641.