1.3 The group algebra of a group

Let X be a finite set, and let

$$\mathbb{F}X = \{\text{functions from } X \text{ to } \mathbb{F}\}.$$

Lemma 1.5 *$\mathbb{F}X$ is a vector space. For $x \in X$, let $\delta_x : X \to \mathbb{F}$ be the function defined as*

$$\delta_x(y) = \begin{cases} 1 & \text{if } y = x \\ 0 & \text{if } y \neq x \end{cases}$$

Then the set $\{\delta_x\}_{x\in X}$ is a basis of $\mathbb{F}X$, and therefore $\mathbb{F}X$ has dimension $|X|$.

Proof: It is tedious but straightforward to check that $\mathbb{F}X$ is a vector space under the usual addition of functions and product of functions by scalars:

$$\begin{aligned} (f+g)(x) &:= f(x) + g(x) \\ (\lambda f)(x) &:= \lambda f(x). \end{aligned}$$

To see that $\{\delta_x\}_{x\in X}$ is a basis, we prove

1. Linear independence: Suppose that $\sum_{x\in X} a_x \delta_x = 0$, where $a_x \in \mathbb{F}$. Let y be any element of X. Then
$$0 = \sum_{x\in X} a_x \delta_x(y) = a_y \quad \text{since all other summands are 0.}$$
Therefore $a_y = 0$ for all $y \in X$, so the set $\{\delta_x\}_{x\in X}$ is linearly independent.

2. Generates $\mathbb{F}X$: let $f \in \mathbb{F}X$. Note that, for all $y \in X$,
$$\left(\sum_{x\in X} f(x)\delta_x\right)(y) = \sum_{x\in X} f(x)\delta_x(y) = f(y) \quad \text{(all other summands are 0).}$$
Thus
$$f = \sum_{x\in X} f(x)\delta_x,$$
and therefore $\{\delta_x\}_{x\in X}$ generates X.

∎

Now let G be a group acting on X. Define an action of G on $\mathbb{F}X$ by

$$(g \cdot f)(x) = f(g^{-1} \cdot x).$$

Lemma 1.6 *This action gives a representation of G in $\mathbb{F}X$.*

Proof:

1. It is an action:

   (a) $(hg) \cdot f = h \cdot (g \cdot f)$ since

$$\begin{aligned} ((hg)\cdot f)(x) &= f((hg)^{-1} \cdot x) \quad \text{by definition} \\ &= f((g^{-1}h^{-1}) \cdot x) \quad \text{by properties of a group} \\ &= f(g^{-1} \cdot (h^{-1} \cdot x)) \quad \text{by properties of action} \\ &= (g \cdot f)(h^{-1} \cdot x) \quad \text{by definition} \\ &= h \cdot (g \cdot f) \quad \text{by definition} \end{aligned}$$

(b) $\mathbf{1} \cdot f = f$ since $(\mathbf{1} \cdot f)(x) = f(\mathbf{1}^{-1} \cdot x) = f(\mathbf{1}x) = f(x)$.

2. The action is linear.

(a) $g \cdot (f_1 + f_2) = g \cdot f_1 + g \cdot f_2$ since

$$\begin{aligned} (g \cdot (f_1 + f_2))(x) &= (f_1 + f_2)(g^{-1} \cdot x) \\ &= f_1(g^{-1} \cdot x) + f_2(g^{-1} \cdot x) \\ &= g \cdot f_1(x) + g \cdot f_2(x) \\ &= (g \cdot f_1 + g \cdot f_2)(x) \end{aligned}$$

(b) $g \cdot (\lambda f) = \lambda(g \cdot f)$ since

$$\begin{aligned} (g \cdot (\lambda f))(x) &= (\lambda f)(g^{-1}x) \\ &= \lambda f(g^{-1}x) \\ &= \lambda(g \cdot f)(x) \end{aligned}$$

Therefore, it is a representation.

∎

Now let $X = G$. G acts on G by $g \cdot h = gh$. Then $\mathbb{F}G$ is called the *group algebra* of G: $\mathbb{F}G$ is on the one hand a vector space and on the other hand a ring (see exercise sheet 2). An object that is both a vector space and a ring is called and *algebra*.

Definition 1.7 *The* regular representation *is the representation of G on $\mathbb{F}G$ given by*

$$\begin{aligned} G \times \mathbb{F}G &\longrightarrow \mathbb{F}G \\ (g, f) &\longrightarrow g \cdot f, \end{aligned}$$

where $g \cdot f$ is the function from G to $\mathbb{F}$ given by $(g \cdot f)(h) = f(g^{-1}h)$.

Theorem 1.8 *The regular representation is faithful. Therefore, every finite group has at least one faithful representation.*

Proof: We need to check that if some $g \in G$ acts as the identity in $\mathbb{F}G$, then $g = \mathbf{1}$.
If $g \cdot f = f$ for all $f \in \mathbb{F}G$, then $f(h) = (g \cdot f)(h)$ for all $f \in \mathbb{F}G$ and for all $h \in G$. In particular, taking $f = \delta_{\mathbf{1}}$ and $h = g$, we have

$$\delta_{\mathbf{1}}(g) = (g \cdot \delta_{\mathbf{1}})(g) = \delta_{\mathbf{1}}(g^{-1}g) = \delta_{\mathbf{1}}(\mathbf{1}) = 1.$$

Therefore $g = \mathbf{1}$ since $\delta_{\mathbf{1}}(g)$ is 1 only if $g = \mathbf{1}$.

