Let G be a group, $\mathbb{F}$ a field, and V be a finite dimensional vector space over $\mathbb{F}$.
All morphisms act on the right unless specified otherwise. So if $f : A \longrightarrow B$ is a morphism (function), then we denote the image of $a \in A$ under f by af.

Definition

An $\mathbb{F}$-algebra is a finite dimensional $\mathbb{F}$ vector space A which admits a ring structure with identity 1_A such that for all $\lambda \in \mathbb{F}$ and $x, y \in A$ we have

$$\lambda(xy) = (\lambda x)y = x(\lambda y).$$

The formula in the definition of an $\mathbb{F}$-algebra is a compatibility condition between the scalar- and ring- multiplication of A.

We now give examples of F-algebras.
Example 1: The set of all linear transformations from V to itself denoted by $\mathrm{End}(V)$ is an algebra under the operations of addition, scalar multiplication and composition of functions. Specifically we define $\forall \lambda \in \mathbb{F}, x, y \in \mathrm{End}(V), v \in V$ that

$$v(x+y) := vx + vy$$

$$v(\lambda x) := \lambda(vx) = (\lambda v)x$$

$$v(xy) := (vx)y.$$

We denote the set of invertible elements (i.e. those possessing a multiplicative inverse) of $\mathrm{End}(V)$ by $\mathrm{GL}(V)$. We recall that the set of elements in a ring with identity which possess a multiplicative inverse always from a group, called the group of units. Thus we note that $\mathrm{GL}(V)$ is a group.

Example 2: The set $M_n(\mathbb{F})$ of all $n \times n$ matrices with coefficients in $\mathbb{F}$ where the operations are addition, scalar multiplication and multiplication of matrices. The group of units in this example is $\mathrm{GL}_n(\mathbb{F})$.
We recall that a fundamental result from linear algebra is that every linear transformation between finite dimensional vector spaces can be represented by a matrix. This suggests that $\mathrm{End}(V)$ and $M_n(\mathbb{F})$ might be isomorphic as algebras. This is in fact true. To see this we recall that representing a linear transformation $x : V_1 \longrightarrow V_2$ by a matrix requires a choice of bases $\mathcal{B}_i$ of V_i. The $\dim(V_1) \times \dim(V_2)$ matrix $M_{\mathcal{B}_1}^{\mathcal{B}_2}(x)$ representing x with respect to the pair of bases $\mathcal{B}_1$, $\mathcal{B}_2$ is defined as follows:
Let e_i be the i-th basis vector of $\mathcal{B}_1$.Express the image $e_i x$ as a linear combination of the elements of $c_j \in \mathcal{B}_2$, say if
$e_i x = \alpha_{i,1} c_1 + \cdots + \alpha_{i,n} c_n$ then define

$$M_{\mathcal{B}_1}^{\mathcal{B}_2}(x) := (\alpha_{i,j}).$$

Theorem

The following are true:

1. *If $x, y : V_1 \longrightarrow V_2$ are linear transformations and $\mathcal{B}_i$ are bases of V_i then*
$$M_{\mathcal{B}_1}^{\mathcal{B}_2}(x+y) = M_{\mathcal{B}_1}^{\mathcal{B}_2}(x) + M_{\mathcal{B}_1}^{\mathcal{B}_2}(y).$$

2. *If $\alpha \in \mathbb{F}$ and $x : V_1 \longrightarrow V_2$ is a linear transformation and $\mathcal{B}_i$ are bases of V_i then*
$$M_{\mathcal{B}_1}^{\mathcal{B}_2}(\alpha x) = \alpha M_{\mathcal{B}_1}^{\mathcal{B}_2}(x).$$

3. *If V_3 is a vector space with basis $\mathcal{B}_3$ and $y : V_2 \longrightarrow V_3$ is a linear transformation then*
$$M_{\mathcal{B}_1}^{\mathcal{B}_3}(x \circ y) = M_{\mathcal{B}_1}^{\mathcal{B}_2}(x) M_{\mathcal{B}_2}^{\mathcal{B}_3}(y).$$

Definition

Let A and B be $\mathbb{F}$-algebras. A linear transformation $\Psi : A \longrightarrow B$ which is also a ring homomorphism such that $1_A\Psi = 1_B$ is called an $\mathbb{F}$-algebra homomorphism or algebra homomorphism for short.

Now, for example, if in the formulae of Theorem 1.2 above we take $V_1 = V_2 = V_3$ and $\mathcal{B}_1 = \mathcal{B}_2 = \mathcal{B}_3$, then then we see that the map $x\Psi_1 := M_{\mathcal{B}_1}^{\mathcal{B}_1}(x)$ is an isomorphism of algebras.
Next we consider the question of how the matrix representing x changes when we change bases.To make this precise we need some notation. Let $\mathcal{B}_1 = \{e_1, \ldots, e_m\}$ and $\mathcal{B}_3 = \{f_1, \ldots, f_m\}$ be bases of V_1, $\mathcal{B}_2$ and $\mathcal{B}_4$ be bases of V_2 and x a linear transformation $x : V_1 \longrightarrow V_2$ where $m = \dim(V_1)$ and $n = \dim(V_2)$. Now express the vectors $e_i \in \mathcal{B}_1$ as linear combinations elements from $\mathcal{B}_3$. Say $e_i = \beta_{i,1} f_1 + \cdots + \beta_{i,m} f_m$ then we define

$$P := (\beta_{i,j}).$$

The matrix P is called a *base change matrix from basis* $\mathcal{B}_1$ *to basis* $\mathcal{B}_3$ as its rows express the elements of $\mathcal{B}_1$ as linear combinations of the vectors form $\mathcal{B}_3$. As a consequence we have that if $v \in V_1$ and

$$v = \sum_{i=1}^{m} \delta_i e_i = \sum_{i=1}^{m} \gamma_i f_i$$

then

$$[\delta_1, \ldots, \delta_m]P = [\gamma_1, \ldots, \gamma_m],$$

that is P “converts” $\mathcal{B}_1$ coordinates into $\mathcal{B}_3$ coordinates.

Thus we see that

$$[\delta_1, \ldots, \delta_m] = [\gamma_1, \ldots, \gamma_m]P^{-1}$$

and so P^{-1} "converts" $\mathcal{B}_3$ coordinates into $\mathcal{B}_1$ coordinates. Similarly we define Q to be the base change matrix from basis $\mathcal{B}_2$ to basis $\mathcal{B}_4$.

Theorem

With the notation as above we have

$$M_{\mathcal{B}_3}^{\mathcal{B}_4}(x) = P^{-1} M_{\mathcal{B}_1}^{\mathcal{B}_2}(x) Q.$$

We summarize what we have

Theorem

Let V be an F-vector space of dimension n and $\mathcal{B}_1$, $\mathcal{B}_3$ bases of V. Denote the base change matrix from $\mathcal{B}_1$ to $\mathcal{B}_3$ by P. The following are true:

1. *The maps $\Psi_i : \mathrm{End}(V) \longrightarrow M_n(\mathbb{F})$, with $i \in \{1, 3\}$ defined by $x\Psi_i = M_{\mathcal{B}_i}^{\mathcal{B}_i}(x)$ is an algebra isomorphism.*
2. *For all $x \in \mathrm{End}(V)$ we have*

$$x\Psi_3 = P^{-1}(x\Psi_1)P.$$

So the part 1 of Theorem 1.5 makes precise the statement that a choice of basis of V yields an $\mathbb{F}$ algebra isomorphism between $\mathrm{End}(V)$ and $M_n(F)$, hence also establishes a group isomorphism between $\mathrm{GL}(V)$ and $\mathrm{GL}_n(\mathbb{F})$. As $GL_n(\mathbb{F})$ is transitive on the set of bases of V, part 2 of Theorem 1.5, in effect, shows that up to conjugation by $\mathrm{GL}_n(\mathbb{F})$ the algebra isomorphism is unique.

Our next example of an algebra is the one of primary interest for us.
Example 3: The *group algebra (of G over* $\mathbb{F}$*)* $\mathbb{F}[G]$ is the set of "formal $\mathbb{F}$ linear combinations of group elements" namely $\{\sum_{g\in G} \alpha_g g \ : \ \alpha_g \in \mathbb{F}\}$. The operations are as follows:
$\forall g, h \in G, \lambda, \alpha_g, \beta_g \in \mathbb{F}$

$$\sum_{g\in G} \alpha_g g + \sum_{g\in G} \beta_g g := \sum_{g\in G} (\alpha_g + \beta_g) g$$

$$\lambda \sum_{g\in G} \alpha_g g := \sum_{g\in G} (\lambda \alpha_g) g$$

$$(\sum_{g\in G} \alpha_g g)(\sum_{g\in G} \beta_g g) := \sum_{g\in G} \gamma_g g,$$

where $\gamma_g := \sum_{x,y\in G \ , \ xy=g} \alpha_x \beta_y$.
Note that we embed G into $\mathbb{F}[G]$ via $g \longrightarrow \sum_{h\in G} \delta_{g,h} h$. Thus we see that the identity element of G and the identity element of $\mathbb{F}[G]$ are identified in this way. We call the image of G in $\mathbb{F}[G]$ the *distinguished basis* of $\mathbb{F}[G]$.

Definition

An algebra homomorphism $\rho : \mathbb{F}[G] \longrightarrow M_n(\mathbb{F})$ *is called a representation of* $\mathbb{F}[G]$*.n is called the degree of the representation.We say that two representations* ρ_1, ρ_2 *of* $\mathbb{F}[G]$ *are similar if there exists a* $g \in \mathrm{GL}_n(\mathbb{F})$ *such that* $\forall x \in \mathbb{F}[G]$ *we have* $g^{-1}(x\rho_1)g = x\rho_2$*.*

Definition

A group homomorphism $\rho : G \longrightarrow \mathrm{GL}_n(\mathbb{F})$ *called a representation of G. We say that two representations* ρ_1, ρ_2 *of G are similar if there exist* $g \in \mathrm{GL}_n(\mathbb{F})$ *such that* $\forall x \in G$ *we have* $g^{-1}(x\rho_1)g = x\rho_2$*.*

Using the identification of G with the distinguished basis of $\mathbb{F}[G]$ we see that a representation of $\mathbb{F}[G]$ induces a representation of G. It is an easy exercise to show the converse. From now on we will use the identification of G and $\mathbb{F}[G]$ representations whenever it is convenient to do so. In light of Theorem 1.5 we see that similarity of representations is just invariance under base change; i.e. that similarity classes are independent of choice of basis of $\mathbb{F}^n$.

We conclude this section with some examples. Let $n \in \mathbb{N}$ and $G = \mathbb{Z}/n\mathbb{Z}$ the cyclic group of order n.Let $i \in \mathbb{C}$ be such that $i^2 = 1$. For $n \in \mathbb{N}$ define $\zeta_n := e^{2\pi i/n}$. Fix a generator x of G.

Example 1: $\mathbb{F} = \mathbb{C}$, $\rho_{1,k} : G \longrightarrow GL_1(\mathbb{C})$, $x\rho_1 = [\zeta_n^k]$.

Example 2: $\mathbb{F} = \mathbb{C}$, $\rho_{2,j,k} : G \longrightarrow GL_2(\mathbb{C})$, $x\rho_2 = \begin{pmatrix} \zeta_n^j & 0 \\ 0 & \zeta_n^k \end{pmatrix}$.

Example 3: $\mathbb{F} = \mathbb{Q}$, $n = 3$ resp. 4, $\rho_3 : G \longrightarrow GL_2(\mathbb{Q})$, $x\rho_3 := \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ resp. $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

Example 4: $\mathbb{F} = \mathbb{F}_p$ a finite field of prime order p, $n = p$,

$\rho_4 : G \longrightarrow GL_2(\mathbb{F})$, $x\rho_4 := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

Example 5: $\mathbb{F} = \mathbb{F}_p$ a finite field of odd prime order p, $n = 2p$,

$\rho_5 : G \longrightarrow GL_2(\mathbb{F})$, $x\rho_5 := \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}$.

Note that $x\rho_i$ is a diagonalizable matrix for $i \leq 3$; i.e. the characteristic of $\mathbb{F}$ is coprime to $|G|$,whereas $x\rho_i$ is not diagonalizable for $i > 3$; i.e. the characteristic of $\mathbb{F}$ is a divisor of $|G|$. We shall see a generalization of this in the next section, namely Maschke's Theorem

Although the results and definitions of this section hold for general associative algebras with identity, our main examples will be group algebras. Throughout A denotes an associative F-algebra with identity.

Definition

If A is an $\mathbb{F}$ algebra, then an $\mathbb{F}$ vector space V is called an A- module if there exists a map $\psi : V \times A \longrightarrow V$ such that for all $v, w \in V$, $x, y \in A$ and all $\lambda, \mu \in \mathbb{F}$ we have

1. $(\lambda v + \mu w)x = \lambda(vx) + \mu(wx)$,
2. $v(\lambda x + \mu y) = \lambda(vx) + \mu(vy)$,
3. $v(xy) = (vx)y$,
4. $v1 = v$.

If V is an A-module and $x \in A$, then item 1 in the definition above is equivalent to the assertion that the map $x_V : V \longrightarrow V$ defined by $v \longrightarrow vx$ is an F-linear transformation; i.e. $x_V \in \mathrm{End}(V)$. Another consequence of the definition of A-module is:

Lemma

If V is an A-module, then the map $x \longrightarrow x_V$ is an algebra homomorphism.

We denote the image of A in $\mathrm{End}(V)$ by A_V.
We now give some examples of A modules.
Example 1: V is an A-module for any subalgebra of $\mathrm{End}(V)$.
Example 2: If $A = M_n(\mathbb{F})$, then the space of row vectors of length n over $\mathbb{F}$ is an A-module.
Example 3: Any right ideal M of A is an A-module.
Note that have to verify that M is in fact a vector space. To see this we first note that $\{\lambda 1_A : \lambda \in \mathbb{F}\}$ embeds $\mathbb{F}$ in to the center of A. The center $Z(A)$ of A is defined as expected, namely we define $Z(A) := \{z \in A : xz = zx \ \forall x \in A\}$.Now for all $\lambda \in \mathbb{F}$ and all $x \in M$ we have

$$\lambda x = (\lambda 1_A)x = x(\lambda 1_A) = x\lambda \in M,$$

showing closure under scalar multiplication.
Example 3' The right ideal A of A is called the *regular* A-module and is denoted by A^o.

Definition

If V and W are A-modules then an A-module homomorphism a linear transformation $\phi : V \longrightarrow W$ such that $\forall x \in A$, $v \in V$ and $w \in W$ we have $(v\phi)x = (vx)\phi$.

If in the definition above ϕ is an isomorphism, then we say that the A modules V and W are isomorphic.
A primary goal in representation theory is to classify similarity classes of representations.
Recall that if V is a vector space of dimension n, then a basis $\mathcal{B}$ of V defines an algebra isomorphism between $\mathrm{End}(V)$ and $M_n(\mathbb{F})$. This shows that similarity classes of A representations are in one to one correspondence with isomorphism classes A modules.

Definition

A subspace U of an A-module V is called an A-submodule if $\forall u \in U, x \in A$ we have $ux \in U$. An A-module V is irreducible if it possesses no proper submodules.

The following lemma gives a connection between module homomorphisms and submodules.

Lemma

If $\phi : V \longrightarrow W$ is a homomorphism of A-modules, then $\mathrm{Ker}(\phi)$ and $\mathrm{Im}(\phi)$ are submodules of V and W respectively.

Proof : Let $u \in \mathrm{Ker}(\phi)$ and $x \in A$. Then $(ux)\phi = (u\phi)x = 0x = 0$, showing that $ux \in \mathrm{Ker}(\phi)$. Hence $\mathrm{Ker}(\phi)$ is a submodule of V
Now if $u \in \mathrm{Im}(\phi)$ and $x \in A$, then $\exists v \in V$ with $u = v\phi$. Thus

$$ux = (v\phi)x = (vx)\phi,$$

showing that $\mathrm{Im}(\phi)$ is a submodule of W. **QED**

Definition

For A modules V and W the set of A-module homomorphisms from V to W is denoted by $\mathrm{Hom}_A(V, W)$.

Note that addition of linear transformations and scalar multiplication turn $\mathrm{Hom}_A(V, W)$ into an $\mathbb{F}$ vector space. If $W = V$, then $\mathrm{Hom}_A(V, V)$ is a subalgebra of $\mathrm{End}(V)$.

Definition

If B is a subalgebra of A then

$$C_A(B) := \{x \in A \ : \ xb = bx \ \forall b \in B\}$$

is called the centralizer of B in A.

For example if $B = A$, then, by definition of $Z(A)$, we have that $C_A(A) = Z(A)$, the center of A. The next lemma is an exercise in applying the definitions, which we leave for the reader.

Lemma

If V is an A-module, then $\mathrm{Hom}_A(V, V) = C_{\mathrm{End}(V)}(A_V)$. Moreover $A_V \subset C_{\mathrm{End}(V)}(\mathrm{Hom}_A(V, V)) = C_{\mathrm{End}(V)}(C_{\mathrm{End}(V)}(A_V))$.

We now come to

Lemma (Schur)

If V and W are non-trivial irreducible A-modules, then every element of $\mathrm{Hom}_A(V,W)^*$ has an inverse in $\mathrm{Hom}_A(W,V)$.

Proof : Let $\phi \in \mathrm{Hom}_A(V,W)^*$. Then $\mathrm{Im}(\phi)$ is a non-trivial submodule of W. As W is irreducible this means that $\mathrm{Im}(\phi) = W$; i.e. ϕ is surjective. Also $\mathrm{Ker}(\phi)$ is a submodule of V which,as V is irreducible, is either 0 or equal to V. As $\mathrm{Im}(\phi)$ is non-trivial we see that $\mathrm{Ker}(\phi) \neq V$. Thus $\mathrm{Ker}(\phi) = 0$ proving that ϕ is also injective. **QED**

Corollary

If V is an irreducible A-module and $\mathbb{F}$ is algebraically closed, then

$$\mathrm{Hom}_A(V,V) \cong \mathbb{F} \cong Z(\mathrm{End}(V)) = \{\lambda 1_V \ : \ \lambda \in \mathbb{F}\}.$$

Proof : Clearly $Z(\mathrm{End}(V)) = \{\lambda 1_V \ : \ \lambda \in \mathbb{F}\} \subset \mathrm{Hom}_A(V,V)$. Now let $\phi \in \mathrm{Hom}_A(V,V)$ and let λ be an eigenvalue of ϕ. Then $\phi - \lambda 1_V \in \mathrm{Hom}_A(V,V)$ as the latter is closed under addition. Thus by Schur's lemma $\phi - \lambda 1_V$ is either 0 or invertible. The latter is impossible as $\mathrm{Ker}(\phi - \lambda 1_V) \neq 0$, showing that $\phi = \lambda 1_V$. **QED**

Definition

An A module is completely reducible if for every submodule W there exists a submodule U such that $V = W \oplus U$.

Remark: If G is the trivial group and $A = \mathbb{F}[G]$, then every A module is completely reducible as every subspace of a vector space has a complement.

Theorem (Maschke)

If G is a finite group and $\mathrm{char}(\mathbb{F})$ *is coprime to* $|G|$*, then all* $\mathbb{F}[G]$*-modules are completely reducible.*

Proof : Let V be an $\mathbb{F}[G]$ and W be submodule. Let U' be some complement of W and let $\pi : V \longrightarrow W$ be the natural projection along U' onto W. To be clear, every $v \in V$ can be uniquely expressed as $w + u'$ where $w \in W$ and $u' \in U'$, and we define $v\pi := w$. Now π is not an $\mathbb{F}[G]$ homomorphism but we can use it to define one namely

$$v\phi := \frac{1}{|G|} \sum_{g \in G} ((vg)\pi)g^{-1}.$$

As G is finite $\phi \in \mathrm{End}(V)$. We first show that $\phi \in \mathrm{End}_{\mathbb{F}[G]}(V)$.
Let $h \in G$, then

$$(v\phi)h = (\frac{1}{|G|} \sum ((vg)\pi)g^{-1})h$$

$$= (\frac{1}{|G|} \sum_{hg \in G} ((vhg)\pi)(hg)^{-1}h) = (vh)\phi.$$

Thus ϕ is an $\mathbb{F}[G]$ homomorphism and $\mathrm{Im}(\phi) \subset W$, as W is a submodule. Also if $w \in W$, then

$$w\phi = \frac{1}{|G|} \sum_{g \in G} ((wg)\pi)g^{-1})$$

$$= \frac{1}{|G|} \sum_{g \in G} (wg)g^{-1} = \frac{|G|}{|G|} w = w.$$

So we see that $v\phi^2 = w\phi = w$; i.e. $\phi^2 = \phi$.
Finally we show that $\mathrm{Ker}(\phi) \cap W = 0$. To this end let $u \in \mathrm{Ker}(\phi) \cap W$.Then $u \in W$, hence $u = u\phi$.But $u \in \mathrm{Ker}(\phi)$, hence $u = u\phi = 0$ which proves that $\mathrm{Ker}(\phi) \cap W = 0$. As $\dim(V) = \dim(W) + \dim(\mathrm{Ker}(\phi))$ we see that $V = W \oplus \mathrm{Ker}(\phi)$. Now everything is proved as $\mathrm{Ker}(\phi)$ is an $\mathbb{F}[G]$ submodule.

QEDMaschke's theorem proves that $\mathbb{F}[G]^o$ is completely reducible if $\mathrm{char}(\mathbb{F})$ is coprime to $|G|$.

Theorem

An A module is completely reducible if and only if it is generated by its irreducible submodules.

Proof : If V is completely reducible, then let W be the submodule generated by the irreducible submodules of V. By complete reducibility $V = W \oplus U$ for some A submodule U. Now any irreducible submodule of U will, by definition of W, lie in $U \cap W = 0$.Thus U contains non nontrivial submodules hence $U = 0$. Conversely suppose that V is generated by its irreducible submodules and let W be a the submodule of V. Pick U maximal subject to $W \cap U = 0$. This is possible as $\dim(V)$ is finite. We claim that $V = W \oplus U$; else there exists an irreducible submodule M such that $(W \oplus U) \cap M = 0$. That implies that $W \cap (U \oplus M) = 0$, violating the maximality of U. **QED**

Lemma

If V is an A-module generated by irreducible submodules, then V is a direct sum of irreducibles.

Proof : Let W be maximal subject to being a direct sum of irreducibles. If $W \neq V$, then,as V is completely reducible, there exists a submodule U of V such that $V = W \oplus U$. Now if M is a nontrivial irreducible submodule of U,then $W \oplus M$ is a direct sum of irreducibles; violating the maximality of W. So $M = 0$ which implies that $U = 0$ and hence $V = W$. **QED**

We will now prove some general results concerning the representation theory of finite dimensional semisimple algebras. By definition an algebra A is *semisimple* if A^o is completely reducible.

Definition

If V is an A-module and M is a submodule, then we define

$$\mathrm{Ann}(M) := \{x \in A \ : \ mx = 0 \ \forall m \in M\}$$

the annihilator and

$$I_V(M) := \sum_{M \cong W \subset V} W$$

to be the isotypic component of M in V

We note that $\mathrm{Ann}(M)$ is an ideal of A and that $I_V(M)$ is a direct sum of isomorphic copies of M, and that if $M \ncong N$ then $I_V(M) \cap I_V(N) = 0$.

Lemma

$I_V(M)$ is a $\mathrm{Hom}_A(V, V) = C_{\mathrm{End}(V)}(A_V)$ invariant.

Proof : If M is irreducible and $\phi \in \mathrm{Hom}_A(V, V)$ then either $\mathrm{Ker}(\phi|_M) = 0$ or M. In the first case $M \cong \mathrm{Im}(\phi|_M)$ and hence, by definition, $\mathrm{Im}(\phi) \subset I_V(M)$. **QED**By $\mathcal{M}(A)$ we denote the isomorphism classes of irreducibles A modules.

Lemma

If A is a algebra and V is an irreducible A-module, then V is a factor module of A^o. If A is semisimple, then V is also a direct summand of A^o.

Proof : Let $0 \neq v \in V$ and for $x \in A^o$ define $x\phi := vx$. Now for all $y \in A$ we have

$$xy\phi = v(xy) = (vx)y = (x\phi)y$$

showing that ϕ is an A-homomorphism. As V is irreducible and $0 \neq v = 1_A\phi$ we see that $\mathrm{Im}(\phi) = V$ and the first claim follows. If A^o is semisimple, then $\mathrm{Ker}(\phi)$ has a complement which must be isomorphic to $\mathrm{Im}(\phi) = V$. **QED**

Theorem (Wedderburn)

Let A be a semisimple algebra and let M be an irreducible A-module. The following are true:

1. $I_A(M)$ *is a minimal ideal of* A.
2. *If* N *is irreducible, then* $I_A(M) \subset \mathrm{Ann}(N)$ *unless* $M \cong N$.
3. *The restriction of the representation of* $\phi : I_A(M) \longrightarrow A_M \subset \mathrm{End}(M)$ *is one to one and onto.*
4. $\mathcal{M}(A)$ *is a finite set.*

Proof : If $x \in A$ then the map $\phi_x : A^o \longrightarrow A^o$ defined by $y\phi_x = xy$ lies in $\mathbb{C}_A(\mathrm{End}(A^o))$ as for all $z \in A$ we have $(y\phi_x)z = (xy)z = x(yz) = (yz)\phi_x$. So Lemma 3.2 implies that ϕ_x leaves $I_A(M)$ invariant, hence is a left ideal of A^o. As as every submodule of A^o is a right ideal of A^o we see that $I_A(M)$ is an ideal; proving the first part of 1.

To prove part 2 note that for irreducible A-modules $M \ncong N$ we have $I_A(N)I_A(M) \subset I_A(N) \cap I_A(M) = 0$.
Part 4 is a consequence of Lemma 3.3 and the finite dimensionality of A. Moreover

$$A = \oplus_{M \in \mathcal{M}(A)} I_A(M)$$

To prove part 3 we note that part 2 implies that for $N \ncong M$ we have $I_A(N) \subset \mathrm{Ker}(\phi)$ which proves that ϕ is onto. Now suppose that $x \in \mathrm{Ker}(\phi) \cap I_A(M)$. Then x annihilates every irreducible A-module and so

$$x = 1_A x \in Ax = 0$$

proving that ϕ is injective.
Suppose $I \subset I_A(M)$ is an ideal of A. Now $I_M(A)$ is a direct sum of copies of M, so if $I \neq I_A(M)$ then there exists a submodule $M' \cong M$ of $I_A(M)$ such that M' does not lie in I.Thus $I \cap M' = 0$ as M' is irreducible and hence $M'I \subset M' \cap I = 0$. Thus I annihilates M' hence if $x \in I$ then $x_M = 0$. As $x \longrightarrow x_M$ is one to one we have that $x = 0$.; i.e. $I = 0$. **QED**

Theorem (Double Centralizer)

If V is an irreducible A-module of a semisimple $\mathbb{F}$-algebra A, then

$$A_V = C_{\mathrm{End}(V)}(\mathrm{Hom}_A(V, V))) = C_{\mathrm{End}(V)}(C_{\mathrm{End}(V)}(A_V))$$

.

Proof : We have already seen that $A_V \subset C_{\mathrm{End}(V)}(C_{\mathrm{End}(V)}(A_V))$. So now suppose $\theta \in C_{\mathrm{End}(V)}(C_{\mathrm{End}(V)}(A_V))$. Without loss we may assume that $V \subset I_A(V) \lhd A$
For $v \in V$ define $\alpha_v : V \longrightarrow A$ by $x\alpha_v = vx$, as V is an A module $vx \in M$. Also for all $a \in A$ we have that
$(xa)\alpha_v = v(xa) = (vx)a = (x\alpha_v)a$ showing that $\alpha_v \in C_{\mathrm{End}(V)}(A_V)$.
Thus for all $v, w \in V$ we have

$$(vw)\theta = (w\alpha_v)\theta = v(w\theta).$$

For fixed $w \in V$ we have $AwA < I_A(V)$. Let e denote the projection of 1_A onto $I_A(V)$.As AwA is an ideal and $I_A(V)$ is a minimal ideal of A, we see that $e \in A = I_A(V)$. So there exist $a_i, b_i \in A$ such that
$e = \sum a_i w b_i$ so for all $v \in V$ we have

$$v\theta = ve\theta = \sum (va_i wb_i)\theta = \sum (va_i)(wb_i)\theta$$

$$\sum (wb_i)\alpha_{va_i}\theta = \sum (wb_i)\theta\alpha_{va_i} = \sum (va_i)((wb_i)\theta) = v\sum a_i((wb_i)\theta).$$

We observe that $\sum a_i((wb_i)\theta) \in AwA = I_A(V)$ and thus $\theta = \sum a_i((wb_i)\theta) \in I_A(V) = A_M$. This is what we claimed. **QED**

We can now prove the following important corollary which reveals the structure of a semisimple algebra and its representations.

Theorem

Let A be a semisimple $\mathbb{F}$ algebra, where $\mathbb{F}$ is algebraically closed, V be an A-module and let $\mathcal{M}(A)$ be a set of representatives of irreducible A-modules. The following are true:

1. $A_V = \mathrm{End}(V)$
2. $\dim(A_V) = \dim(I_A(V)) = \dim(V)^2$
3. $I_A(V)$ *is direct sum of* $\dim(V)$ *copies of* V
4. $\dim(A) = \sum_{V\in\mathcal{M}(A)} \dim(V)^2$
5. $\dim(Z(A)) = |\mathcal{M}(A)|$

Proof : By the corollary to Schur's Lemma $C_{\mathrm{End}(V)}(A_V) = \mathbb{F}\cdot 1_V$.

So by the Double Centralizer Theorem

$$\mathrm{End}(V) = C_{\mathrm{End}(V)}(\mathbb{F} \cdot 1_V) = C_{\mathrm{End}(V)}(C_{\mathrm{End}(V)}(A_V)) = A_V$$

which is our first claim. Our second claim follows from part 1 of Theorem 1.5.
The third claim follows from the second and the fact that A^o, hence also $I_A(V)$, is completely reducible.
The fourth claim follows from the second and from Lemma 3.3. Recall that $A_V A_W = 0$ if $V \ncong W$. So as $A = \oplus_{\mathcal{M}(A)} I_A(V)$ we have

$$Z(A) = \oplus_{\mathcal{M}(A)} Z(I_A(V)) = \mathbb{F}^{|\mathcal{M}(A)|}$$

and our last claim follows. **QED**

Characters

Let G be a group, $\mathbb{F}$ a field, and V be an n-dimensional vector space over $\mathbb{F}$. We saw in the previous sections that an $\mathbb{F}[G]$-module V together with a basis $\mathcal{B}$ of V gives rise to a representation $\phi : G \longrightarrow \mathrm{GL}_n(\mathbb{F})$.If $g \in G$ then recall that the characteristic polynomial of $g\phi$ is defined as

$$m_{g\phi}(x) := \mathrm{Det}(g\phi - x1_n)$$

is invariant under base change; i.e. $\forall P \in \mathrm{GL}_n(\mathbb{F})$ we have

$$m_{P^{-1}g\phi P} = \mathrm{Det}(P^{-1}g\phi P - x1_n) = \mathrm{Det}(P^{-1}(g\phi - x1_n)P)$$

$$= \mathrm{Det}(P^{-1})\mathrm{Det}(g\phi - x1_n)\mathrm{Det}(P) = \mathrm{Det}(g\phi - x1_n) = m_{g\phi}(x).$$

Thus we record

Lemma

1. *If ϕ and ψ are similar representations of G then $\forall g \in G$ we have $m_{g\phi}(x) = m_{g\psi}(x)$.*
2. *$\forall g, h \in G$ we have $m_{g\phi}(x) = m_{h^{-1}gh\phi}(x)$.*

Clearly the coefficients of the minimal polynomial are invariants of the representation of of G. We recall that the constant coefficient of $m_{g\phi}(x)$ is equal to $(-1)^n \mathrm{Det}(g\phi)$, the determinant of $g\phi$, and that the coefficient of x^{n-1} in $m_{g\phi}(x)$ is $-\mathrm{Tr}(g\phi)$, the trace of $g\Phi$.

Definition

If V is an $\mathbb{F}[G]$-module and $\mathcal{B}$ be a basis for V, then the function $\chi : \mathbb{F}[G] \longrightarrow \mathbb{F}$ defined by $\chi(g) = \mathrm{Tr}(M_{\mathcal{B}}^{\mathcal{B}}(g))$ is called the $\mathbb{F}$ character of V. Correspondingly if ϕ is a representation then the F-charcter of ϕ is the function $\chi(g) = \mathrm{Tr}(g\phi)$. A function from G to $\mathbb{C}$ which is constant on conjugacy classes of G is a class function.

We if $\Phi : G \longrightarrow GL(V)$ is representation with character χ we say that *V is a module affording χ*.
Evidently by 2 of Lemma 4.1 $\mathbb{F}$-characters of G are class functions.
We also have the following

Lemma

If χ is an $\mathbb{F}$ character, then $\chi(g)$ is independent of choice of basis and choice of conjugate.

The lemma guarantees that characters of modules and representations are well-defined. We call a character *irreducible* if its underlying representation is irreducible.The *degree* of a character χ is $\chi(1)$. We note that if $(\mathrm{char}(\mathbb{F}), |G|) = 1$, then the degree of an $\mathbb{F}$-character is equal to the dimension of an $\mathbb{F}[G]$-module affording it.
The lemma guarantees that characters of modules and representations are well-defined.
By $\mathrm{Irr}(G)$ we denote the set of all irreducible $\mathbb{C}$ characters of G and note that $||\mathrm{Irr}(G)| = |\mathcal{M}(\mathbb{C}[G)|$.
The the character of the regular $\mathbb{C}[G]^o$-module is called the *regular character* and is denoted by ρ. Form corollary **??** we see that

$$|G| = \sum_{\mathcal{M}(\mathbb{C}[G])} \chi_i(1)^2.$$

If $\{C_1, \ldots, C_k\}$ are the conjugacy classes of G then we define the class sum of C_i by $\bar{C}_i := \sum_{g \in C_i} g \in \mathbb{C}[G]$.

Theorem

The class sums form a basis of $Z(\mathbb{C}[G])$.

Proof : As conjugation by $g \in G$ permutes the elements of C_i we see that $\bar{C}^g = \bar{C}$,which shows that $\bar{C} \in Z(\mathbb{C}[G])$.
Now let $z \in Z(\mathbb{C}[G])$ and let α_g be the coefficient of g in z. As $z = z^h = \sum_{g \in G} \alpha_g g^h$ we see by comparing coefficients that $a_g = a_{g^h}$.So the coefficients are constant on elements of a conjugacy class. Thus z is a linear combination of class sums, showing that the class sums span $Z(\mathbb{C}[G])$.As conjugacy classes are disjoint,linear independence of them is guaranteed. **QED**

We already saw that the number of similarity classes of $\mathbb{C}[G]$ modules is equal to $\dim(Z(\mathbb{C}[G]))$ and thus the theorem yields the following fundamental corollary.

Corollary

The number of similarity classes of irreducible $\mathbb{C}[G]$-modules is equal to the number conjugacy classes of G.

Corollary

G is abelian if and only if $\chi(1) = 1$ for all $\chi \in \mathrm{Irr}(G)$.

Proof : Let $k = |\mathcal{M}(\mathbb{C}[G])| = |Irr(G)| = \dim(Z(\mathbb{C}[G])$, which, by the above, is equal to the number of conjugacy classes of G.Now G is abelian if and only if the $|G| = k$.
On the other hand by Wedderburn's theorem we have $|G| = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2 \geq k = |G|$. As $\chi(1) \geq 1$ we see that $\chi(1) = 1$ for all $\chi \in \mathrm{Irr}(G)$ if and only if $|G| = k$ if and only if G is abelian. **QED**
We call a character of degree 1 a *linear character*.