Let $\mathbb{F}X = \{\text{functions from } X \text{ to } \mathbb{F}\}$

Lemma 1.5

$\mathbb{F}X$ is a vector space. For $x \in X$, let δ_x be defined as $\delta_x(y) = \begin{cases} 1 & \text{if } y = x \\ 0 & \text{if } y \neq x. \end{cases}$

Then $\{\delta_x\}_{x \in X}$ is a basis of $\mathbb{F}X$ and therefore $\mathbb{F}X$ has dimension $|X|$.

Proof: It is tedious but straightforward to check that $\mathbb{F}X$ is a vector space under the usual addition and multiplication of functions:

$$(f+g)(x) := f(x) + g(x)$$
$$(\lambda f)(x) := \lambda f(x).$$

To see that $\{\delta_x\}_{x \in X}$ is a basis,

1) Linear independence: Let $\sum_{x \in X} a_x \delta_x = 0$. Let $y \in X$ arbitrary. Then

$$0 = \sum_{x \in X} a_x \delta_x(y) = a_y \quad \text{(all other summands are 0)}.$$

Therefore $a_y = 0$ $\forall y \in X$, so the $\{\delta_x\}_{x \in X}$ are lin. indep.

2) Generate $\mathbb{F}X$: let $f \in \mathbb{F}X$. Note:

$$\left(\sum_{x \in X} f(x)\, \delta_x\right)(y) = \sum_{x \in X} f(x)\, \delta_x(y) = f(y) \quad \text{(since all other summands are 0)}$$

Thus

$$f = \sum_{x \in X} f(x)\, \delta_x,$$

proving that $\{\delta_x\}_{x \in X}$ generates $\mathbb{F}X$.

Let G be a group acting on X.
Define an action of G on $\mathbb{F}X$ by

$$(g \cdot f)(x) = f(g^{-1}x)$$

(i.e. it takes the function
$(x \to f(x))$ into $(x \to g \cdot f(x) = f(g^{-1} \cdot x))$)

Lemma 1.6
This action gives a representation of G on $\mathbb{F}X$.

Proof:
1) It is an action, i.e

a) $(hg)\cdot f = h\cdot(g\cdot f)$, since

$$\begin{aligned}((hg)\cdot f)(x) &= f((hg)^{-1}\cdot x) \quad \text{by def}\\ &= f((g^{-1}h^{-1})\cdot x)\\ &= f(g^{-1}\cdot(h^{-1}\cdot x))\\ &= (g\cdot f)(h^{-1}\cdot x)\\ &= (h\cdot(g\cdot f))(x).\end{aligned}$$

b) $1\cdot f = f$, since

$$(1\cdot f)(x) = f(1^{-1}\cdot x) = f(1\cdot x) = f_1(x).$$

2) It is linear:

a) $$\begin{aligned}(g\cdot(f_1+f_2))(x) &= (f_1+f_2)(g^{-1}\cdot x)\\ &= f_1(g^{-1}\cdot x) + f_2(g^{-1}\cdot x)\\ &= g\cdot f_1(x) + g\cdot f_2(x)\\ &= (g\cdot f_1 + g\cdot f_2)(x),\end{aligned}$$

b) $(g\cdot(\lambda f))(x) = (\lambda f)(g^{-1}\cdot x) = \lambda f(g^{-1}\cdot x) = (\lambda\, g\cdot f)(x)$

Thus it is a representation. ▨

L 3/3

Now let $X = G$. G acts on G by $g \cdot h = gh$.

Definition 1.7

The regular representation is the representation of G on $\mathbb{F}G$ given by

$$G \times \mathbb{F}G \to \mathbb{F}G$$
$$(g, f) \longrightarrow g \cdot f \text{ defined as } (g \cdot f)(h) = f(g^{-1}h).$$

Theorem 1.8

The regular representation is faithful. Therefore, every finite group has a faithful representation

Proof:

We need to check that if some $g \in G$ acts as the identity on $\mathbb{F}G$, then $g = 1$.

If $g \cdot f = f \ \forall f \in \mathbb{F}G \Rightarrow f(h) = g \cdot f(h) \quad \forall f \in \mathbb{F}G, h \in G$.

In particular, taking $f = \delta_1$, $h = g$, we have

$$\delta_1(g) = g \cdot \delta_1(g) = \delta_1(g^{-1}g) = \delta_1(1) = 1.$$

This implies $g = 1$, as derived

▨

Remark: $\mathbb{F}G$ is called the group algebra of G. It is both a vector space and a ring (Ex. sheet 2). A set that is both a vector space and a ring is called an algebra

3.4 The first projection formula and inner products of characters

To continue with our study of characters we define the following:

Definition 3.10 *The inner product $\langle\ ,\ \rangle$ in $\mathbb{C}G$ (i.e. functions from G to $\mathbb{C}$) is defined by*

$$\langle \phi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \phi(g)\overline{\psi(g)}.$$

FACTS:

1. It really is an inner product (exercise sheet 6).
2. $\langle \phi, \psi \rangle = \langle g \cdot \phi, g \cdot \psi \rangle$ for all $g \in G$ (check).

GOAL: Prove that if χ_1, χ_2 are irreducible characters then

$$\langle \chi_1, \chi_2 \rangle = \begin{cases} 1 & \text{if } \chi_1 = \chi_2 \\ 0 & \text{if } \chi_1 \neq \chi_2 \end{cases}$$

This will have several implications, the most important of all being that the character determines the representation. First we need some tools:

Definition 3.11 *For V a G-module, V^G is the submodule of V given by*

$$V^G = \{v \in V : g \cdot v = v \quad \forall g \in G\}.$$

Remark: V^G really is a submodule: If $v_1, v_2 \in V^G$ and $a \in \mathbb{C}$ then for all $g \in G$, $g \cdot (av_1 + v_2) = a\, g \cdot v_1 + g \cdot v_2 = av_1 + v_2$, so $av_1 + v_2 \in V^G$ (and therefore V^G is a subspace) and if $g \in G$ and $v \in V^G$ then $g \cdot v = v \in V^G$, so it is a submodule.

In fact V^G is the isotypic component of V corresponding to the trivial representation.

Example

- If V is irreducible then V^G is a submodule of V, so V^G is equal to $\{0\}$ if V is not the trivial representation, and it is equal to V for the trivial representation.
- $(\mathrm{Hom}(V, W))^G = \mathrm{Hom}_G(V, W) := \{G\text{-linear maps from } V \text{ to } W\}$.
  In fact, if $T \in \mathrm{Hom}(V, W)$, then

$$\begin{aligned} g \cdot T = T\ \forall g \in G \quad &\iff \quad (g^{-1} \cdot T)(v) = T(v)\ \forall g \in G, \forall v \in V \\ &\iff \quad g^{-1} \cdot (T(g \cdot v)) = T(v)\ \forall g \in G, \forall v \in V \\ &\iff \quad T(g \cdot v) = g \cdot (T(v))\ \forall g \in G, \forall v \in V \\ &\iff \quad T \in \mathrm{Hom}_G(V, W). \end{aligned}$$

Theorem 3.12 *(First projection formula)*
Let V be a G-module. Define $\pi : V \to V$ by

$$\pi(v) = \frac{1}{|G|} \sum_{g \in G} g \cdot v.$$

Then π is a G-linear projection and $Im(\pi) = V^G$.

Proof:

Let $\rho : G \to GL(V)$ be the representation. Then

1. π linear: since $\pi = \frac{1}{|G|}\sum_{g\in G}\rho(g)$, π is a linear combination of linear maps, and therefore it is linear.
2. $\mathrm{Im}(\pi) \subseteq V^G$: Let $h \in G$, $v \in V$. Then
$$h \cdot \pi(v) = h \cdot \left(\frac{1}{|G|}\sum_{g\in G} g \cdot v\right) = \frac{1}{|G|}\sum_{g\in G}(hg)\cdot v = \pi(v).$$
Therefore, $\pi(v) \in V^G$ for all $v \in V$.
3. $\mathrm{Im}(\pi) \supseteq V^G$: If $v \in V^G$ then $g \cdot v = v$ for all $g \in G$, and therefore
$$\pi(v) = \frac{1}{|G|}\sum_{g\in G} g \cdot v = \frac{1}{|G|}\sum_{g\in G} v = v.$$
Therefore, if $v \in V^G$, then $v = \pi(v) \in \mathrm{Im}(\pi)$.
4. $\pi^2 = \pi$: In (3) we proved that if $v \in V^G$, $\pi(v) = v$. Since $\pi(v) \in V^G$ for all v by (2), $\pi(\pi(v)) = \pi(v)$.
5. π is G-linear: $\pi(h \cdot v) = \frac{1}{|G|}\sum_{g\in G}(gh)\cdot v = \pi(v) = h \cdot (\pi(v))$.

∎

Corollary 3.13 *Let V be a G-module with character χ. Then*
$$dim(V^G) = \frac{1}{|G|}\sum_{g\in G}\chi(g).$$

Proof: $\pi = \frac{1}{|G|}\sum_{g\in G}\rho(g)$. Take traces in both sides to get
$$\dim(V^G) = \dim(\mathrm{Im}(\pi)) = \mathrm{Trace}(\pi) = \frac{1}{|G|}\sum_{g\in G}\mathrm{Trace}(\rho(g)) = \frac{1}{|G|}\sum_{g\in G}\chi(g).$$

∎

Using this tool, let us study inner products of characters.