Corollary

The number of $\chi \in \mathrm{Irr}(G)$ *such that* $\chi(1) = 1$ *is equal to* $[G : G']$*, the index of the commutator subgroup of G in G.*

Proof : Let ℓ be the number of linear irreducible characters of G. The factor goup G/G' is abelian, so by the above, $\ell \geq [G : G']$.Conversely if $\chi(1) = 1$ and Φ is a representation affording χ, then $\mathrm{Im}(\Phi) \subset \mathrm{GL}_1(\mathbb{C}) = \mathbb{C}^*$ is abelian. Thus $G' \subset \mathrm{Ker}(\Phi)$;showing that Φ can be interpreted as a map from G/G' to $\mathrm{GL}_1(\mathbb{C})$. Thus $\ell \leq [G : G']$ which yields our claim. **QED**

Lemma

The elements of $\mathrm{Irr}(G)$ *are distinct.*

Proof : If $\{V_1, \ldots, V_k\} = \mathcal{M}(\mathbb{C}[G])$, then recall that $\mathbb{C}[G] = \oplus_{i=1}^{k} I_{\mathbb{C}[G]}(V_i)$.
By e_i we denote the projection of 1 onto $I_{\mathbb{C}[G]}(V_i)$ and by χ_i we denote the character of V_i.
As the $I_{\mathbb{C}[G]}(V_i)$ are non-intersecting ideals we see that $e_i e_j = 0$ and thus $e_i|_{V_j} = 0$, so $\chi_i(e_j) = \delta_{i,j}\dim(V_i)$ showing that $\forall i \neq j$ we have $\chi_i \neq \chi_j$.

QED

Lemma

Every class function ϕ can be uniquely expressed as

$$\phi = \sum_{\chi \in \mathrm{Irr}(G)} a_\chi \chi.$$

Moreover ϕ is a character if and only if each a_χ is a positive integer.

Proof : It suffices to show that $\mathrm{Irr}(G)$ is a basis for the vector space of class functions. We have already seen that $|\mathrm{Irr}(G)|$ is equal to the number of conjugacy classes of G and thus equal to the dimension of the space of class functions.So it suffices to prove that $\mathrm{Irr}(G)$ is linearly independent.To this end suppose that $\sum_{\chi \in \mathrm{Irr}(G)} a_\chi \chi = 0$,then

$$0 = \sum_{\chi \in \mathrm{Irr}(G)} a_\chi \chi(e_\chi) = a_\chi$$

$\forall \chi \in \mathrm{Irr}(G)$, showing linear independence.
If χ is a character then there is a module V affording ϕ.By Maschke's theorem V is a direct sum of irreducibles.Moreover if a_i is the number of times that the irreducible V_i (affording character χ_i),then $\chi = \sum_i a_i \chi_i$ showing that a_i is a non-negative integer. On the other hand if a class function $\psi = \sum_i a_i \chi_i$ with $a_i \in \mathbb{N}$,then the module $W = \oplus_i V_i^{a_i}$ affords ψ. **QED**

Corollary

Two representations ρ_1 and ρ_2 of G are similar if and only if their characters are equal.

Proof : We have already seen that if ρ_1 and ρ_2 are similar then their characters are equal.The converse follows from the lemma. **QED**
We will now work towards the orthogonality relations which requires some lemmas involving the regular character.

Lemma

Let ρ be the regular character of G. We have

$$\rho = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi.$$

Proof : This a reformulation of Wedderburn's theorem. **QED**

Lemma

Let ρ be the regular character of G. If $g \in G$, then $\rho(g) = \delta_{1,g}|G|$.

Proof : In the regular representation the matrix representing g is a permutation matrix.The result follows as the trace of a permutation matrix is the number of fixed points. In the regular representation only the identiy element has fixed points. The number of fixed points of the identity element is the group order. **QED**Recall that e_i is the projection of the identy of the groups algebra onto the i'th isotypic component.

Lemma

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

Proof : Write $e_i = \sum a_g g$. By the previous two lemmas we have

$$\sum_j \chi_j(1)\chi_j(e_i g^{-1}) = \rho(e_i g^{-1}) = a_g|G|.$$

If Ψ is a representation affording ρ, then

$$(e_i g^{-1})\Psi = (e_i\Psi)(g^{-1}\Psi) = \delta_{i,j}(g^{-1}\Psi).$$

So $a_g|G| = \chi_i(1)\chi_i(g^{-1})$ and the claim follows. **QED**

Theorem (Generalized Orthogonality)

For all $h \in G$ we have

$$\frac{1}{|G|}\sum_{g\in G}\chi_i(gh)\chi_j(g^{-1}) = \delta_{i,j}\frac{\chi_i(h)}{\chi_i(1)}.$$

Proof : Recall that $e_i e_j = \delta_{i,j} e_i$. Substituting the formula for e_i given in the previous lemma into this formula yields

$$(\frac{1}{|G|}\sum_{g\in G}\chi_i(1)\chi_i(g^{-1})g)(\frac{1}{|G|}\sum_{g\in G}\chi_j(1)\chi_j(g^{-1})g)$$

$$=\delta_{i,j}\frac{1}{|G|}\sum_{g\in G}\chi_i(1)\chi_i(g^{-1})g$$

The coefficient for h on the right hand side is

$$\delta_{i,j}\frac{1}{|G|}\chi_i(1)\chi_i(h^{-1})$$

whereas the coefficient for h on the left hand side is

$$\frac{\chi_i(1)^2}{|G|^2}\sum_{g\in G}\chi_i((hg^{-1})^{-1})\chi_j(g^{-1})((hg^{-1})g).$$

Equating, re-aranging and substituting h for h^{-1} yields the desired formula. **QED**

Corollary (First Orthogonality Relation)

$$\frac{1}{|G|}\sum_{g\in G}\chi_i(g)\chi_j(g^{-1})=\delta_{i,j}.$$

Proof : In the theorem above, set $h=1$. **QED**

Lemma

Let Ψ be a representation affording the character χ, $g \in G$ of order n. The following are true:

1. *$g\Psi$ is similar to a diagonal matrix with diagonal entries $\epsilon_1, \ldots, \epsilon_k$, where $k = \chi(1)$,*
2. *$\forall i$ we have $\epsilon_i^n = 1$,*
3. *$\chi(g) = \sum_i \epsilon_i$ and $|\chi(g)| \leq \chi(1)$,*
4. *$\chi(g^{-1}) = \overline{\chi_i(g)}$.*

Proof : The minimal polynomial of g is a divisor of $x^n - 1$.Over $\mathbb{C}$ the polynomial $x^n - 1$ has no multiple roots. Thus the minimal polynomial of g has no multiple roots and each root is an n-th root of unity.So $g\Psi$ is diagonalizable and parts 1, 2 and the first part of 3 follow.The second part of 3 follows from the first and the triangle inequality.The last part follows from 1 and 3. **QED**

In light of part 4 we can rewrite the first orthogonality relation as

$$\frac{1}{|G|} \sum_{g \in G} \chi_i(g)\overline{\chi_j(g)} = \delta_{i,j}.$$

Definition

For class functions θ and ψ of G we define a hermitian inner product via

$$[\theta, \psi] = \frac{1}{|G|} \sum_{g \in G} \theta(g)\overline{\psi(g)}.$$

The first orthogonality relation states that $\mathrm{Irr}(G)$ is an orthonormal basis of the space of class functions on G.

Lemma

For class functions θ_i and ψ_i of G and $a_1, a_2 \in \mathbb{C}$, the following are true

1. $[\theta, \psi] = \overline{[\psi, \theta]}$,
2. $[\psi, \psi] \geq 0$ *with equality if and only if* $\psi = 0$,
3. $[a_1\theta_1 + a_2\theta_2, \psi] = a_1[\theta_1, \psi] + a_2[\theta_2, \psi]$,
4. $[\theta, a_1\psi_1 + a_2\psi_2] = \overline{a_1}[\theta, \psi_1] + \overline{a_2}[\theta, \psi_2]$.

Proof : clear **QED**

Recall that g^G denotes the conjugacy class of g in G.

Theorem (Second Orthogonality Relation)

Let $g, h \in G$. We have

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(g)\overline{\chi(h)} = \delta_{g^G,h^G}|C_G(g)|.$$

Proof : Let $g_1, \ldots, g_k$ be conjugacy class representatives.Let $X := (\chi_i(g_j))$; i.e. the character table.Let $D := \delta_{i,j}|g_i^G|$.By the first orthogonality relation we have

$$\delta_{i,j}|G| = \sum_{g \in G} \chi_i(g)\overline{\chi_j(g)} = \sum_{\nu=1}^{k} |g_\nu^G|\chi_i(g_\nu)\overline{\chi_j(g_\nu)}$$

We can put these k^2 equations into matrix form to obtain

$$|G|I_k = XD\overline{X}^t$$

where I_k means $k \times k$ identity matrix and X^t means the transpose of the matrix X.

In a matrix algebra one sided inverses are also two sided inverses so we have

$$|G| I_k = D\overline{X}^t X$$

which yields

$$\delta_{i,j}|G| = \sum_{\nu=1}^{k} |g_i^G| \chi_\nu(g_i)\overline{\chi_\nu(g_j)}.$$

Using that $|g_i^G| = \frac{|G|}{|C_G(g_i)|}$ now yields the result. **QED**

As an application of the orthogonality relations we will now compute the character table of the alternating group A_4. We know that A_4 has four conjugacy classes represented by $(), (1,2)(3,4), (1,2,3), (1,3,2)$ and that $\mathbb{Z}/3\mathbb{Z} \cong A_4/[A_4, A_4]$. This information yields the following portion of the character table.

g_i	$()$	$(1,2)(3,4)$	$(1,2,3)$	$(1,3,2)$
$\lvert C_G(g_i)\rvert$	12	4	3	3
χ_1	1	1	1	1
χ_2	1	1	ω	ω^2
χ_3	1	1	ω^2	ω

where $\omega = e^{2\pi i/3}$.

As A_4 has four conjugacy classes the number of irreducible characters of A_4 is also four. So we are missing a fourth irreducible character χ_4. Now

$$\chi_4(())^2 = |A_4| - \chi_1(())^2 - \chi_2(())^2 - \chi_3(())^2 = 12 - 1 - 1 - 1 = 9;$$

showing that $\chi(()) = 3$.Also

$$|\chi_4((1,2,3))|^2$$

$$= |C_{A_4}((1,2,3))| - |\chi_1((1,2,3))|^2 - |\chi_2((1,2,3))|^2 - |\chi_3((1,2,3))|^2$$

$$= 3 - 1 - 1 - 1 = 0$$

and

$$|\chi_4((1,3,2))|^2$$

$$= |C_{A_4}((1,2,3))| - |\chi_1((1,2,3))|^2 - |\chi_2((1,2,3))|^2 - |\chi_3((1,2,3))|^2$$

$$= 3 - 1 - 1 - 1 = 0.$$

So $\chi_4((1,2,3)) = 0 = \chi_4((1,3,2))$.

Finally we compute that

$$|\chi_4((1,2)(3,4))|^2$$

$$= |C_{A_4}((1,2)(3,4))| - |\chi_1((1,2)(3,4))|^2 - |\chi_2((1,2)(3,4))|^2 - |\chi_3((1,2)(3,4))|^2$$

$$= 4 - 1 - 1 - 1 = 1.$$

So $\chi_4((1,2)(3,4)) = \pm 1$.To determine the sign we use the first orthogonality relation.

$$0 = [\chi_1, \chi_4] = \frac{1}{12}((1 \times 1 \times 3) + (3 \times 1 \times \pm 1) + (4 \times 1 \times 0) + (4 \times 1 \times 0)).$$

This yields $\chi_4((1,2)(3,4)) = -1$ and so the character table of A_4 is

g_i	$()$	$(1,2)(3,4)$	$(1,2,3)$	$(1,3,2)$
$\lvert C_G(g_i)\rvert$	12	4	3	3
χ_1	1	1	1	1
χ_2	1	1	ω	ω^2
χ_3	1	1	ω^2	ω
χ_4	3	-1	0	0

where $\omega = e^{2\pi i/3}$.

Definition

The kernel $\mathrm{Ker}(\chi)$ *of a character* χ *is the set of* $g \in G$ *for which* $\chi(g) = \chi(1)$.

The center $Z(\chi)$ *of a character* χ *is the set of* $g \in G$ *for which* $|\chi(g)| = \chi(1)$.

It is easy to see that if Ψ is a representation affording χ, then $\mathrm{Ker}(\chi) = \mathrm{Ker}(\Psi)$ and $Z(\Psi)$ is the preimage of $(Z(\mathrm{Im}(\Psi)))$ in G.

We note that any character χ of a factor group G/K can be extended to a character ψ of G by defining $\psi(g) := \chi(Kg)$.

A character χ is *faithful* if $\mathrm{Ker}(\chi) = 1$.

Lemma

$Z(\chi)/Ker(\chi)$ *is cyclic if* χ *is a faithful irreducible character of* G.

Proof : Let Ψ be a representation affording χ and V the corresponding module. The image of G acts irreducibly.Thus $Z(\chi)/Ker(\chi)\Psi \subset C_{\mathrm{End}(V)}(G\Psi) = \mathbb{C}$. The last equality is the corollary to Schur's lemma.Our claim follows if we can show that a finite subgroup of $\mathbb{C}^*$ is in fact cyclic.To see this let $z \in \mathbb{C}^*$ be an element of finite order.Writing $z = re^{i\theta}$ in polar form shows that $z^k = 1$ implies that $r^k = 1$ and $e^{i\theta k} = 1$. Thus $r = 1$ and θ is an integer multiple of $2\pi/k$. Now we note that $\langle e^{2\pi/k}, e^{2\pi/m}\rangle = \langle e^{2\pi/\ell}\rangle$ where $\ell = \mathrm{lcm}(k, n)$. Thus any finite subgroup of $\mathbb{C}^*$ is cyclic and our claim follows. **QED**We conclude this section with a few more examples of characters.

If $\dim(v) = n$ with basis $\{v_1, \ldots, v_n\}$, then S_n embeds naturally into $GL_n(\mathbb{C})$ via $v_i(\sigma\Psi) = v_{i\sigma}$. The matrix $\sigma\Psi$ is called a permutation matrix. Note that it has only one non-zero entry per row and column.For $x \in \Omega$ and $\sigma \in S_n$ we define $\mathrm{Fix}_\Omega(\sigma) := \{x \in \Omega x\sigma = x\}$.When it's clear which set is being acted on we drop the subscript Ω.We now record

Lemma

If $\Psi : S_n \longrightarrow \mathrm{GL}_n(\mathbb{C})$ *and* $\sigma \in S_n$, *then* $\mathrm{Tr}(\sigma) = |\mathrm{Fix}(\sigma)|$.

So if H is a subgroup of G of index n then the permutation action of G on the right cosets of H defines a map $\Psi_1 : G \longrightarrow S_n$. The composition of Ψ_1 with the map Ψ in the lemma above is a representation of G by permutation matrices.We call the corresponding module a *permutation module* and the corresponding character *permutation character*.

We recall that every transitive permutation action of a group G is equivalent to the action of G on the right cosets of a subgroup H via right multiplication. Thus permutation modules are a rich source of representations and characters which are relatively easy to handle from a computational point of view.
For example values of the permutation character ψ_3 of S_3 acting on $\{1, 2, 3\}$ are
$\psi_3(()) = 3$, $\psi_3((1, 2)) = 1$, $\psi_3((1, 2, 3)) = 0$
and the values of the permutation character ψ_4 of and S_4 acting on $\{1, 2, 3, 4\}$ are
$\psi_4(()) = 4$, $\psi_4((1, 2)(34)) = 0$,$\psi_4((1, 2)) = 2$, $\psi_4((1, 2, 3)) = 1$, $\psi_4((1, 2, 3, 4)) = 0$.

Integrality

Definition

An algebraic integer is a complex number that is a root of a monic integer coefficient polynomial.

Lemma

An algebraic integer which is a rational number is an integer.

Proof : If α is an algebraic integer in $\mathbb{Q}$, then $\exists r.s\mathbb{Z}$ such that $\alpha = \frac{r}{s}$. As α is an algebraic integer there exists $p(x) \in \mathbb{Z}[x]$ with $p(a) = 0$.If $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$,then evaluation of $p(x)$ at α and rewriting leads to

$$s(a_0 s^{n-1} + a_1 s^{n-2} r + \cdots + a_{n-1} r^{n-1}) = -r^n.$$

As $(s, r) = 1$, Euclids lemma implies $s = 1$, which is our claim. **QED**

Lemma

Let $\alpha_1, \ldots, \alpha_n$ be algebraic integers and let S be the smallest subring of $\mathbb{C}$ containing $\alpha_1, \ldots, \alpha_n$. Then there exists a subset Y of S such that every element of S is a $\mathbb{Z}$-linear combination of elements of elements of Y.

Proof : Let $p_i \in Z[x]$ of degree n_i such that $p(\alpha_i) = 0$.So $\alpha_i^{n_i}$ is a $\mathbb{Z}$ linear combination of lower powers of α_i. Set $Y_i = \{1\alpha_i, \alpha_i^2, \ldots, \alpha_{n_i-1}$ and set $Y := \{\prod_{i=1}^{r} \beta_i | \beta_i \in Y_i$. So as every α_i^k with $k \geq n_i$ can be expressed as a $\mathbb{Z}$-linear combination of Y_i it is now clear that every monomial $\prod_i \alpha_i^{k_i}$ is a $\mathbb{Z}$-linear combination of elements of Y. Thus R,the $\mathbb{Z}$-span R of Y,is a subring and hence $S = R$; which is our claim. **QED**

Lemma

Let $\mathbb{Z} \subset S \subset \mathbb{C}$. If S is a finitely generated $\mathbb{Z}$-module, then every element of S is an algebraic integer.