Proposition 3.14 *Let V, W be G-modules with characters χ_V, χ_W respectively. Then*
$$\langle\chi_V, \chi_W\rangle = dim(Hom_G(V, W)).$$

Proof: Recall that $\chi_{\mathrm{Hom}(V,W)} = \chi_W\overline{\chi_V}$. Recall also that $(\mathrm{Hom}(V, W))^G = \mathrm{Hom}_G(V, W)$ (example after definition 3.10). Using this and the previous corollary (corollary 3.13) we have
$$\mathrm{Hom}_G(V, W) = \dim(\mathrm{Hom}(V, W))^G = \frac{1}{|G|}\sum_{g\in G}\chi_{\mathrm{Hom}(V,W)}(g) = \frac{1}{|G|}\sum_{g\in G}\chi_W(g)\overline{\chi_V}(g) = \langle\chi_V, \chi_W\rangle.$$

∎

Corollary 3.15 *Let V, W be representations of G.*

1. *The inner product of two characters is always a nonnegative integer.*
2. *$dim(Hom_G(V,W)) = \langle \chi_V, \chi_W \rangle = \langle \chi_W, \chi_V \rangle = dim(Hom_G(W,V))$.*

Proof: Clear. ∎

Proposition 3.16 *If V and W are irreducible representations then*

$$dim(Hom_G(V,W)) = \begin{cases} 1 & if \quad V \cong W \\ 0 & if \quad V \ncong W \end{cases}$$

Proof: $\dim(\mathrm{Hom}_G(V,W))$ is the multiplicity of V in W (see theorem 2.15). If W is isomorphic to V, then the multiplicity of V in W is 1, and if W is not isomorphic to V, then the multiplicity of V in W is 0. ∎

Theorem 3.17 *Let $\chi_1, \ldots, \chi_\ell$ be distinct irreducible characters. Then*

$$\langle \chi_i, \chi_j \rangle = \begin{cases} 1 & if \quad i = j \\ 0 & if \quad i \neq j \end{cases}$$

Proof: Clear from the last two propositions. ∎

3.5 Character determines representation

Recall from last lecture:

- $\langle \chi_V, \chi_W \rangle = \dim(\mathrm{Hom}_G(V, W))$.
- If $U_1, \dots, U_k$ irreducible, then $\langle \chi_i, \chi_j \rangle = \delta_{ij}$.

Theorem 3.18 *(Fundamental Theorem of Representation Theory)*
Let V, W be G-modules. Then $V \cong W \iff \chi_V = \chi_W$.

Proof:

($\Rightarrow$) already proved (Prop. 3.5 (a)).

($\Leftarrow$) Let $U_1, \dots, U_k$ be the irreducible representations of G, with characters $\chi_1, \dots, \chi_k$. By complete reducibility we have

$$\begin{aligned} V &\cong a_1U_1 \oplus \cdots \oplus a_kU_k, &\quad& \text{where } a_i = \dim(\mathrm{Hom}_G(U_i, V)) = \langle \chi_V, \chi_i \rangle \\ W &\cong b_1U_1 \oplus \cdots \oplus b_kU_k, && \text{where } b_i = \dim(\mathrm{Hom}_G(U_i, W)) = \langle \chi_W, \chi_i \rangle \end{aligned}$$

Since $\chi_V = \chi_W$ by assumption, we have $a_i = b_i$ for all i and therefore $V \cong W$.

■

The following is quite interesting and useful.

Theorem 3.19 *χ irreducible $\iff \langle \chi, \chi \rangle = 1$.*

Proof:

($\Rightarrow$) already proved (Theorem 3.17).

($\Leftarrow$) Suppose V is a G-module with character χ satisfying $\langle \chi, \chi \rangle = 1$. Let $U_1, \dots, U_k$ be the irreducible representations of G, with characters $\chi_1, \dots, \chi_k$. By complete reducibility we have

$$V \cong a_1U_1 \oplus \cdots \oplus a_kU_k, \text{ where } a_i = \dim(\mathrm{Hom}_G(U_i, V)) = \langle \chi_V, \chi_i \rangle.$$

By Corollary 3.7, $\chi = a_1\chi_1 + \cdots + a_k\chi_k$. Therefore, since $\langle \chi_i, \chi_j \rangle = \delta_{ij}$, we have

$$1 = \langle \chi_V, \chi_V \rangle = \langle a_1\chi_1 + \cdots + a_k\chi_k, a_1\chi_1 + \cdots + a_k\chi_k \rangle = a_1^2 + \cdots + a_k^2.$$

This implies that all the a_i are 0 except for one of them, i.e. V is isomorphic to one of the U_i and therefore irreducible.

■

Theorem 3.20 *The multiplicity of an irreducible G-module U_i in $\mathbb{C}G$ is equal to $\dim(U_i)$.*

Proof: Write $\mathbb{C}G \cong a_1U_1 \oplus \cdots \oplus a_kU_k$. We will give two proofs:

1) (Without using characters)

$$\begin{aligned} a_i &= \dim(\mathrm{Hom}_G(U_i, \mathbb{C}G)) && \text{(Theorem 2.15)} \\ &= \dim(\mathrm{Hom}_G(\mathbb{C}G, U_i)) && \text{(Ex. Sheet 5)} \\ &= \dim(U_i) && \text{(Proposition 2.16)} \end{aligned}$$

2) (Using characters)

$$a_i = \langle \chi_{\text{reg}}, \chi_i \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_{\text{reg}}(g)\overline{\chi_i(g)} = \frac{1}{|G|}\ |G|\ \overline{\chi_i(1)} = \dim(U_i),$$

where the third equality comes from the fact that $\chi_{\text{reg}}(g) = 0$ if $g \neq 1$ and $\chi_{\text{reg}}(1) = |G|$.

∎

Corollary 3.21 *Let $U_1, \ldots, U_k$ be the irreducible representations of G, and let $d_i := dim(U_i)$. Then $|G| = d_1^2 + \cdots + d_k^2$.*

Proof:

We actually proved this before. It is easy using characters:

$$|G| = \dim(\mathbb{C}G) = \sum_{i=1}^{k} a_i \dim(U_i) = \sum_{i=1}^{k} d_i^2$$

since $a_i = d_i = \dim(U_i)$ by the previous theorem.

∎

3.6 Conjugacy classes, class functions and the number of irreducible representations.

Recall:

Definition: Let G be a group and let $x, y \in G$. We say that x is conjugate to y if there exists $g \in G$ such that $y = gxg^{-1}$ (or if you prefer, $y = g^{-1}xg$; it is of course equivalent).

Definition 3.22 *Let G be a group and let $x \in G$. The conjugacy class of x, denoted x^G, is the set*

$$x^G = \{gxg^{-1} : g \in G\}.$$

NOTE: Conjugacy is an equivalence relation. Therefore every group G gets partitioned into its conjugacy classes:

$$G = x_1^G \cup x_2^G \cup \cdots \cup x_k^G,$$

where $x_1, x_2, \ldots, x_k$ are representatives of the different conjugacy classes.

Examples:

- $1^G = \{1\}$ since $g\,1\,g^{-1} = 1$ for all $g \in G$.
- G abelian $\iff$ $gxg^{-1} = x$ for all $g, x \in G$ $\iff$ $x^G = \{x\}$ for all $x \in G$.

Recall:

Definitions:

- The centraliser of $x \in G$ is the set (actually subgroup)

$$C_G(x) = \{g \in G : gxg^{-1} = x\}.$$

- The centre of G is the set (actually subgroup)

$$Z(G) = \{g \in G : gh = hg \text{ for all } h \in G\}.$$

FACTS: (exercise sheet 7)

- $\langle x \rangle \leq C_G(x) \leq G$.
- $Z(G) \leq C_G(x)$ for all $x \in G$.

Proposition 3.23

$$|x^G| = \frac{|G|}{|C_G(x)|}.$$

In particular, both $|x^G|$ and $|C_G(x)|$ divide G.

Proof: Define $\phi : \{\text{right cosets of } C_G(x) \text{ in } G\} \to x^G$ by $\phi(g\, C_G(x)) = gxg^{-1}$. Then ϕ is well defined an bijective (ex. sheet 7) and therefore the cardinality of the two sets is the same, i.e.

$$\frac{|G|}{|C_G(x)|} = |\{\text{right cosets of } C_G(x) \text{ in } G\}| = |x^G|.$$

∎

Proposition 3.24 *(Class equation) Let $x_1, \dots, x_k$ be representatives of the different conjugacy classes of G. Then*

$$|G| = |Z(G)| + \sum_{x_i \notin Z(G)} |x_i^G|.$$

Proof: Since conjugacy classes partition G,

$$|G| = \sum_{i=1}^{k} |x_i^G| = \sum_{x_i \in Z(G)} |x_i^G| + \sum_{x_i \notin Z(G)} |x_i^G| = \sum_{x_i \in Z(G)} 1 + \sum_{x_i \notin Z(G)} |x_i^G| = |Z(G)| + \sum_{x_i \notin Z(G)} |x_i^G|,$$

since $x_i^G = \{x_i\}$ when $x_i \in Z(G)$.

∎

Class functions

Definition 3.25 *$f : G \to \mathbb{C}$ is a* class function *if f is constant on conjugacy classes, i.e.*

$$f(gxg^{-1}) = f(x) \quad \forall x, g \in G.$$

The set of class functions is denoted $\mathbb{C}_{\text{class}}G$.

Lemma 3.26

$$\textit{dim}(\mathbb{C}_{\text{class}}G) = \textit{number of conjugacy classes of } G.$$

Proof:

Let $C_1, \dots, C_k$ be the conjugacy classes of G. Define $\delta_i : G \to \mathbb{C}$ by

$$\delta_i(g) = \begin{cases} 1 & \text{if} \quad g \in C_i \\ 0 & \text{if} \quad g \notin C_i \end{cases}$$

Then $\{\delta_1, \dots, \delta_k\}$ is a basis of $\mathbb{C}_{\text{class}}G$ (exercise sheet 7), so $\dim(\mathbb{C}_{\text{class}}G) = k$.