Proof : Let $Y = \{y_1, \ldots, y_n\}$ be a $\mathbb{Z}$-spanning set of S and s be in S. As usual s acts on S via right multiplication. And more explicitly we have

$$y_i s = \sum_{j=1}^{n} a_{i,j} y_j$$

for some $a_{i,j} \in \mathbb{Z}$.So if $v = (y_1, y_2, \ldots, y_n)$ and $A = (a_{i,j})$ we have $vs = vA$ which is equivalent to $v(s - A) = 0$ which implies that

$$0 = \mathrm{Det}(sI - A).$$

As $\mathrm{Det}(xI - A) \in \mathbb{Z}[x]$ we have that s is an algebraic integer. The claim follows as s was arbitrary. **QED**

Corollary

Sums and products of algebraic intergers are algebraic integers.

Proof : If α, β are algebraic integers, then by Lemma 5.3 there exists a subring *S* containing α, β which is a finitely genrated $\mathbb{Z}$-module. Evidently $\alpha + \beta, \alpha\beta \in S$ so Lemma 5.4 gives the claim. **QED**

Corollary

If χ is a character of a finite group, then $\chi(g)$ is an algebraic integer.

Proof : $\chi(g)$ is a sum of roots of unity and each such is an algebraic integer. So the previous corollary gives the claim. **QED**

Corollary

If $g \in G$ of order n and for all k with $(k, n) = 1$ there exists $h \in G$ such that $g^k = g^h$, then for every $\chi \in \mathrm{Irr}(G)$ we have $\chi(g) \in \mathbb{Z}$.

Proof : We leave the proof as an exercise for the reader.Hint: The generators of the cyclic group $\langle g \rangle$ are the elements of the form g^k with $(k, n) = 1$. **QED**

We now define for all $\chi \in \mathrm{Irr}(G)$ the function $\omega_\chi : Z(\mathbb{C}[G]) \longrightarrow \mathbb{C}$. Let Ψ be a representation affording χ and $z \in Z(\mathbb{C}[G])$.then we define the function ω_χ via the formula $z\Psi = \omega_\chi(z) I_{\chi(1)}$.By the corollary to Schur's lemma this is well defined.We drop the subscript χ from ω_χ if there is no ambiguity about χ.

If $C = g^G$, $\bar{C}$ the class sum of C then

$$\chi(1)\omega_\chi(\bar{C}) = \chi(\bar{C}) = \sum_{x \in \bar{C}} \chi(x) = |\bar{C}|\chi(g).$$

Thus

$$\omega_\chi(\bar{C}) = \frac{\chi(g)|\bar{C}|}{\chi(1)}.$$

Theorem

If $\chi \in \mathrm{Irr}(G)$, and $\bar{C} \in \mathbb{C}[G]$ is a class sum, then $\omega_\chi(\bar{C})$ is an algebraic integer.

Proof : Let $\bar{C}_1, \ldots, \bar{C}_k$ denote the class sums and recall that

$$\bar{C}_i \bar{C}_j = \sum_\nu a_{i,j,\nu} \bar{C}_\nu$$

where $a_{i,j,\nu} \in \mathbb{Z}$.As ω_χ is an algebra homomorphism we have

$$\omega_\chi(\bar{C}_i)\omega_\chi(\bar{C}_j) = \sum_\nu a_{i,j,\nu}\omega_\chi(\bar{C}_\nu).$$

Now $\omega_{\chi_1}(1) = 1$ so $S = \mathbb{Z}[\omega_i(\bar{C}_j)]$ is a subring of $\mathbb{C}$ containing $\mathbb{Z}$ and is a finitely generated $\mathbb{Z}$-module.Thus Lemma 5.4 yields the claim. **QED**

Theorem

Let $\chi \in \mathrm{Irr}(G)$. *If* $(\chi(1), |C|) = 1$ *and* $g \in C$, *the either* $g \in Z(\chi)$ *or* $\chi(g) = 0$.

Proof : By hypothesis there exist u, v such that $u\chi(1) + v|C| = 1$.So

$$\frac{\chi(g)}{\chi(1)} - u\chi(g) = \frac{\chi(g)(1 - u\chi(1)}{\chi(1)} = v\frac{\chi(g)|C|}{\chi(1)}.$$

Clearly $u\chi(g)$ is an algebraic integer and $\frac{\chi(g)|C|}{\chi}$ is an algebraic integer by the previous theorem. Thus $\alpha := \chi(g)/\chi(1)$ is an algebraic integer.If $g \notin Z(\chi)$, then $|\alpha| < 1$.Let $\mathcal{O}$ be the orbit of α under the Galois group $\mathrm{Gal}(\mathbb{Q}(e^{2\pi i/|g|}) : \mathbb{Q})$. Then $\prod_{\beta\in\mathcal{O}} \beta \in \mathbb{Q}$ as it is invariant under $\mathrm{Gal}(\mathbb{Q}(e^{2\pi i/|g|}) : \mathbb{Q})$. Also $0 \leq |\prod_{\beta\in\mathcal{O}} |\beta < 1$ as $|\beta| < 1$.So $\prod_{\beta\in\mathcal{O}} \beta \in \mathbb{Z}$ hence is equal to 0;which means all factors are equal to zero. Thus $0 = \alpha = \chi(g)/\chi(1)$ and $\chi(g) = 0$ as claimed. **QED**

Theorem

If G is a nonabelian simple group, then $1^G = \{1\}$ *is the only conjugacy class of prime power size.*

Proof : Suppose that for some $g \in G$ we have $|g^G| = p^a$ for some prime p. Let $\chi_1 \neq \chi \in \mathrm{Irr}(G)$.As G is simple and nonabelian,$\mathrm{Ker}(\chi) = 1 = Z(\chi)$.If $(p, \chi(1)) = 1$, then $\chi(g) = 0$ by our previous theorem. So, recalling that ρ is the regular character we have

$$0 = g\rho = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi(g) = 1 + \sum_{\chi \in \mathrm{Irr}(G):p|\chi(1)} \chi(1)\chi(g).$$

But that means that

$$-1 = p(\sum_{\chi \in \mathrm{Irr}(G):p|\chi(1)} \chi(1)\chi(g)/p).$$

Thus $-1/p$ is an algebraic integer;a contradiction. **QED**

Theorem

If p, q are prime integers and G is a group of order $p^a q^b$, then G is solvable.

Proof : We induct on $|G|$.If N has a proper normal subgroup, then by inductive hypothesis both G/N and N are solvable which implies that G is solvable.
So without loss we may assume that G is simple.Let P be a Sylow p-subgroup of G and let $g \in Z(P)$. Then $P \subset C_G(g)$ which shows that $|g^G| = q^c$ for some $0 \leq c \leq b$.Clearly $c \neq 0$ as $Z(G) = 1$.The previous theorem rules out all other possibilities.Thus G is not simple and the theorem follows. **QED**

Theorem

If $\chi \in \mathrm{Irr}(G)$*, then* $\chi(1)$ *is a divisor of* $|G|$.

Proof : Let $\bar{C}_1, \ldots, \bar{C}_k$ be the class sums.Recall the first orthogonality relation

$$|G| = \sum_{g \in G} \chi(g)\chi(g^{-1})$$

$$= \sum_{i=1}^{k} |\bar{C}_i|\chi(g_i)\chi(g_i^{-1}) = \sum_{i=1}^{k} \chi(1)\omega_\chi(\bar{C}_i)\chi(g_i^{-1}).$$

But now $|G|/\chi(1)$ is a rational algebraic integer; i.e. an integer. **QED**
We now see that the character degrees of a p-groups are necessarily of degree a power of p.

Consider D_{16}, the dihedral group of order 16. The character degrees are of the form 2^a where $0 \leq a \leq 4$. As $[D_{16}, D_{16}] = \mathbb{Z}/4\mathbb{Z}$ we see that D_{16} has 4 linear characters.From the second orthogonality relation we have that

$$12 = 16 - 4 = \sum_{\chi \in \mathrm{Irr}(G):\chi(1)\neq 1} \chi(1)^2.$$

Now $4^2 = 16$,hence all nonlinear characters have degree two,and there are precisely three such.
As another example consider the simple group A_5 which has 5 conjugacy classes and order 60. What are its character degrees? As A_5 is simple,the restriction of any nontrivial A_5 charater to A_4 must contain the faithful irreducible character of A_4so the degree of all the irreducible nontrivial A_5 characters must be at least 3.From the second orthogonality we know that $\chi(1) \leq 7$.Now 7 is ruled out by the theorem above and $\sqrt{(60 - 1^2 - 6^2)/3} < 3$, leaving the following possible character degrees $\{1, 3, 3, 4, 5\}$; we check that
$60 = 1^1 + 3^2 + 3^2 + 4^2 + 5^2$.

Tensor products and the representation ring

Let U, V and W be vector spaces with basis $\{v_1, \ldots, v_n\}$ repsectively $\{w_1, \ldots, w_m\}$.

Definition

A map $f : V \times W \longrightarrow U$ is called bilinear is it is linear in each argument.

Definition

The tensor product $V \otimes W$ is a vector space together with a bilinear map

$$\iota : V \times W \longrightarrow V \otimes W$$

such that if U is another vector space and $f : V \times W \longrightarrow U$ is bilinear, then there exists a unique linear map $g : V \otimes W \longrightarrow U$ such that $f = \iota g$. We define $v_i \otimes w_j := (v_i, w_j)\iota$

Lemma

The tensor product $V \otimes W$ exists, is unique and the set $\{v_i \otimes w_j\}$ is a basis for $V \otimes W$.

Proof : Existence: Let M be a space of dimension nm with basis $e_{i,j}$. The linear map $(v_i, w_j) \mapsto e_{i,j}$ can be extended to a bilinear map ι by defining $(\sum a_i v_i) \otimes (\sum b_j w_j) \mapsto \sum_{i,j} a_i b_j e_{i,j}$.Now and if $f : V \times W \longrightarrow M'$ is bilinear,then the unique map g from M to M'such that $f = \iota g$ must be the map $e_{i,j}$ to $(v_i, w_j)f$.
Uniquness: If M_1, M_2 are tensor products of V and W with corresponding bilinear maps ι_1, ι_2, then there exists maps $g_1 : M_1 \longrightarrow M_2$and $g_2 : M_2 \longrightarrow M_1$such that $\iota_2 = \iota_1 g_1$ and $\iota_1 = \iota_2 g_2$. So

$$\iota_2 I_{M_2} = \iota_2 = \iota_1 g_1 = \iota_2 g_2 g_1,$$

and thus by uniqueness

$$I_{M_2} = g_2 g_1$$

.Similarly we get $I_{M_1} = g_1 g_2$ and so uniquess is now proved.
The last part is implicit in the existence proof as $e_{i,j}$ is a basis for M.

QED

Lemma

If V and W are G-modules with bases as above, then G acts on $V \otimes W$ via $(v_i \otimes w_j)g := v_i g \otimes w_j g$.

The proof is left as an exercise.

Lemma

If V, W are G-modules affording characters χ and ϕ respectively, then the G-module $V \otimes W$ affords the charcter $\chi\phi$; where $\chi\phi(g) := \chi(g)\psi(g)$.

Proof : If $v_i g = \sum a_{i,j} v_j$ and $w_k g = \sum b_{k,\ell} w_\ell$,then

$$(v_i \otimes w_k)g = v_i g \otimes w_k g = \sum_{j,\ell} a_{i,j} b_{k,\ell} v_j \otimes w_\ell,$$

So the trace of the matrix representing g with respect to the basis $\{v_i \otimes w_k\}$ is

$$\sum_{i,k} a_{i,i} b_{k,k} = (\sum_i a_{i,i})(\sum_k b_{k,k}).$$

QED

Lemma

If V is an $\mathbb{F}[G]$-module, then $V^* := \mathrm{Hom}_{\mathbb{F}}(V, \mathbb{F})$ becomes an $\mathbb{F}[G]$-module via: For $\alpha \in V^*$ we define αg via $v(\alpha g) = (vg^{-1})\alpha$ for all $v \in V$. .

Proof : Let $v \in V$, $\alpha \in V^*$ and $g, h \in G$.We have

$$v(\alpha(gh)) = (vh^{-1}g^{-1})\alpha = (vh^{-1})(\alpha g) = v((\alpha g)h),$$

proving that $\alpha(gh) = (\alpha g)h$. **QED**The module V^* is the *dual $\mathbb{F}[G]$-module* of V

Lemma

If $v_1, \ldots, v_n$ is a basis for V, then the set $v_1^*, \ldots, v_n^*$ where $v_i v_j^* := \delta_{i,j}$ is a basis for V^*

Proof : If $v^* \in V^*$, then $v^* = \sum_i (v_i v^*) v_i^*$ showing that $v_1^*, \ldots, v_n^*$ spans V^*.Now if $\sum_i a_i v_i^* = 0$, then

$$0 = v_i \sum_i a_i v_i^* = a_i,$$

showing that $v_1^*, \ldots, v_n^*$ is linearly independent. **QED**The set $v_1^*, \ldots, v_n^*$ is called the *dual basis* of V.

Lemma

If V is a $\mathbb{C}[G]$-module affording χ, then the character χ^* afforded $V*$ is equal to $\overline{\chi}$.

Proof : Find a basis $\{v_1, \ldots, v_n\}$ with respect to which g acts diagonaly, say $v_i g = \lambda_i$.Then

$$v_j(v_i^* g) = (v_j g^{-1}) v_i^* = \lambda_j^{-1} \delta_{i,j},$$

showing that g acts diagonaly on V^* with respect to the dual basis. Also, as the λ_i are roots of unity, we have
$\chi^*(g) = \lambda_1^{-1} + \cdots + \lambda_n^{-1} = \overline{\lambda_1} + \cdots + \overline{\lambda_n} = \overline{\chi}$. **QED**

Lemma

If χ, ψ and ϕ are characters, then

1. $[\chi, \psi\phi] = [\chi\overline{\psi}, \phi]$
2. *If $\chi \in \mathrm{Irr}(G)$, then* $1 = [\chi\chi^*, 1_G] = [\chi, \chi]$

Proof : Evidently the second part follows from the first. For the first part note that

$$[\chi, \psi\phi] = \frac{1}{|G|}\sum_{g\in G}\chi(g)\overline{\psi(g)\phi(g)}$$

$$= \frac{1}{|G|}\sum_{g\in G}(\chi(g)\overline{\psi(g)})\overline{\phi(g)} = [\chi\overline{\psi}, \phi]$$

QEDWe now see that characters of a group can be added and multiplied component wise to yield new characters. Also the set of class functions is a ring under the operations of component wise addition and multiplication.

Definition

The representation ring $R_{\mathbb{C}}(G)$ of a group G is the subring $\mathbb{Z}[\mathrm{Irr}(\mathbb{C}[G]]$ of the ring of class functions of G.

The additive group of $R_{\mathbb{C}}(G)$ is an example of a Grothendieck group built from the monoid whose elements are the isomorphism classes of $\mathbb{C}[G]$-modules. The representation ring is usually defined by starting with the Grothendieck of the monoid of isomorphism classes of $\mathbb{C}[G]$-modules,and extending that to a ring structure where the mutliplication operation is the tensor product.Our definition is equivalent to the standard definition. The elements in $R_{\mathbb{C}}(G)$ which are not positive linear combinations of irreducible characters are called *virtual characters*.

The next theorem can be interpreted as general result concerning the multiplication in the representation ring of a general group.It is also a useful tool for generating new characters from old and can, in practice, be used to help compute character tables.

Theorem

(Brauer) Let ψ be a faithful character of a finite group G. Suppose that ψ takes on exactly m distinct values. Then for every $\chi \in \mathrm{Irr}(G)$ there exists some $0 < k \leq m$ such that $[\chi, \psi^k] \neq 0$.

Proof : Let $\{\psi(1) = \alpha_1, \ldots, \alpha_m\} = \mathrm{Im}(\psi) \subset \mathbb{C}$. Define $G_i := \{g \in G \ : \ \psi(g) = \alpha_i\}$.So $G_1 = \mathrm{Ker}(\psi)$.
Now let $\chi \in \mathrm{Irr}(G)$and let $\beta_i = \sum_{g \in G_i} \overline{\chi(g)}$.Then

$$[\psi^k, \chi] = \frac{1}{|G|} \sum_{i=1}^{m} (\alpha_i)^j \beta_i$$

.
If χ is not a consituent of ψ^j for all $j < m$, then

$$[\beta_1, \ldots, \beta_m](\alpha_i^j) = 0$$

.But (α_j^i) is a Vandermonde matrix hence its determinant is $\pm \prod_{i \neq j}(\alpha_i - \alpha_j) \neq 0$. Thus $b_i = 0$ for all i. But $\beta_1 = \chi(1) \neq 0$; a contradiction.

QEDWe remark that the fact that every irreducible character is a constituent of the regular character is a special case of Brauers theorem above.

We conclude this section with

Theorem

Let $G = H \times K$, then $\mathrm{Irr}(G) = \mathrm{Irr}(H) \times \mathrm{Irr}(K)$.

Proof : Let $\psi_1, \psi_2 \in \mathrm{Irr}(H)$ and $\chi_1, \chi_2 \in \mathrm{Irr}(K)$. Then

$$[\psi_1 \times \chi_1, \psi_2 \times \chi_2] = \frac{1}{|H||K|} \sum_{(h,k)} \psi_1(h)\chi_1(k)\overline{\psi_2(h)\chi_2(k)}$$

$$= (\frac{1}{|H|} \sum_{h \in H} \psi_1(h)\overline{\psi_2(h)})(\frac{1}{|K|} \sum_{k \in K} \chi_1(k)\overline{\chi_2(k)}) = [\psi_1, \psi_2][\chi_1, \chi_2]$$

Thus the characters $\psi_i \times \chi_i$ are irreducible and distinct. Now we compute that

$$\sum_{\psi \times \chi \in \mathrm{Irr}(H) \times \mathrm{Irr}(K)} \psi \times \chi(1) = \sum_{\psi \times \chi} \psi(1)^2 \chi(1)^2$$

$$= (\sum_{\psi \in \mathrm{Irr}(H)} \psi(1)^2)(\sum_{\chi \in \mathrm{Irr}(K)} \chi(1)^2) = |H||K| = |G|,$$

showing that every character is of the desired form. **QED**

Involutions and the Brauer-Fowler Thereom

We now want to use characters to count involutions in finite groups and prove the Brauer-Fowler theorem which provides about half of the philosophical underpinning of the classification of the finite simple groups.The other half off course being the Odd Order Theorem by Feit and Thompson.
We define

$$\Theta_n(g) := |\{x \in G \mid x^n = g\}|$$

and observe that Θ_n is a class function and that $\Theta_2(1)$ counts the number of elments of order at most 2 in G. Thus $\Theta_2(1) = 1 + t$ where t is the number of involutions in G.