∎

Corollary 3.27 *The number of irreducible representations of a group is less than or equal to the number of conjugacy classes of that group.*

Proof: The set of irreducible characters of G forms a linearly independent subset (since characters are orthonormal) of the set of class functions, and its cardinality is equal to the number of irreducible representations of G. Thus, the number of irreducible representations of G is less than or equal to the dimension of the space of class functions, which is equal to the number of conjugacy classes of G.

∎

Conjugacy classes, class functions and the number of irreducible representations (cont.)

GOAL: Prove that the number of conjugacy classes of a group is equal to the number of irreducible representations.

We have already proved that the number of irreducible representations is less than or equal to the number of conjugacy classes of a group. To prove the opposite inequality we need some tools.

For V a representation of G and $f \in \mathbb{C}G$, define

$$\begin{array}{rcl} T_f : V & \rightarrow & V \\ v & \rightarrow & T_f(v) := \sum_{g \in G} f(g)\, g \cdot v. \end{array}$$

Note that T_f is defined for any representation $\rho : G \rightarrow GL(V)$; it can also be expressed as

$$T_f = \sum_{g \in G} f(g)\, \rho(g).$$

When V is the regular representation $\mathbb{C}G$, T_f has some interesting properties:

Lemma 3.28 *Let $f \in \mathbb{C}G$ and consider $T_f : \mathbb{C}G \rightarrow \mathbb{C}G$. Suppose that T_f os G-linear. Then*

(i) $T_f(\delta_h) = h \cdot f$ for all $h \in G$.

(ii) $T_f = 0$ (as a map) implies $f = 0$.

Proof:

(i) Since we are supposing that T_f is G-linear,

$$T_f(\delta_h) = T_f(h \cdot \delta_1) = h \cdot T_f(\delta_1) = h \cdot \left(\sum_{g \in G} f(g)\, g \cdot \delta_1 \right) = h \cdot \left(\sum_{g \in G} f(g)\, \delta_g \right) = h \cdot f.$$

(ii) $T_f = 0$ implies, using (i), $0 = T_f(\delta_1) = 1 \cdot f = f$.

∎

The following characterises those $f \in \mathbb{C}G$ such that T_f is G-linear for every representation of G.

Theorem 3.29 *$T_f : V \rightarrow V$ is G-linear for every representation V of G $\iff$ f is a class function.*

Proof:

($\Leftarrow$) Let V be a representation of G and suppose that $f \in \mathbb{C}_{\text{class}}G$. Then for any $h \in G$ and $v \in V$,

$$h \cdot (T_f(v)) = h \cdot \left(\sum_{g \in G} f(g)\, g \cdot v \right) = \sum_{g \in G} f(g)\, (hg) \cdot v.$$

Change the summation variable: let $u = hgh^{-1}$. Then the last expression equals

$$\sum_{g \in G} f(g)\, (hg) \cdot v = \sum_{u \in G} f(h^{-1}uh)\, (hh^{-1}uh) \cdot v = \sum_{u \in G} f(u)\, u \cdot (h \cdot v) = T_f(h \cdot v),$$

where the hypothesis that f is a class function was used in the second equality. This proves that T_f is G-linear.

($\Rightarrow$) If T_f is G-linear for every representation of G in particular it is G-linear for the regular representation $\mathbb{C}G$. We will show that $f(g^{-1}hg) = f(h)$ for all $g, h \in G$.

$$\begin{aligned}
f(g^{-1}hg) &= (g \cdot f)(hg) \quad \text{by definition of the regular representation} \\
&= \big(T_f(\delta_g)\big)(hg) \quad \text{by Lemma 3.28} \\
&= \left(\sum_{u \in G} f(u)\, u \cdot \delta_g\right)(hg) \quad \text{by def. of } T_f \\
&= \left(\sum_{u \in G} f(u)\, \delta_{ug}\right)(hg) \quad \text{by properties of regular rep.} \\
&= \sum_{u \in G} f(u)\, \delta_{ug}(hg) \\
&= f(h) \quad \text{since } \delta_{ug}(hg) = 1 \text{ if } u = h \text{ and } 0 \text{ otherwise.}
\end{aligned}$$

∎

Now we will prove that irreducible characters span the space of class functions. We need the following technical lemma.

Lemma 3.30 *If χ is irreducible, so is $\overline{\chi}$.*

Proof: Use Theorem 3.19: $\langle \overline{\chi}, \overline{\chi} \rangle = \langle \chi, \chi \rangle = 1$ since χ irreducible. Hence $\overline{\chi}$ irreducible.

∎

Theorem 3.31 *Irreducible classes span $\mathbb{C}_{class}G$.*

Proof: Suppose that the span of the set of irreducible characters is not all of $\mathbb{C}_{\text{class}}G$. Then there exists $f \in \mathbb{C}_{\text{class}}G$, with $f \neq 0$, that is perpendicular to the span of the set of irreducible characters, i.e. $\langle f, \chi \rangle = 0$ for every irreducible character χ.

So let $\rho : G \to GL(U)$ be an irreducible representation of G with character χ and consider the function $T_f : U \to U$. By the previous theorem, T_f is G-linear since $f \in \mathbb{C}_{\text{class}}G$. But since U is irreducible, Schur's lemma (ii) implies that $T_f = \lambda\, \text{Id}_U$ for some $\lambda \in \mathbb{C}$. Therefore we have

$$\lambda\, \text{Id}_U = \sum_{g \in G} f(g)\, \rho(g),$$

and taking traces we obtain

$$\lambda \dim(U) = \sum_{g \in G} f(g)\, \chi(g).$$

Now observe that the right hand side equals $\langle f, \overline{\chi} \rangle$, which is 0 by assumption. Therefore we have

$$\lambda \dim(U) = 0,$$

which implies $\lambda = 0$ and therefore $T_f = 0$. But then Lemma 3.28 (ii) gives $f = 0$, which is a contradiction.

∎

Corollary 3.32 *The number of irreducible representations of a group is equal to the number of conjugacy classes of the group.*

Proof: Clear:

$$\begin{aligned}|\{\text{conjugacy classes}\}| = \dim(\mathbb{C}_{\mathsf{class}}G) &= \dim(\text{span}(\{\text{irreducible characters}\}))\\ &= \text{number of irreducible representations.}\end{aligned}$$

$\blacksquare$

This has several consequences. For example,

Proposition 3.33 *(Characters separate conjugacy classes)*
Let $g, h \in G$. Then g and h are in the same conjugacy class of and only if $\chi(g) = \chi(h)$ for every character χ.

Proof:
If g and h are in the same conjugacy class then $\chi(g) = \chi(h)$ since characters are class functions. Conversely, if $\chi(g) = \chi(h)$ for every character χ, define

$$\delta(x) = \begin{cases} 1 & \text{if} \quad x \in g^G \\ 0 & \text{if} \quad x \notin g^G \end{cases}$$

Then δ is a class function, so it can be expressed as a linear combination of the set of irreducible characters:

$$\delta = \sum_{i=1}^{k} a_i \chi_i \quad \text{for some complex coefficients } a_i.$$

Therefore,

$$1 = \delta(g) = \sum_{i=1}^{k} a_i \chi_i(g) = \sum_{i=1}^{k} a_i \chi_i(h) = \delta(h),$$

since by assumption $\chi_i(g) = \chi_i(h)$ for all i. This implies that $h \in g^G$.

$\blacksquare$

Corollary 3.34 *An element $g \in G$ is conjugate to g^{-1} if and only if $\chi(g)$ is real for every character χ.*

Proof: Recall that for every character χ, $\chi(g^{-1}) = \overline{\chi(g)}$ by properties of characters.
If g^{-1} is conjugate to g then $\chi(g) = \chi(g^{-1})$ by properties of characters, so $\chi(g)$ must be real.
Conversely, if $\chi(g)$ is real then $\chi(g^{-1}) = \chi(g)$ for every character χ, so the last theorem implies that g is conjugate to g^{-1}.

$\blacksquare$

3.7 Orthogonality relations and character tables

Throughout this section $U_1, \ldots, U_\ell$ will denote the irreducible representations of the finite group G with characters $\chi_1, \ldots, \chi_\ell$, and $g_1, \ldots, g_\ell$ will denote representatives of the conjugacy classes of G.

Note that the characters χ_i are completely determined by their values at $g_1, \ldots, g_\ell$ (since they are class functions).

Definition 3.35 *The character table of the group G is the $\ell \times \ell$ matrix whose entry ij is $\chi_i(g_j)$.*

Note on ordering: We will always assume that $g_1 = \mathbf{1}$ and that χ_1 is the trivial representation.

Example:

For $G = S_3$, take $\mathbf{1}$, (123) and (12) as representatives of the conjugacy classes. Then the character table of G is

g_i	$\mathbf{1}$	(123)	(12)
χ_1	1	1	1
χ_2	1	1	-1
χ_3	2	-1	0

It is useful to have in the table the size of the centraliser of each conjugacy class for reasons that we will see immediately. Thus the table of S_3 will look like

g_i	$\mathbf{1}$	(123)	(12)
$\lvert C_G(g_i)\rvert$	6	3	2
χ_1	1	1	1
χ_2	1	1	-1
χ_3	2	-1	0

The columns and rows of character tables satisfy some orthogonality relations, as follows.