Lemma

If $(n, |G|) = 1$*, then* $\Theta_n(g) = 1$ *for all* $g \in G$*.*

Proof : Let $m \in \mathbb{Z}$ be such that $nm = 1 \bmod |G|$,then if $h^n = k^n$ we have

$$h = h^{nm} = (h^n)^m = (k^n)^m = k^{nm} = k$$

and so the map $x \longrightarrow x^n$ is injective. But as G is a finite set the map must also be surjective and the claim follows. **QED**

As Θ_n is a class function it uniquely expressible as a linear combination of irreducibles; i.e., we have

$$\Theta_n = \sum_{\chi \in \mathrm{Irr}(G)} \nu_n(\chi)\chi.$$

Lemma

$\nu_n(\chi) = \frac{1}{|G|}\sum_{g\in G}\chi(g^n)$.

Proof : The orthogonality relations give

$$\nu_n(\chi) = [\Theta_n, \chi] = \frac{1}{|G|}\sum_{g\in G}\Theta_n(g)\overline{\chi(g)}.$$

Now $\Theta_n(g)\overline{\chi(g)} = \sum_{h\in G\,:\,h^n=g}\overline{\chi(h^n)}$ so we get

$$\nu_n(\chi) = \frac{1}{|G|}\sum_{h\in G\,:\,h^n=g}\overline{\chi(h^n)}.$$

Replacing h by h^{-1} yields the claim. **QED**

For a class function ϕ define $\phi^{(n)}(g) := \phi(g^n)$. So the previous lemma is the assertion that $\nu_n(\chi) = [\phi^{(n)}, 1_G]$.

Theorem

(Frobenius-Schur) If $\chi \in \mathrm{Irr}(G)$*, then*

1. $\chi^{(2)}$ *is the difference of two characters,*
2. $\nu_2(\chi) \in \{-1, 0, 1\}$*,*
3. $\nu_2(\chi) \neq 0$ *if and only if* $\chi(g) \in \mathbb{R}$ *for all* $g \in G$*.*

Proof : Let V be a $\mathbb{C}[G]$-module affording χ. Let $W = V \otimes V$ and let $\tau : W \longrightarrow W$ be the linear transformation defined by $v \otimes w\tau = w \otimes v$. Note that $\tau^2 = 1$ and thus τ has at most two eigenvalues, namely ± 1. The 1 eigenspace of τ is called the *symmetric square of* V and is denoted by W_S whereas the 1 eigenspace of τ is called the *alternating square of* V and is denoted by W_A. If $\dim(V) \geq 2$, and if $v, w \in V$ are linearly independent, then $0 \neq v \otimes w + w \otimes v \in W_S$ whereas $0 \neq v \otimes w - w \otimes v \in W_A$.Now we observe that τ is a $\mathbb{C}[G]$ homomorphism as

$$(v \otimes w)\tau g = wg \otimes vg = (vg \otimes wg)\tau = (v \times w)g\tau.$$

So W_S and W_A are $\mathbb{C}[G]$-modules with corresponding characters χ_S and χ_A and

$$\chi^2 = \chi_S + \chi_A.$$

Let $v_1, \ldots, v_n$ be a basis for V. Then the set $e_{i,j} := v_i \otimes v_j - v_j \otimes v_i$ where $j > i$ is a basis for W_A. If $g \in G$ and $v_i g = \sum_j \alpha_{i,j} v_j$, then

$$e_{i,j}g = v_i g \otimes v_j g - v_j g \otimes v_i g$$

$$= \sum_{r,s} (\alpha_{i,r}\alpha_{j,s} - \alpha_{j,r}\alpha_{i,s}) v_r \otimes v_s = \sum_{r<s} (\alpha_{i,r}\alpha_{j,s} - \alpha_{j,r}\alpha_{i,s}) e_{r,s}.$$

Thus

$$\chi_A(g) = \sum_{i<j} (\alpha_{i,i}\alpha_{j,j} - \alpha_{i,j}\alpha_{j,i}.$$

So

$$2\chi_A(g) = \sum_{i \neq j} (\alpha_{i,i}\alpha_{j,j} - \alpha_{i,j}\alpha_{j,i}$$

$$= (\sum_i \alpha_{i,i})(\sum_j \alpha_{j,j}) - \sum_{i,j} \alpha_{i,j}\alpha_{j,i}.$$

Which proves

$$2\chi_A(g) = \chi(g)^2 - \chi(g^2) = \chi^2(g) - \chi^{(2)}(g).$$

Rewriting yields our first claim.

Now

$$\nu_2(\chi) = [\chi^{(2)}, 1_G] = [\chi^2, 1_G] - 2[\chi_A, 1_G].$$

χ is real valued if and only if $\chi = \overline{\chi}$. So if χ is not real valued, then

$$0 = [\chi, \overline{\chi}] = [\chi^2, 1_G] = [\chi_S, 1_G] + [\chi_A, 1_G],$$

which implies that

$$[\chi_S, 1_G] = 0 = [\chi_A, 1_G]$$

and thus $\nu_2(\chi) = 0$. On the other hand if χ is real valued, then

$$1 = [\chi, \overline{\chi}] = [\chi^2, 1_G] = [\chi_S, 1_G] + [\chi_A, 1_G].$$

If $[\chi_S, 1_G] = 1$ then $0 = [\chi_A, 1_G]$ and thus $\nu_2(\chi) = 1 - 2 \times 0 = 1$. Or if $[\chi_S, 1_G] = 0$ then $1 = [\chi_A, 1_G]$ and thus $\nu_2(\chi) = 1 - 2 \times 1 = -1$. The proof is now complete. **QED**

A direct application of the Frobenius-Schur Theorem is a character theoretic formula for the number of involutions in a finite group.

Corollary

If G has exactly t involutions, then

$$1 + t = \nu_2(\chi) = \Theta_2(\chi) = \sum_{\chi \in \mathrm{Irr}(G)} \nu_2(\chi)\chi_1.$$

The number $\nu_2(\chi)$ is called the *Frobenius-Schur indicator*. Form our setup the following is clear

Lemma

Let $\chi \in \mathrm{Irr}(G)$*. Then*

$$[1_G, \chi_S] + [1_G, \chi_A] = [1_G, \chi^2] = [\overline{\chi^2}, 1_G] = [\overline{\chi_S}, 1_G] + [\overline{\chi_A}, 1_G]$$

Recall that $\overline{\chi}$ is the character of the dual of V. Now V^* is the set of 1-forms on V and so $V^* \otimes V^*$ is the set of two forms of V. The symmetric 2-forms are symmetric bilinear forms whereas the anti-symmetric 2-forms are the alternating forms (also known as symplectic forms). The stabilizer in $\mathrm{GL}_n(\mathbb{C})$ of a non-degenerate quadratic form is an orthogonal group,whereas the stabilizer in $\mathrm{GL}_n(\mathbb{C})$ of a non-degenerate alternating form is a symplectic group. So if Ψ is a representation affording χ and $\nu_2(\chi) = 1$, then $\mathrm{Im}(\Psi)$ is contained in an orthogonal group,and if $\nu_2(\chi) = -1$, then $\mathrm{Im}(\Psi)$ is contained in an symplectic group.

Corollary

If $\chi \in \mathrm{Irr}(G)$ *and* $[1_G, \chi_S] = 1$ *respectively* $[1_G, \chi_A] = 1$*, then the G-invariant quadratic repsectively G-invariant symplectic form is non-degenerate.*

Proof : If V is a G-module affording χ and $f : V \times V \longrightarrow \mathbb{C}$ a bilinear G-inavriant map;i.e. $f(v, w) = f(vg, wg)$ for all $v, w \in V$ and all $g \in G$. So $v \in V^{\perp}$ iff $f(v, w) = 0$ for all $w \in V$ iff $0 = f(vg, wg)$ for all $wg \in W$ iff $vg \in V^{\perp}$. So $V^{\perp}$ is a G-submodule of V. As G acts irreducibly on V is is the case either $V = V^{\perp}$ or that $V^{\perp} = 0$. In the former case $f(v, w) = 0$ for all $v, w \in V$ i.e. f is trivial and in the second case f is non-degenerate. **QED**

Lemma

If $a_1, \ldots, a_n \in \mathbb{R}$*, then*

$$\sum_i a_i^2 \geq \frac{1}{n}(\sum a_i)^2$$

Proof : This a special case of Schwarz' inequality

$$(\sum_i a_i b_i)^2 \leq (\sum a_i^2)(\sum_i b_i^2)$$

obtained by setting all $b_i = 1$. **QED**

Theorem

Let G be a group of even order n and exactly t involutions. Set $\alpha = (n-1)/t$*. The following are true*

1. *There exists* $1 \neq g \in G$*, with* $[G : C_G(g)] \leq \alpha^2$*.*
2. *There exists* $1_G \neq \chi \in \mathrm{Irr}(G)$*, with* $\chi = \overline{\chi}$ *and* $\chi(1) \leq \alpha$*.*

Proof : By RV we denote the non-trivial real valued irreducible characters of G. By Corollary 7.4 we have

$$0 < (n-1)/\alpha = t \leq \sum_{RV} \chi(1).$$

Thus we see that $|RV| \geq 1$. Thus

$$t^2 \leq (\sum_{\chi \in RV} \chi(1))^2 \leq |RV| \sum_{\chi \in RV} \chi(1)^2 \leq (|RV|(n-1)).$$

As $t = (n-1)/\alpha$ this shows that

$$n - 1 \leq |RV|\alpha^2.$$

Hence

$$\sum_{R} V\chi(1)^2 \leq |RV|\alpha^2.$$

Thus for some $\chi \in RV$ we have $\chi(1) \leq \alpha$; proving part 2.
Now $|RV| \leq (k-1)$, where $k = |\mathrm{Irr}(G)|$. So

$$n - 1 \leq |RV|\alpha^2. \leq (k-1)\alpha^2.$$

Thus not all non-identity classes of G can be larger that α^2 and part 1 follows. **QED**

Theorem

(Brauer-Fowler) Let $m \in \mathbb{N}$. There exist at most finitely many simple groups containing an involution with centralizer of order at most m.

Proof : If G is simple of order n, then G contains at least n/m involutions and hence $(n-1)/t = \alpha < m$. Thus there exists $1 \neq g \in G$ with $1 < [G : C_G(g)] < m^2$. Thus G embeds into A_{m^2-1}. **QED**

For example G is simple and $x \in G$ is an involution such that $|C_G(x)| = 4$, then G is a subgroup of A_{15}. Note that A_5 is a simple group of order 60 such that the centralizer of every involution has order 4.

Theorem

(Feit-Thompson) Every finite group of odd order is solvable. In particular nonabelian simple groups possess involutions.

The proof of the Feit-Thompson is over 200 pages long. The first part restricts the structure of the normalizers of p-subgroups,that is the *local* subgroups, of a mimimal simple nonabelian group G of odd order. The local analysis is then exploited in the character theoretic analysis which culminates in the establishing the existence of two local maximal solvable subgroups of G.The final contradiciton is a 25 page generator and relation calculation showing that $G = 1$.
The classification of the finite simple groups is organized around the analysis of involution centralizers.The exisiting proof is over 15000 pages long and spread out over 100+ books and journal articles.It is an ongoing effort of high current interest to simplify the existing proof and to give an account of the classification in under 5000 pages.
The series of problems is desigend to establish

Theorem

If G is a simple group which possesses an involution centralizer of order 4*, then* $G \cong A_5$.

Induced characters, Frobenius reciprocity, permutation characters.

We have already seen that if $N \lhd G$ then $\mathrm{Irr}(G/N)$ embeds into $\mathrm{Irr}(G)$.In this section we begin to relate characters and class functions of H and G where H is a subgroup of G.This is a subtle business and is an active area of modern research. However, there are off course many classical results some of which we will now explore.

Lemma

If ψ is a class function of G and H is a subgroup of G, then $\psi|_H$ is a class function of H. Moreover if ψ is a character and Ψ is a representation affording ψ, then ψ_H is the charcter of H afforded by $\Psi|_H$.

Proof : Clear **QED**

Definition

For $H \subset G$ and a class function ψ of H define

$$\psi \uparrow^G := \frac{1}{|H|} \sum_{x \in G} \phi^o(xgx^{-1})$$

where $\phi^o(y) = \psi(y)$ if $y \in H$ and 0 otherwise. The class function $\psi \uparrow^G$ is called the induced class function.

Clearly $\psi \uparrow^G$ is a class function of G and moreover $\psi \uparrow^G (1) = [G : H]\psi(1)$.The formula in the definition of above can be rewritten as

$$\psi \uparrow^G = \sum_{t \in T} \phi^o(tgt^{-1})$$

where T is a *right transversal* of H in G;i.e., T is a set of right coset representatives of H in G.

Theorem

(Frobenius Reciprocity) If H is a subgroup of G and ψ, χ are class functions of H and G respectively, then

$$[\psi \uparrow^G, \chi] = [\psi, \chi|_H].$$

Proof : We have

$$[\psi \uparrow^G, \chi] = \frac{1}{|G|} \sum_{g \in G} \psi \uparrow^G (g)\chi(g) = \frac{1}{|G||H|} \sum_{g \in G} \sum_{x \in G} \psi^o(xgx^{-1})\chi(g)$$

Now set $y = xgx^{-1}$ and observe that $\chi(g) = \chi(y)$ to see that

$$[\psi \uparrow^G, \chi] = \frac{1}{|G||H|} \sum_{y \in G} \sum_{x \in G} \psi^o(y)\chi(y) = \frac{1}{|H|} \sum_{y \in H} \psi(y)\chi(y) = [\psi, \chi|_H].$$

QED

Corollary

If H is a subgroup of G and $\psi \in \mathrm{Irr}(H)$, then there exists $\chi \in \mathrm{Irr}(G)$ such that ψ is a constituent of $\chi|_H$.

Proof : Let χ be an irreducible constituent of $\psi \uparrow^G$, then

$$0 \neq [\psi \uparrow^G, \chi] = [\psi, \chi|_H].$$

Before we give examples of induced characters we want to reformulate the definition of induced class function in a slightly more convenient way. To this end we assume that H is a subgroup of G and that ψ is a character of H.Now if $g \in G$, then $g^G \cap H$ is a union of H conjugacy classes and let's say that these are represented by $x_1, \ldots, x_m \in H$. We have

$$\psi \uparrow^G (g) = \frac{1}{|H|} \sum_{x \in G} \psi^o(xgx^{-1}) = |C_G(g)| \sum_{i=1}^{m} \frac{\psi(x_i)}{|C_H(x_i)|}.$$

Just like tensoring known irreducibles leads to new irreducible characters so does and induction of irreducibles of subgroups.We illustrate the latter to compute the character tables of D_{10} and A_5.First we consider the character table of D_{10}. The conjugacy classes of D_{10} (as a subgroup of S_5) are (),$x := (2,5)(3,4)$,$y := (1,2,3,4,5)$, $(1,3,5,2,4)$ with centralizer orders 10, 2,5 and 5 respectively. Let H be the Sylow 5-subgroup of D_{10}.Let $\zeta_5 := e^{2\pi i/5}$.We compute that

$$1_H \uparrow^{D_{10}} (()) = 10/5 = 2$$

$$1_H \uparrow^{D_{10}} (x) = 0$$

$$1_H \uparrow^{D_{10}} (y) = 5 \times (1+1)/5 = 2$$

This yields

g_i	$()$	$(1,2)(3,4)$	$(1,2,3,4,5)$	$(1,3,5,2,4)$
$\lvert C_G(g_i)\rvert$	10	2	5	5
χ_1	1	1	1	1
χ_2	1	-1	1	1
χ_3	?	?	?	?
χ_4	?	?	?	?

where ? denotes yet to be determined entries.

Next we induce the linear character λ of H whose at y is ζ_5. We compute

$$\lambda_H \uparrow^{D_{10}} (()) = 10/5 = 2$$

$$\lambda_H \uparrow^{D_{10}} (x) = 0$$

$$\lambda_H \uparrow^{D_{10}} (y) = 5(\zeta_5 + \zeta_5^4)/5 = (\zeta_5 + \zeta_5^4)$$

$$\lambda_H \uparrow^{D_{10}} (y^2) = 5(\zeta_5^2 + \zeta_5^3)/5 = (\zeta_5^2 + \zeta_5^3)$$

As $\lambda_H \uparrow^{D_{10}}$ is clearly not a linear combination of χ_1 and χ_2 we can deduce that $\lambda_H \uparrow^{D_{10}}$ must be irreducible.Next we see that $\overline{\lambda_H \uparrow^{D_{10}}} \neq \lambda_H \uparrow^{D_{10}}$ which yields our last irreducible.Thus the character table of D_{10} is

g_i	$()$	$(1,2)(3,4)$	$(1,2,3,4,5)$	$(1,3,5,2,4)$
$\lvert C_G(g_i)\rvert$	10	2	5	5
χ_1	1	1	1	1
χ_2	1	-1	1	1
χ_3	2	0	a	$\overline{a}$
χ_4	2	0	$\overline{a}$	a

where $a = \zeta_5 + \zeta_5^4$.

Now we turn to the character table of A_5. Recall that the conjugacy class representatives of A_5 are $()$, $(1,2)(3,4)$, $(1,2,3)$, $(1,2,3,4,5)$, and $(1,3,5,2,4)$, with centralizer orders 60,4,3,5, and 5 repsectively.The permutation character ρ_5 has values $[5,1,2,0,0]$ and $[4,0,1,-1,-1] = \rho_5 - \chi_1 \in \mathrm{Irr}(A_5)$.Recall that we know aleady that the character degrees of A_5 are $1,3,3,4$ and 5. We record what we have in the table below.

g_i	$()$	$(1,2)(3,4)$	$(1,2,3)$	$(1,2,3,4,5)$	$(1,3,5,2,4)$
$\lvert C_G(g_i)\rvert$	60	4	3	5	5
χ_1	1	1	1	1	1
χ_2	3	?	?	?	?
χ_3	3	?	?	?	?
χ_4	4	0	1	-1	-1
χ_5	5	?	?	?	?

where ? denotes yet to be determined entries.

The normalizers of the Sylow 2, 3, and 5-subgroups of A_5 are A_4,D_6 and D_{10} respectively.
We want to induce the trivial character of D_{10}.Now by Sylow's Theorem $(1,2)(3,4)^{A_5} \cap D_{10} = (1,2)(3,4)^{D_{10}}$.As the Sylow 5-subgroup of A_5 is abelian conjugacy is determined in the normalizer. So $1_{D_{10}} \uparrow^{A_5} (()) = 6$,
$1_{D_{10}} \uparrow^{A_5} ((1,2)(3,4)) = 4 \times 1_{D_{10}}((1,2)(3,4))/2 = 2$,
$1_{D_{10}} \uparrow^{A_5} ((1,2,3)) = 0$, $1_{D_{10}} \uparrow^{A_5} ((1,2,3,4,5)) = 5 \times 1/5 = 1$and
$1_{D_{10}} \uparrow^{A_5} ((1,3,5,2,4)) = 5 \times 1/5 = 1$.So

$$1_{D_{10}} \uparrow^{A_5} = [6,2,0,1,1].$$

Now the inner product of the character with itself is

$$[1_{D_{10}} \uparrow^{A_5}, 1_{D_{10}} \uparrow^{A_5}] = \frac{1}{60}(36 + 15 \times 4 + 12 \times 1 + 12 \times 1) = 2$$

and

$$[1_{D_{10}} \uparrow^{A_5}, \chi_1] = \frac{1}{60}(6 + 15 \times 2 + 12 \times 1 + 12 \times 1) = 1.$$

So now we have that $[5,1,-1,0,0] = 1_{D_{10}} \uparrow^{A_5} -\chi_1 \in \mathrm{Irr}(A_5)$ and we record our currect statement of affairs in

g_i	()	$(1,2)(3,4)$	$(1,2,3)$	$(1,2,3,4,5)$	$(1,3,5,2,4)$
$\lvert C_G(g_i)\rvert$	60	4	3	5	5
χ_1	1	1	1	1	1
χ_2	3	?	?	?	?
χ_3	3	?	?	?	?
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

Now we need to determine the character values of χ_2 and χ_3. To this end we observe that $\chi_2|_{A_4}$ and $\chi_3|_{A_4}$ must contain a faithful constituent. But now we see from our earlier calculation that the only faithful A_4 character of is of degree 3.Thus $\chi_2(()) = \chi_3(()) = 3$,$\chi_2((1,2)(3,4)) = -1 = \chi_3((1,2,)(3,4))$. and $\chi_2((1,2,3)) = 0 = \chi_3((1,2,3))$. Thus we have

g_i	()	$(1,2)(3,4)$	$(1,2,3)$	$(1,2,3,4,5)$	$(1,3,5,2,4)$
$\lvert C_G(g_i)\rvert$	60	4	3	5	5
χ_1	1	1	1	1	1
χ_2	3	-1	0	a	b
χ_3	3	-1	0	c	d
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

where a, b, c, d are yet to be determined.

To find the last four entries we restrict χ_2 to D_{10} which yields the D_{10} character $[3, -1, a, b]$ which due to the simplicity of A_5 must be faithful. So it must be the sum of the second and either the third or fourth irreducible character of D_{10}.Whichever it is, it is, the resulting A_5 character will not be self dual.Thus without loss we can set it up that $a = 1 + (\zeta_5 + \zeta_5^4)$ and $b = 1 + (\zeta_5^2 + \zeta_5^3) = \overline{a}$.Then taling duals yields that $c = b$ and $d = a$. So the character table of A_5 is

g_i	()	$(1,2)(3,4)$	$(1,2,3)$	$(1,2,3,4,5)$	$(1,3,5,2,4)$
$\lvert C_G(g_i)\rvert$	60	4	3	5	5
χ_1	1	1	1	1	1
χ_2	3	-1	0	a	$\overline{a}$
χ_3	3	-1	0	$\overline{a}$	a
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

where $a = 1 + \zeta_5 + \zeta_5^4$.

We now turn to the module theoretic interpretation of character induction.

Definition

Let V be an $\mathbb{F}[G]$-module.We call $V = \oplus_{i=1}^{k} V_i$ an imprimitivity decomposition if for all $g \in G$ and all V_i we have $V_i g = V_j$ and for all V_i, V_j there exists $h \in G$ such that $V_i h = V_j$. If V has an imprimitivity decomposition we say that the G-module V is imprimitive. If V does not possess an imprimitivity decomposition then we say that V is a primitive G-module.

Assume now that the $\mathbb{F}[G]$-module V has impimitivity decomposition $\oplus_{i=1}^{k} V_i$.Let $H := \{h \in G \ : \ V_1 h = V_1\}$ be the stabilizer of V_1. Clearly V_1 is an H-module.Note that $k = [G : H]$ as G acts transitively on the set $\{V_1, \ldots, V_k\}$.

Theorem

Let V, G, V_i and H be as above.Assume $\mathbb{F} \subset \mathbb{C}$, that V affords the $\mathbb{F}[G]$-character χ,and V_1 affords the $\mathbb{F}[H]$-character ψ. We have that $\chi = \psi \uparrow^G$.

Proof : Let $T := \{1 = t_1, t_2, ..., t_k\}$ be a right transversal of H in G.Without loss we may set things up in a way that $V_s = V_1 t_s$. We compute the character value of g on V. Now if $g \in G$ then $V_i g = V_i$ if an only if $V_1 t_i g = V_1 t_i$ if and only if $t_i g t_i^{-1} \in H$. Thus the contribution of V_i to the trace of g is the trace of $t_i g t_i^{-1}$ on V_1; i.e. $\psi^0(t_i g t_i^{-1})$. So $\chi(g) = \sum_i \psi^0(t_i g t_i^{-1}) = \psi \uparrow^G (g)$ and the claim follows. **QED**

Definition

Let W be an $\mathbb{F}[H]$-module and $H \subset G$.

$$W \otimes_{\mathbb{F}[H]} \mathbb{F}[G] := (W \otimes \mathbb{F}[G])/R$$

where $R := \langle w \otimes hg = wh \otimes g \ : \ \forall\, w \in W$ and $h \in H \rangle$.

Lemma

Let W be an $\mathbb{F}[H]$-module and $H \subset G$. $W \otimes_{\mathbb{F}[H]} \mathbb{F}[G]$ is a G-module of dimension $[G : H]\dim(W)$

Proof : Let $k = [G : H]$ and let $T := \{t_1, \ldots, t_k\}$ be a right transversal of H in G.Define $V_i := \{w \otimes t_i \ : \ w \in W\}$. Clearly V_i is a subspace of dimension $\dim(W)$.Now if $g \in Ht_i$, then
$0 \neq w \otimes g = w \otimes ht_i = wh \otimes t_i \in V_i$, which shows that the V_i's span V. Now note that
$\dim(R) \leq \sum_{t \in T}(|H| - 1)\dim(W) = (|G| - [G : H])\dim(W)$and hence $\dim(W \otimes_{\mathbb{F}[H]} \mathbb{F}[G]) = |G|\dim(W) - \dim(R) \geq [G : H]\dim(W)$. The fact that the V_i span V proves that the reverse inequality also holds and thus our lemma follows. **QED**

Theorem

If W is an $\mathbb{F}[H]$-module then there exists an $\mathbb{F}[G]$-module V with imprimitivity decomposition $\oplus_{i=1}^{r} V_i$ such that $V_1 H = V_1$ and W is isomorphic to V_1 as an H-module.

Proof : Take $V = W \otimes_{\mathbb{F}[H]} \mathbb{F}[G]$.Keeping the notation of the previous lemma we already have $V = \oplus_{i=1}^{k} V_i$.Let $g \in G$ and $v \in V_i$.Then there exists $w \in V_1$ such that $v = w \otimes t_i$. Thus

$$vg = (w \otimes t_i)g = w \otimes (t_i g) = w \otimes (ht_j) = wh \otimes t_j \in V_j$$

so $V_i g = V_j$ proving that $\oplus_{i=1}^{k} V_i$ is an imprimitivity decomposition of V. Evidently V_1 is an H-module isomorphic to W and our theorem follows. **QED**

We now see that permutation characters are in fact examples of induced characters. We also see that if λ is a representation of H of degree 1, then with respect to the basis $\{\lambda \otimes t_i\}$every $g \in G$ acts on $\lambda \uparrow^G$ as a monomial matrix.

Definition

A character χ of G is monomial if it is induced from some linear character of some subgroup H of G.A group G is called an M-group if every $\chi \in \mathrm{Irr}(G)$ is monomial.

Lemma

If θ is a character of $H \subset G$, then

$$\mathrm{Ker}(\theta \uparrow^G) = \cap_{x \in G} (\mathrm{Ker}\theta)^x$$

Proof : $g \in \mathrm{Ker}(\theta \uparrow^G)$ if and only if

$$\sum_{x \in G} \theta^0(xgx^{-1}) = \sum_{x \in G} \theta(1).$$

But now $|\theta^0(xgx^{-1})| \leq \theta(1)$ and thus $xgx^{-1} \in \mathrm{Ker}(\theta)$ for all $x \in G$; i.e. $g \in \mathrm{Ker}(\theta)^x$ for all $x \in G$. **QED**

By $G^{(i)}$ we denote the i'th term of the derived series of G. Recall that is defined recursively via $G^(i) := [G^{(i-1)}, G^(i-1)]]$ and $G^(1) := [G, G]$.

Theorem

Let G be an M-group and let $1 = d_1 < d_2 < \cdots < d_k$ be the set of distinct irreducible character degrees of G. Let $\chi \in \mathrm{Irr}(G)$ with $\chi(1) = d_i$. Then $G^(i) \subset \mathrm{Ker}(\chi)$.

Proof : We induct on i.If $i = 1$, then every character of degree $d_1 = 1$ is linear and thus $G^(1) \subset \mathrm{Ker}(\chi)$. So assume that $i > 1$. Pick $\psi \in \mathrm{Irr}(G)$ with $\psi(1) = d_{i1}$.Then

$$G^{(i)} \subset G^{(i-1)} \subset \mathrm{Ker}(\psi).$$

Now $\chi = \lambda \uparrow^G$ for some linear character λ of H. Now $\lambda \neq 1_H$, as

$$[1_H \uparrow^G, 1_G] = [1_H, 1_H] = 1$$

and hence the permutation character $1_H \uparrow^G$ is never irreducible.Now if ψ is a constituent of $1_H \uparrow^G$, then $\psi(1) \leq [G : H] = \lambda \uparrow^G (1) = \chi(1)$ and thus $G^{(i-1)} \subset \mathrm{Ker}(\psi)$ and thus $G^{(i-1)} \subset H$.Thus

$$G^{(i)} \subset H^{(1)} \subset \mathrm{Ker}(\lambda).$$

So as $G^{(i)} \lhd G$ we have

$$G^{(i)} \subset \cap_{x \in G} (\mathrm{Ker}\lambda)^x = \mathrm{Ker}(\chi).$$

Which is our claim. **QED**

Thus if G is an M-group, then $G^{(i)} \subset \mathrm{Ker}(\rho) = 1$, where ρ is the regular character. So we have proved:

Corollary

(Taketa) M-groups are solvable.

We will now make precise the connetion between induced characters and permutation characters and derive a few consequences.

Lemma

If G acts transitively on Ω with point stabilizer G_α for $\alpha \in \Omega$, then $1_{G_\alpha} \uparrow^G$ is the permutation character of the action.

Proof : Let V be the permutation module comming from the G-action on Ω (see Lemma 4.22 and the discussion for more detail). Then $\sum_{\omega \in \Omega} \langle v_\omega \rangle$ is an imprimitivity decomposition of V. **QED**

Corollary

If G acts on Ω which permutation character χ, then $[\chi, 1_G] = k$ is equal to the number of orbits of G on Ω.

Proof : If G is transitive then $[\chi, 1_G] = [1_{G_\alpha} \uparrow^G, 1_G] = [1_{G_\alpha}, 1_{G_\alpha}] = 1$.(The second $=$ is due to Frobenius Reciprocity.)Now it G has k orbits with orbit representatives $\alpha_1, \ldots, \alpha_k\}$, then $\chi = \sum_{a_i} 1_{G_{a_i}} \uparrow^G$ and hence

$$[\chi, 1_G] = [\sum_{a_i} 1_{G_{a_i}} \uparrow^G, 1_G] = \sum_{a_i} [1_{G_{a_i}} \uparrow^G, 1_G] = k.$$

QED

Corollary

If G acts on Ω which permutation character χ, then $[\chi, \chi] = r$ where r is the number of orbits of G_α on Ω.

Proof : We have

$$r = [\chi|_{G_\alpha}, 1_{G_\alpha}] = [\chi, 1_{G_\alpha} \uparrow^G] = [\chi, \chi]$$

QED

Definition

If G acts transitively on Ω and $\alpha \in \Omega$, then the number of G_α-orbits on Ω is called the permutation rank of the G action on Ω.

If the permutation rank of G on Ω is two, then G_α acts transitively on $\Omega \setminus \{\alpha\}$; i.e. G acts 2-transitively on Ω.

Corollary

If G acts transitively on Ω with permutation character χ, then G acts 2-transitively if and only if $\chi = 1_G + \psi$ with $\psi \in \mathrm{Irr}(G)$.

Example 1: The permutation character of S_n in its action on $\{1,\ldots,n\}$ is $1_{S_n}+\chi$ where $\chi\in \mathrm{Irr}(S_n)$ is of degree $n-1$.The module affording χ is called the *reduced permutation module*.
Example 2: S_n acting on Ω_k,the set of unordered k-elements subsets of $\{1,\ldots,n\}$ with $k<[n/2]$ is a permutation action of rank k.
Example 3: $\mathrm{GL}_n(\mathbb{F}_q)$ acting on the 1-spaces of $\mathbb{F}_q^n$ is an example of a 2-transitive permutation action. This shows that $\mathrm{GL}_n(\mathbb{F}_q)$ has an irreducible character of degree $\frac{q^n-1}{q-1}-1=q\frac{q^{n-1}-1}{q-1}$.
Example 4: Assume n is even. The restriction of the action above to $Sp_n(q)$ is an example of a rank 3-action.The stabilizer of a 1-space is transitive on the set of 1-spaces of perpendicular but not equal to it,and transitive on the set of 1-spaces not perpendicular to it.
Example 5: The dihedral group D_{2n} acting on the vertices of a regular n-gon is of rank $(n+1)/2$ if n is odd,and rank $(n+2)/2$ if n is even.

1. Show that the set of distinct character degrees of the dihedral group D_{2n} is $\{1, 2\}$.
   Hint: Depending on whether n is even or odd, D_{2n} has either 4 or repsectively 2 distinct linear characters. Now show that all nonlinear characters are obtained via induction from a nontrivial linear character of $\mathbb{Z}/\mathbb{Z}_n \subset D_{2n}$.
2. Prove that S_n acting on Ω_k, the set of unordered k-elements subsets of $\{1, \ldots, n\}$ with $k < [n/2]$ is a permutation action of rank k.
3. Using the notation and hypotheses of the problem 8 in section 7 show that $|G| = q(q-1)(q+1)$.

Note that it is now easy to show that the group in problem 3 is isomorphic to $\mathrm{SL}_2(q)$. This was first proved by Brauer, Suzuki and Wall.

Clifford's theorem and consequences

If H is a subgroup of G, then generally very little can be said about the induction and restriction maps. However the situation improves dramatically when H is normal in G.
If $H \lhd G$ and ϕ is a class function of H, then for $g \in G$ define

$$\phi^g(h) := \phi(ghg^{-1}).$$

We call ϕ^g a conjugate of ϕ.

Lemma

If $H \lhd G$ and ϕ, ψ are class functions of H and $x, y \in G$, then

1. ϕ^x *is a class function of* H.
2. $(\phi^x)^y = \phi^{xy}$.
3. $[\phi^x, \psi^x] = [\phi, \psi]$.
4. $[\chi_H, \psi^x] = [\chi_H, \psi]$ *for class functions* χ *of* G.
5. ϕ^x *is a character iff* ϕ *is a character.*

Proof : Let $g, h, t \in H$ with $g^t = h$.Then

$$\phi^x(h) = \phi^x(g^t) = \phi(xt^{-1}gtx^{-1}) = \phi((xt^{-1}x^{-1})xhx^{-1}(xtx^{-1})) = \phi(xhx^{-1}) = \phi$$

as $(xtx^{-1})^{-}1 = xt^{-1}x^{-1} \in H$ due to our hypothesis that $H \lhd G$.
For part 2 note that

$$(\phi^x)^y(h) = \phi^x(yhy^{-1}) = \phi(x(yhy^{-1})x^{-1}) = \phi((xy)h(xy)^{-1}) = \phi^{xy}(h).$$

For part 3 note that the sums are identical as conjugation by x simply just permutes the summands.
For part 4 observe that $\chi_H^x = \chi$ and then apply part 3.
For part 5 let Φ be a representation affording ϕ and let $\alpha \in \mathrm{Aut}(H)$, then $\alpha \circ \Phi$ is a representation affording the character $\psi(h\alpha)$.Now observe that as $H \lhd G$ conjugation by x^{-1} induces an automorphism on H. **QED**

We if Φ is a representation of H and $\alpha \in \mathrm{Aut}(H)$ then we say that $\alpha \circ \Phi$ and Φ are *quasi-equivalent*. The terminology $\alpha \circ \Phi$ is the *twist of* Φ *by* α is also in use. When H is a normal subgroup of G and α is conjugation on N by an element of G, then we call $\alpha \circ \Phi$ a *conjugate of* Φ.

Theorem

(Clifford) If $H \lhd G$ and $\chi \in \mathrm{Irr}(G)$,ψ a constituent of χ_H and $\psi = \psi_1, \ldots, \psi_t$ the distinct G-conjugates of ψ, then

$$\chi_H = e \sum_{i=1}^{t} \psi_i$$

where $e = [\chi_H, \psi]$.

Proof : We compute $(\psi \uparrow^G)_H$. For $h \in H$ we have

$$(\psi \uparrow^G)_H(h) = \frac{1}{|H|} \sum_{x \in G} \psi^0(xhx^{-1}) = \frac{1}{|H|} \sum_{x \in G} \psi^x(h).$$

Thus

$$|H|(\psi \uparrow^G)_H = \sum_{x \in G} \psi^x.$$

Now if $\phi \in \mathrm{Irr}(H) \setminus \{\psi = \psi_1, \ldots, \psi_t\}$, then

$$[|H|(\psi \uparrow^G)_H, \phi] = |H|[(\psi \uparrow^G)_H, \phi] = [\sum_{x \in G} \psi^x, \phi] = 0.$$

By Frobenius Reciprocity we have χ is a constituent of $\psi \uparrow^G$ and thus $[\chi_H, \phi] = 0$.

Also we have that $[\chi_H, \psi_i] \neq 0$ and moreover that

$$\chi_H = \sum_{i=1}^{t} [\chi_H, \psi_i]\psi_i.$$

But now by part 4 of the previous lemma we have $[\chi_H, \psi_i] = [\chi_H, \psi]$ and the theorem follows. **QED**

We would now like have a module theoretic interpretation of Clifford's Theorem.

Lemma

Let V be an $\mathbb{F}[G]$-module and let $H \lhd G$. Suppose that W is an $\mathbb{F}[H]$-submodule of V. The following are true:

1. *For all $g \in G$, Wg is an $\mathbb{F}[H]$-module conjugate to W.*
2. *If M is a $\mathbb{F}[H]$ module conjugate to W, then $M \cong Wg$ for some $g \in G$.*
3. *If $U \subset V$ is an $\mathbb{F}[H]$-submodule isomorphic to W, $Ug \cong Wg$ as $\mathbb{F}[H]$-modules.*

Proof : Note that $(Wg)h = (W(ghg^{-1}))g = Wg$ as $ghg^{-1} \in H$. Moreover we see that the H action is the action on the conjugate, proving part 1.The other two are consequences of the first. **QED**

Theorem

(Clifford) Let V be an irreducible $\mathbb{F}[G]$-module and let $H \lhd G$. Suppose that W is an irreducible $\mathbb{F}[H]$-submodule of V. The following are true:

1. $V = \oplus I_V(Wg)$ *where Wg ranges over the W conjugates of G.*
2. *We have* $\dim(I_V(W)) = \dim(I_V(Wg))$.

Proof : This we already saw that all G conjugates of W lie in V.Also the isotypic components are permuted transitively by G.Thus both parts follow. **QED**

Corollary

If V be an irreducible $\mathbb{F}[G]$-module and let $H \lhd G$, then V is completely reducible as $\mathbb{F}[H]$-module.

Remark: Clifford's Theorem is independent of Maschke's Theroem and needs no assumptions on $\mathbb{F}$, thus making it usefull in both ordinary and modular representation theory.

We now derive some consequences of Clifford's Theorem.

Lemma

If $\chi \in \mathrm{Irr}(G)$*,* $H \lhd G$ *and* $[\chi_H, 1_H] \neq 0$*, then* $H \subset \mathrm{Ker}(\chi)$*.*

Proof : The conjugates of 1_H are all equal to 1_H and thus $\chi_H = e1_H = \chi(1)1_H$. So H acts trivially and the claim follows. **QED**

Lemma

If $\chi \in \mathrm{Irr}(G)$*,* $H \lhd G$*,* $\psi \in \mathrm{Irr}(H)$ *and* $[\chi_H.\psi] \neq 0$*, then* $\psi(1)$ *is a divisor of* $\chi(1)$

Proof : As $\psi(1) = \psi^g(1)$ Clifford's Theorem implies $\chi(1) = et\psi(1)$ where t is the number of G conjugates of ψ.This is our claim.

Theorem

If p is a prime and $\chi(1) = p^{a(\chi)}$ *for all* $\chi \in \mathrm{Irr}(G)$*, then G has a normal abelian p-complement.*

Proof : Let $N \lhd G$.By the previous lemma every irreducible character is of p-power degree.Thus by induction N has an abelian p-complement. So it suffices to find a normal subgroup of G of index p.
Now

$$|G| = [G : G'] + \sum_{\chi \in \mathrm{Irr}(G) \,:\, \chi(1) > 1} \chi(1)^2.$$

If G is abelian then clearly G has a normal subgroup of index p.So without loss we assume that G is not abelian.But then the formula above implies that p divides $[G : G']$. But now the subgroup correspondence theorem implies the existence of a normal subgroup of index p.Our proof is complete. **QED**

Definition

If $H \lhd G$, ψ is a character of H, then $I_G(\psi) := \{g \in G \ : \ \psi^g = \psi\}$.

The number of conjugates of ψ is $[G : I_G(\psi)]$. It is worth noting that the integer t that appears in Clifford's Theorem is the index of an inertial group.

Theorem

Suppose $H \lhd G$, $\theta \in \mathrm{Irr}(H)$, and $T = I_G(\theta)$.Define $\mathcal{A} = \{\psi \in \mathrm{Irr}(T) \ : \ [\psi_H, \theta] \neq 0\}$, $\mathcal{B} = \{\chi \in \mathrm{Irr}(G) \ : \ [\chi_H, \theta] \neq 0\}$.The following are true:

1. *If $\psi \in \mathcal{A}$, then $\psi \uparrow^G \in \mathrm{Irr}(G)$.*
2. *The map $\psi \longrightarrow \psi \uparrow^G$ is a bijection of $\mathcal{A}$ onto $\mathcal{B}$.*
3. *If $\psi \uparrow^G = \chi$, with $\psi \in \mathcal{A}$, then ψ is the unique irreducible constituent of χ_T which lies in $\mathcal{A}$.*
4. *If $\psi \uparrow^G = \chi$, with $\psi \in \mathcal{A}$, then $[\psi_H, \theta] = [\chi_H, \theta]$.*

Proof : Let $\psi \in \mathcal{A}$ and let χ be some irreducible constituent of $\psi \uparrow^G$. Then ψ is an irreducible constituent of χ_T. As θ is a constituent of ψ_H we see that $\chi \in \mathcal{B}$.
Let $\theta = \theta_1, \ldots, \theta_t$ be the distinct G conjugates of θ. Then $t = [G : T]$ and $\chi_H = e \sum_{i=1}^{t} \theta_i$ for some $e \in \mathbb{N}$.Since θ is T-invariant we see, by Clifford's Theorem that $\psi_H = f\theta$.Since ψ is a constituent of χ_T, we have $f \leq e$.So

$$et\theta(1) = \chi(1) \leq \psi \uparrow^G (1) = t\psi(1) = ft\theta(1) \leq et\theta(1),$$

and thus we have equality throughout. Hence $\chi(1) = \psi \uparrow^G (1)$and thus $\chi = \psi \uparrow^G$, which implies part 1.
Now $[\chi_H(1), \theta] = e = f = [\psi_H, \theta]$ proving part 4.

To prove part 3 observe that if $\psi_1 \in \mathcal{A}$ with $\psi_1 \neq \psi$, and ψ_1 is a constituent of χ_T, then
$[\chi_H, \theta] \geq [(\psi + \psi_1)_H, \theta] = [\psi_H, \theta] + [(\psi_1)_H, \theta] > [\psi_H, \theta]$;a contradition to the last formula in the proof of part 1.
To prove part 2 note that the map is well defined, by part 1,and its image lies in $\mathcal{B}$, by part 4.It is one to one by part 3. So we have to prove that the map is onto.To this end let $\chi \in \mathcal{B}$. Since θ is a constituent of χ_H, there exists an irreducible constituent ψ of χ_T such that $[\psi_H, \theta] \neq 0$.But now $\psi \in \mathcal{A}$ and so χ is a constituent of $\psi \uparrow^G$.So $\chi = \psi \uparrow^G$, completing the proof. **QED**

Corollary

Let $\chi \in \mathrm{Irr}(G)$ be primitive and $N \lhd G$, then χ_N is a multiple of an irreducible character of N.

Proof : By Clifford's theorem $\chi_N = e \sum_{i=1}^{t} \psi_i$ where the ψ_i are the distinct conjugates. Since χ is primitive $t = 1$, hence the claim. **QED**

Remark: This is analogous to the theorem that the orbits of a normal subgroup N of a transitive permutation group G form a system of imprimitivity. This implies that if the action of G is primitive, then N is transitive.

Theorem

(Ito) If A is an abelian normal subgroup of G,then $\chi(1)$ *is a divisor of* $[G : A]$ *for all* $\chi \in \mathrm{Irr}(G)$.

Proof : Without loss we may assume that $A \neq \mathrm{Ker}(\chi)$. So let $\lambda \in \mathrm{Irr}(A)$ with $[\chi_A, \lambda] \neq 0$.Then $A \subset I_G(\lambda) =: T$.So for some $\psi \in \mathrm{Irr}(T)$we have $\chi = \psi \uparrow^G$ and that $\psi_A = e\lambda$.Thus $A \subset Z(\psi)$, so $\psi(1)$ is a divisor of $[T : A]$.(by a strengthening of our result that $\chi(1)$ is a divisor of the group order.) Since $\chi(1) = [G : T]\psi(1)$ we have our desired conclusion. **QED**

ExampleLet $G \subset \mathrm{GL}_3(\mathbb{F}_q)$be the stabilizer of the 1-space of $\mathbb{F}_q^3$ spanned by $[1, 0, 0]$. Then G' contains an abelian normal subgroup $A \cong \mathbb{F}_q^2$ on such that $G'/A \cong \mathrm{SL}_2(q)$acts transitively on $A \setminus 1$.If $\chi \in \mathrm{Irr}(G')$ and $A \not\subset \mathrm{Ker}(\chi)$, then $[G' : I_{G'}(\lambda)] = q^2 - 1$. Now $I_{G'}(\lambda)/A \cong \mathbb{F}_q$ is abelian the group, so G' has exactly q characters of degree $q^2 - 1$ which do not have A in the kernel.

Theorem

(Brauer) Let A be a group which acts on $\mathrm{Irr}(G)$ *and on the set of conjugacy classes of G.Assume that* $\chi(g) = \chi^a(g^a)$ *for all* $\chi \in \mathrm{Irr}(G)$, $g \in G$, $a \in A$ *and that* $g^a \in (g^G)^a$. *Then for each* $a \in A$, *the number of fixed irreducible characters of G is equal to the number of fixed classes.*

Proof : Let χ_i and C_i denote the irreducible characters respectively the conjugacy classes of G.For $a \in A$ we label things so that $g_i^a = g_j$ if $C_i^a = C_j^a$.Now let $X = (\chi_i(g_j))$ be the character table matrix. Let $P(a) := (\delta_{\chi_r^a, \chi_s})$ and $Q(a) := (\delta_{C_r^a, C_s})$.Our hypotheses imply that $P(a)X = XQ(a)$. The orthogonality relations imply that X is invertible and thus $Q(a) = X^{-1}P(a)X$,so $\mathrm{Tr}(P(a)) = \mathrm{Tr}(Q(a))$. That is the number of fixed points of a on both characters and conjugacy classes are equal. **QED**

Corollary

Under the hypotheses of the previous theorem the number of orbits in the actions of A on $\mathrm{Irr}(G)$ and on the G conjugacy classes $C_1, \ldots, C_k$ is the same.

Proof : The proof of the theorem above shows that the permutation characters of A on $\mathrm{Irr}(G)$ and on $\{C_1, \ldots C_k\}$ are equal. Thus the number of orbits must coincide. **QED**

Theorem

If $N \lhd G$ and assume that $C_G(x) \subset N$ for all $1 \neq x \in N$, then

1. *For $1_N \neq \psi \in \mathrm{Irr}(N)$ we have $I_G(\psi) = N$ and $\psi \uparrow^G \in \mathrm{Irr}(G)$.*
2. *For $\chi \in \mathrm{Irr}(G)$ with $N \not\subset \mathrm{Ker}(\chi)$ we have $\chi = \psi \uparrow^G$ for some $\psi \in \mathrm{Irr}(N)$.*

Proof : Let $1_N \neq \psi \in \mathrm{Irr}(N)$. To show that $\psi \uparrow^G \in \mathrm{Irr}(G)$ it suffices to show that $I_G(\psi) = N$. So by the theorem above it suffices to show no element $g \in G \setminus N$ fixes a conjugacy class of N.Let $g \in G \setminus N$ and suppose that $C_i^g = C_i$ and $x \in C_i$.Then $x^g = x^n$ for some $n \in N$ and thus $gn^{-1} \in C_G(x) \setminus N = \emptyset$;which proves part 1.
To prove part 2 let $\chi \in \mathrm{Irr}(G)$ with $N \not\subset \mathrm{Ker}(\chi)$and pick an irreducible constituent $1_N \neq \psi$ of χ_H.Then χ is a constituent of $\psi \uparrow^G \in \mathrm{Irr}(G)$. Thus $\chi = \psi \uparrow^G \in \mathrm{Irr}(G)$ and the proof is complete.

QED

Frobenius' theorem and related results

While it is true that very little can be said about restriction of characters to subgroups in general there are special situations where the situation is much better.One such was the condition that $H \lhd G$. Here we consider a different extremal situation which already came up in the last theorem of the previous section. Namely the situation where $N \lhd G$ and assume that $C_G(x) \subset N$ for all $1 \neq x \in N$.

Lemma

If $N \lhd G$ and assume that $C_G(x) \subset N$ for all $1 \neq x \in N$, then the following are true:

1. *N has a complement H in G.*
2. *If H is a complement to N in G and $g \in G \setminus H$, then $H \cap H^g = 1$.*

Proof : If p is a prime dividing $([G : N], |G|)$ and $P \in \mathrm{Syl}_p(G)$, then $Z(P) \cap N \neq 1$ as P is nilpotent.So if $x \in Z(P) \cap N$,then $P \subset C_G(x)$ but $P \not\subset N$;contradicting our hypothesis. So $([G : N], |G|) = 1$ and now the Schur-Zassenhaus theorem gives the existence of H such that $NH = G$ and $N \cap H = 1$; proving part 1.
To prove part 2 let $g \in G \setminus H$ and write $g = xn$ where $x \in H$ and $n \in N$. If $y \in H \cap H^g$, then there exists $h \in H$ such that $y = h^n$ for some $h \in H$. Thus $h^{-1}y \in H$ and $h^{-1}y = h^{-1}h^n = [h, n] \in N$.So $[h, n] = 1$, that is $h \in C_G(N)$ forcing $h \in N \cap H = 1$.So $h = y = 1$ and part 2 follows. **QED**

Definition

If H is a subgroup of G and for all $g \in G \setminus H$ we have $H \cap H^g = 1$, then we call H a Frobenius complement and G a Frobenius group.

Theorem

(Frobenius) Let G be a Frobenius group with complement H, then H has a normal complement in G. That is G has a normal subgroup N such that $G = HN$ and $H \cap N = 1$.

We need two preperatory lemmas.

Lemma

If H is a Frobenius complement in G then

$$N := (G \setminus \cup_{x \in G} H^x) \cup \{1\}$$

has order $[G : H]$ and if $M \lhd G$ with $M \cap H = 1$, then $M \subset N$.

Proof : Since$N_G(H) = H$ the number of distinct conjugates of H is $[G : H]$.The number of nonidentity elements in $\cup_{x \in G} H^x$ is

$$[G : H](|H| - 1) = |G| - [G : H]$$

, so the claim about the order of N follows. Now let $M \lhd G$ with $M \cap H = 1$, then $M \cap H^x = (M \cap H)^x = 1^x = 1$. Thus $M \subset N$, by definition of N. **QED**

Note that N may not be a subgroup of G. This is in fact the crux of the matter.

Lemma

If H is a Frobenius complement in G and θ a class function of H such that $\theta(1) = 0$, then $(\theta \uparrow^G)_H = \theta$.

Proof : Let $1 \neq h \in H$.Then

$$\theta \uparrow^G (h) = \frac{1}{|h|} \sum_{xinG} \theta^o(xhx^{-1}).$$

Now $0 \neq \theta^o(xhx^{-1})$ implies that $1 \neq xhx^{-1} \in H \cap H^{x^{-1}}$; i.e., $x \in H$. So

$$\theta \uparrow^G (h) = \frac{1}{|h|} \sum_{xinH} \theta(xhx^{-1}) = \theta(h).$$

Finally observe that $\theta \uparrow^G (1) = [G : H]\theta(1) = 0$ and the proof is complete. **QED**

Proof : (of Frobenius' theorem)Let $1_H \neq \psi \in Irr(H)$ and set $\theta = \psi - \psi(1)1_H$. Note that $\theta(1) = 0$ so the previous lemma yields

$$[\theta \uparrow^G, \theta \uparrow^G] = [\theta, (\theta \uparrow^G)_H] = [\theta, \theta] = 1 + \psi(1)^2.$$

Also $[\theta \uparrow^G, 1_G] = [\theta, 1_H] = -\psi(1)$ and thus $\theta \uparrow^G = \psi^* - \psi(1)1_G$,where ψ^* is a class function of G such that $[\psi^*, 1_G] = 0$and

$$1 + \psi(1)^2 = [\theta, \theta] = [\psi^*, \psi^*] + \psi(1)^2.$$

So $[\psi^*, \psi^*] = 1$. As θ is a difference of characters,so is $\theta \uparrow^G$ and thus also ψ^* and hence $\pm\psi^* \in \mathrm{Irr}(G)$.Moreover if $h \in H$, then

$$\psi^*(h) = \theta \uparrow^G (h) + \psi(1) = \theta(h) + \psi(1) = \psi(h),$$

and in particular $\psi^*(1) = \psi(1) \geq 1$;showing that $\psi^* \in \mathrm{Irr}(G)$.
So for all $1_H \neq \psi \in \mathrm{Irr}(H)$ we can find an extension $\psi^* \in \mathrm{Irr}(G)$.Define $M := \cap_\psi \mathrm{Ker}(\psi^*)$. If $x \in M \cap H$, then $\psi(x) = \psi^*(x) = \psi^*(1) = \psi(1)$, for all $\psi \in \mathrm{Irr}(H)$ and hence $x = 1$. So by the previous lemma $M \subset N$. Conversely, if $g \notin \cup_{x \in G} H^x$,then

$$\psi^*(g) - \psi(1) = \theta \uparrow^G, (g) = 0,$$

showing $g \in M$. Thus $M = N$ and $M \cap H = 1$. As $|M| = |N| = [G : H]$ we also have $G = MH$. **QED**

The subgroup N whose existence was proved in the theorem above is called a *Frobenius kernel*.

Corollary

If G is a transitive permutation group on Ω with permutation character χ, and $\chi(g) \leq 1$ for all $g \in G$, then G_α is a Frobenius complement with Frobenius kernel equal to $\{g \in G \ : \ \chi(g) = 0\} \cup \{1\}$.

Proof : Notice that if $1 \neq g \in G_\alpha \cap G_\beta$ then $\chi(g) \geq 2$ which contradicts our hypothesis.Thus G_α is a Frobenius complement. The rest follows from Frobenius' theorem. **QED**

Definition

A subset $X \subset G$ is called a T.I. set (trivial intersection set) if for all $g \in G$ we have $X = X^g$ or $X \cap X^g \subset \{1\}$.

Lemma

If X is a T.I. set in G, ϕ, ψ class functions on $N := N_H(X)$ such that $\phi(n) = 0 = \psi(n)$ for all $n \in N \setminus X$ and $\psi(1) = 0$, then $\psi \uparrow^G (x) = \psi(x)$ for all $x \in X$ and $[\psi \uparrow^G, \phi \uparrow^G] = [\psi, \phi]$.

Proof : If $x \in X$, then $\psi \uparrow^G (x) = \frac{1}{|N|} \sum_{y \in G} \psi^o(yxy^{-1})$.Now if $\psi^o(yxy^{-1}) \neq 0$,then $1 \neq yxy^{-1} \in X \cap X^{y^{-1}}$.So $y \in N$ and $\psi^o(yxy^{-1}) = \psi(x)$ which is our first claim.
To prove the second claim we see that $[\psi \uparrow^G, \phi \uparrow^G] = [(\psi \uparrow^G)_N, \phi]$. As ϕ vanishes on $N \setminus X$and $(\psi \uparrow^G)_N - \psi$ vanishes on X, we have $[(\psi \uparrow^G)_N - \psi, \phi] = 0$ which implies our second claim. **QED**

Recall that a group Q_{2n}, $n = 2^a$ with presentation

$$\langle x, y \ : \ x^n = y^2, \ y^{-1}xy = x^{-1} \rangle$$

is a *generalized quaternion* group of order $2n$. The following lemma is a collection of some standard facts about generalized quaternion groups.

Lemma

If $P \cong Q_{2n}$ then the following are true:

1. $\langle x \rangle$ *is a cyclic subgroup of* P *of index* 2.
2. $[P; P'] = 4$.
3. $|Z(P)| = 2$ *and and in fact* $Z(P) = \langle x^{n/2} \rangle = \langle y^2 \rangle$.
4. *Noncyclic subgroups of* P *are generalized quaternion.*
5. P *contains a unique involution; the central one.*

Theorem

(Brauer-Suzuki) If $P \in \mathrm{Syl}_2(G)$ is a generalized quaternion group of order ≥ 16, then there exists $N \lhd G$ with $|N|$ odd such that G/N has a normal subgroup of order 2.

Remark: The condition $|P| \geq 16$ can be dropped. However the case $P = Q_8$ requires tools from the theory of modular representation theory.

Remark: The normal subgroup of order will lie in $Z(G/N)$ whose pullback into G sometimes referred to as Z^*.

Remark: The condition that P contains a unique involution implies that G has a unique class of involutions t^G and that $t^G \cap P = \{t\}$.

Theorem

(Glauberman) If $P \in \mathrm{Syl}_2(G)$ and t is an involution in G such that $t^G \cap P = \{t\}$,then there exists $N \lhd G$ with $|N|$ odd such that G/N has a normal subgroup of order 2.

The proof of Glauberman's Z^*-theorem requires the strengthend version of the Brauer-Suzuki theorem.

To prove the Brauer-Suzuki theorem we will first prove

Theorem

If $P \in \mathrm{Syl}_2(G)$ is a generalized quaternion group of order ≥ 16, then there exists $M \lhd G$ with $|M|$ even and G/M nonabelian.

Proof : Let H be the unique cyclic subgroup of P of index 2.Clearly $P' \subset H$.As $P' > Z(P)$ we have $H \subset C_P(P') \neq P$; hence $H = C_P(P')$.Now let $N := N_G(P')$ and $C := C_G(P')$,then $P \in \mathrm{Syl}_2(N)$ and so $P \cap C = C_P(P') = H \in \mathrm{Syl}_2(C)$.So C has a normal 2-complement (see problem 2 in section 7)say K.Now N/C is isomorphic to a a subgroup of $\mathrm{Aut}(P')$,and hence a 2-group;as P' is cyclic of 2-power order.Thus we conclude that $N = PK$, and as $P' \lhd C$,that $P'K = P' \times K$.
Now let $U \subset P'$ be the unique subgroup of index 2 in P' and $X = C - UK$. We claim that X is a T.I. setand that $N_G(X) = N$. To see this we first observe that the elements of X all have order divisible by $|P'|$,and thus for all $x \in X$ we have $P' \subset \langle x \rangle$.So if $x \in X \cap X^g$, then P' and $(P')^g$ are contained in $\langle x \rangle$; forcing $P' = (P')^g$, i.e. $g \in N$.
So $C/UK \cong \mathbb{Z}/4\mathbb{Z}$.and $N/UK \cong D_8$.Let λ be a linear character with $\mathrm{Ker}(\lambda) = UK$ and let $\theta = \lambda \uparrow^N -(1_C) \uparrow^N$. As $\mathrm{Ker}(\lambda \uparrow^N) = UK$we see that $\theta(t) = 0$ for all $t \in UK$. Moreover θ vanishes on $N \setminus C$,and thus on $N \setminus X$. So we can apply Lemma 10.8 to conclude that

$$[\theta \uparrow^G, \theta \uparrow^G] = [\theta, \theta].$$

We need to compute $[\theta, \theta]$. To do this note that $1_C \uparrow^N = 1_N + \mu$ where $\mathrm{Ker}(\mu) = C$. We claim that $\lambda \uparrow^N \in \mathrm{Irr}(N)$. Else $\lambda \uparrow^N$ is a the sum of linear characters forcing $P'K \subset \mathrm{Ker}(\lambda \uparrow^N) = UK$,a contradiction. Thus

$$\theta = \lambda \uparrow^N -\mu - 1_N$$

and so $[\theta \uparrow^G, \theta \uparrow^G] = [\theta, \theta] = 3$.We have $[\theta \uparrow^G, 1_G] = [\theta, 1_N] = 1$ which shows that

$$\theta \uparrow^G = \pm\chi_1 \pm \chi_2 - 1_G$$

where $\chi_1, \chi_2 \in \mathrm{Irr}(G) \setminus \{1_G\}$.As $\theta \uparrow^G (1) = \theta(1) = 0$ we may conclude that

$$\theta \uparrow^G = \chi_1 - \chi_2 - 1_G.$$

Now $\theta \uparrow^G (g) = 0$ unless g is conjugate to an element of x so we see that

$$\chi_1(g) - \chi_2(g) = 1$$

if 4 does not divide the order of g.Now let C_1 denote the conjugacy class of involutions of G.Note that by Sylow's theorem all involutions are conjugate to involutions in P,and P has exactly one involution;hence G has a unique class of involutions.

Define the class function ϕ of G via

$$\phi(g) := |\{(x, y) \;\; x, y \in C_1, \;\; xy = g\}|.$$

If $\phi(g) \neq 0$, then $g = xy$ and thus $g^x = x(xy)x = yx = g^{-1}$.If g has even order then $\langle x, y\langle$contains an elementary abelian subgroup of rank 2, which by Sylow's theorem must be isomorphic to a subgroup of P;a contradiction.We conclude that $\phi(g) = 0$ whenever g has even order. Thus for all $g \in G$ we have $\phi(g)(\chi_1(g) - \chi_2(g) - 1) = 0$ and thus

$$[\phi, \chi_1 - \chi_2 - 1_G] = 0.$$

Recall that the class sums in $\mathbb{C}[G]$ form a basis for $Z(\mathbb{C}[G])$ and recall the setup and conclusion of problem 2 in section 5. We have

$$\phi(g) = a_{1,1,\nu} = (|C_1|^2/|G|) \sum_{\chi \in \mathrm{Irr}(G)} \chi(x)^2 \chi(g)/\chi(1).$$

As $\chi(x), \phi(g) \in \mathbb{R}$ we have

$$(|G|/|C_1|^2)\phi = \sum_{\chi \in \mathrm{Irr}(G)} (\chi(x)^2/\chi(1))\chi$$

and thus

$$(|G|/|C_1|^2)[\phi, \chi] = (\chi(x)^2/\chi(1))$$

for all $\chi \in \mathrm{Irr}(G)$.Combining this with $[\phi, \chi_1 - \chi_2 - 1_G] = 0$ yields

$$(\chi_1(x)^2/\chi_1(1)) - (\chi_2(x)^2/\chi_2(1)) = 1.$$

As $\chi_2(x) = \chi_1(x) - 1$ (as $|x|$ is not divisible by 4) and $\chi_2(1) = \chi_1(1) - 1$ we get

$$(\chi_1(x)^2/\chi_1(1)) - (\chi_1(x) - 1)^2/(\chi_1(1) - 1) = 1.$$

which simplifies to

$$(\chi_1(x) - \chi_1(1))^2 = 0.$$

We conclude that $x \in Ker(\chi_1)$ and that $\chi_1(1) = 1 + \chi_2(1) \geq 2$. Thus $G/\mathrm{Ker}(\chi_1)$ is nonabelian and hence our desired subgroup M is $\mathrm{Ker}(\chi_1)$. **QED**

Proof : (of the Brauer-Suzuki theorem) We already established that G has a unique class of involutions. So let U be the subgroup generated by all the involutions in G. If U has a cyclic Sylow 2-subgroup, then U has a normal 2-complement N.As N is characteristic in U and U is normal in G we have $N \lhd G$.So U/N is a cyclic normal 2 subgroup of G/N and the result follows.
If the Sylow 2-subgroups are not cyclic,then as P is generalized quaternion we have that 8 is a divisor of $|U|$and thus there exist a subgroup $U \subset V \subset PU$such that $[V : U] \leq 2$ and 16 divides $|V|$. So we can apply our theorem to produce $M \lhd V$ of even order such that V/M is nonabelian.V also contains a unique class of involutions and hence $U \subset M$. But now $[V : M] \leq [V : U] \leq 2$ contradicting that V/M is non-abelian.Our proof is now complete. **QED**

We already mentioned that the Brauer-Fowler theorem is part of the philosophical basis of the classification of the finite simple groups.At the end of chapter 5 we saw how to classify simple groups G with the smallest possible involution centralizer.All examples lead to A_5.The next smallest situation is when the involution centralizer C has order 8. The case $C \in Syl_2(G)$ is elementary abelian of order 8 leads to the group $\mathrm{PSL}_2(8)$.The case where C abelian but not elementary abelian leads to a contradiction (to simplicity)as does the case where $C \cong Q_8$ (by the stronger form of the Brauer-Suzuki theorem). This leaves the case $C \cong D_8$.

Theorem

If $G = G'$ and $\tau \in G$ is an involution with centralizer $C_G(\tau) \cong D_8$,then $|G| = 168$ or 360.

Proof : We know that $D \subset S \in \mathrm{Syl}_2(G)$. But now $Z(S) \subset Z(D) = \langle \tau \rangle$ and thus $S \subset C_G(\tau) = D$;i.e $D \in \mathrm{Syl}_2(G)$.Let $M \subset D$ be unique cyclic subgroup of order 4 and hence τ is the unique involution in M.Since $G = G'$,problem 1 in section 7 guarantees that all involutions in D are conjugate to τ; showing that G has a single conjugacy class of involutions.
Now observe that M is a T.I. set,as $1 \neq M \cap M^x$ implies $\tau \in M^x$;i.e $\tau^x = \tau$ which means $x \in D \subset N_G(M)$. In fact $D = N_G(M)$, again because τ is the unique involution in M.
Let λ be a faithful linear character of M and let $\theta = (1_M - \lambda) \uparrow^D$. As $\lambda \uparrow^D$ is irreducible$[\theta, \theta] = 3$.Also $\theta(1) = 0$ and θ vanishes on $D \setminus M$,hence Lemma 10.8 yields $(\theta \uparrow^G)_M = \theta$.As in the proof of the Brauer-Suzuki theorem this means there exist $\chi, \psi \in \mathrm{Irr}(G)$ such that $\theta \uparrow^G = 1_G + \chi - \psi$.A calculation involving only D yields

$$0 = 1 + \chi(1) - \psi(1)$$

and

$$4 = 1 + \chi(\tau) - \psi(\tau).$$

Now we argue as in the proof of the Brauer-Suzuki theorem using class sums.

Again we let $C = \tau^G$and let

$$\phi(g) = |\{(x, y) \ : \ x, y \in C, \ xy = g\}|.$$

If $g = xy$ for involutions x, y, then $g^x = g^{-1}$ and conversely if $x \neq g$ and $g^x = g^{-1}$, then $y = xg$ is and involution. So
$\phi(g) = |\{x \in C \ : \ x \neq g, \ g^x = g^{-1}\}|$.
If $1 \neq g \in M$ and $g^x = g^{-1}$, then $\tau^x = \tau$, hence $x \in D$.Thus x is an involution in $D \setminus \{\tau\}$ and thus $\phi(g) = 4$.As in the proof of Brauer-Suzuki we see that

$$\phi = \frac{|C|^2}{|G|} \sum_{\xi \in \mathrm{Irr}(G)} \frac{\xi(\tau)^2}{\xi(1)} \xi.$$

As $|C| = |G|/8$ we get

$$[\theta \uparrow^G, \phi] = \frac{|G|}{64}(1 + \frac{\chi(\tau)^2}{\chi(1)} - \frac{\psi(\tau)^2}{\psi(1)}).$$

We also know

$$[\theta \uparrow^G, \phi] = [(1_M - \lambda), \phi_M] = \frac{4}{4}((1 + i) + 2 + (1 - i)) = 4$$

Equating the two expressions for $[\theta\uparrow^G,\phi]$ yields

$$256 = 2^8 = |G|(1+\frac{\chi(\tau)^2}{\chi(1)}-\frac{\psi(\tau)^2}{\psi(1)}).$$

Now set $a=\chi(1)$ and $b=\chi(\tau)$ which implies that $\psi(1)=a+1$ and $\psi(\tau)=b-3$ and use the second orthogonality relation to conclude that

$$8=|C_G(\tau)|\geq 1+b^2+(b-3)^2=2(b^2-3b+5).$$

As $b\in\mathbb{Z}$we see that $b=1$ or 2.
So $b=1$ implies that

$$2^8=|G|(1+1/a-4/(a+1))$$

which yields

$$|G|=2^8a(a+1)/(a-1)^2$$

Now 2 divides $a(a+1)$ which forces that 8 is a divisor of $(a-1)$. The later shows that $a(a+1)$ is congruent to 2 modulo 4.In turn, as $|P|=8$, this shows that 16 is not a divisor of $(a-1)$. Now no odd prime divisor of $a-1$ can divide $2^8a(a+1)$and thus $8=a-1$and

$$|G|=2^8\times 9\times 10/2^6=360.$$

Now $b = 2$ implies that

$$2^8 = |G|(1 + 4/a - 1/(a+1))$$

which yields

$$|G| = 2^8 a(a+1)/(a+2)^2$$

Again no odd prime divisor of $a+2$ can divide $2^8 a(a+1)$ and thus as above $a+2 = 8$ and

$$|G| = 2^8 \times 6 \times 7/2^6 = 168.$$

QED

We mention without proof that

Theorem

If $G = G'$ and $\tau \in G$ is an involution with centralizer $D := C_G(\tau) \cong D_8$ and $|G| = 168$, then $G \cong \mathrm{PSL}_3(2) \cong \mathrm{PSL}_2(7)$.

Theorem

If $G = G'$ *and* $\tau \in G$ *is an involution with centralizer* $C_G(\tau) \cong D_8$ *and* $|G| = 360$*, then* $G \cong A_6 \cong \mathrm{PSL}_2(9) \cong \mathrm{PSp}_4(2)$.

The hypothesis that $D := C_G(\tau) \cong D_8$ can not be weakend to $\mathrm{Syl}_2(G) = D_8$ as,for example the Sylow 2-subgroup of A_7 is D_8.A similar observation can be made for the case where $C_G(\tau)$ is elementary abelian of order 4 and 8 respectively.Here there exist infinitely many examples. The Sylow 2-subgroups of $\mathrm{PSL}_2(q)$ are elementary abelian of order 4 if $q \pm 1 \equiv 4 \bmod 8$.The Sylow 2-subgroups of the Ree groups ${}^2G_2(q)$, $q = 3^{1+2m}$, and of the sporadic group J_1 are elementary abelian of order 8.