Let χ and ψ be characters. Since χ and ψ are class functions, $\chi(g) = \chi(g_k)$ and $\psi(g) = \psi(g_k)$ for all g in g_k^G. Thus,

$$\begin{aligned}
\langle \chi, \psi \rangle &= \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\psi(g)} \\
&= \frac{1}{|G|} \sum_{k=1}^{\ell} |g_k^G|\, \chi(g_k)\overline{\psi(g_k)} \\
&= \frac{1}{|G|} \sum_{k=1}^{\ell} \frac{|G|}{|C_G(g_k)|}\, \chi(g_k)\overline{\psi(g_k)} \\
&= \sum_{k=1}^{\ell} \frac{\chi(g_k)\overline{\psi(g_k)}}{|C_G(g_k)|}
\end{aligned}$$

The irreducible characters χ_i are orthonormal, and therefore we have the **row orthogonality relations**:

$$\sum_{k=1}^{\ell} \frac{\chi_i(g_k)\overline{\chi_j(g_k)}}{|C_G(g_k)|} = \langle \chi_i, \chi_j \rangle = \delta_{ij}.$$

Now consider the matrix M whose ij-entry is

$$M_{ij} = \frac{\chi_i(g_j)}{\sqrt{C_G(g_j)}}.$$

Then (recall that a star to the right top of a matrix means the transpose and conjugate of the matrix):

$$(MM^*)_{ij} = \sum_{k=1}^{\ell} M_{ik}\,(M^*)_{kj} = \sum_{k=1}^{\ell} M_{ik}\overline{M}_{jk} = \sum_{k=1}^{\ell} \frac{\chi_i(g_k)\overline{\chi_j(g_k)}}{\sqrt{|C_G(g_k)|}\sqrt{|C_G(g_k)|}} = \delta_{ij}.$$

In other words, we have $MM^* = I$. This implies $M^{-1} = M^*$ and therefore $M^*M = I$. Hence

$$(M^*M)_{ij} = \sum_{k=1}^{\ell} (M^*)_{ik} M_{kj} = \sum_{k=1}^{\ell} \overline{M}_{ki} M_{kj} = \sum_{k=1}^{\ell} \frac{\chi_k(g_j)\overline{\chi_k(g_i)}}{\sqrt{|C_G(g_i)|}\sqrt{|C_G(g_j)|}} = \delta_{ij}$$

and therefore we have the **column orthogonality relations**:

$$\sum_{k=1}^{\ell} \chi_k(g_i)\overline{\chi_k(g_j)} = |C_G(g_i)|\;\delta_{ij}.$$

Summarising

Theorem 3.36

$$\sum_{k=1}^{\ell} \frac{\chi_i(g_k)\overline{\chi_j(g_k)}}{|C_G(g_k)|} = \delta_{ij} \quad (\textit{row orthogonality})$$
$$\sum_{k=1}^{\ell} \chi_k(g_i)\overline{\chi_k(g_j)} = |C_G(g_i)|\delta_{ij} \quad (\textit{column orthogonality})$$

Proof:

Done above.

∎

For the examples it is useful to recall the following result.

Consider the group S_n. Then every element $x \in S_n$, $x \neq \mathbf{1}$, can be written uniquely as a product of cycles $(a_1 \cdots a_{k_1})(b_1 \cdots b_{k_2})(c_1 \cdots c_{k_s})$, with $k_1 \geq k_2 \geq \cdots \geq k_s$.

The s-tuple $(k_1, k_2, \ldots, k_s)$ is called the *shape* of x. For example, (12) has shape (2) and (123)(45) has shape $(3, 2)$.

FACT: For $x \in S_n$, x^{S_n} = elements of S_n with the same shape as x.

Example:

Let us go back to the character table of $G = S_3$. Suppose that we only know the size of the conjugacy classes of $\mathbf{1}$ (size 1), (12) (size 3), and (123) (size 2). Then $|C_G(\mathbf{1})| = 6/1 = 6$, $|C_G((123))| = 6/2 = 3$, $|C_G((12))| = 6/3 = 2$. This implies in particular that S_3 is not abelian and it has 3 irreducible representations. Since the sum of the squares of the dimensions of the irreducible representations is equal to the order of the group, we see that S_3 has 3 characters of degrees 1, 1 and 2. So we immediately have (the first row corresponds to the trivial representation and the first column is $\chi_i(\mathbf{1}) = \text{degree}(\chi_i)$)

g_i	$\mathbf{1}$	(123)	(12)
$\lvert C_G(g_i)\rvert$	6	3	2
χ_1	1	1	1
χ_2	1	a	b
χ_3	2	c	d

Now we can determine a, b, c, d from the orthogonality relations. Column orthogonality gives

$$1+a+2c=0 \qquad 1+|a|^2+|c|^2=3 \qquad 1+b+2d=0 \qquad 1+|b|^2+|d|^2=2 \qquad 1+a\bar{b}+c\bar{d}=0,$$

and row orthogonality gives

$$\frac{1}{6}+\frac{a}{3}+\frac{b}{2}=0 \qquad \frac{2}{6}+\frac{c}{3}+\frac{d}{2}=0 \qquad \frac{1}{6}+\frac{|a|^2}{3}+\frac{|b|^2}{2}=0 \qquad \frac{1}{6}+\frac{|c|^2}{3}+\frac{|d|^2}{2}=0 \qquad \frac{1}{6}+\frac{a\bar{c}}{3}+\frac{b\bar{d}}{2}=0.$$

The only solution to these equations is $a=1$, $b=-1$ $c=-1$, $d=0$. In other words, with very little information about the group the orthogonality relations give the whole character table almost for free.

The same technique gives the character table for S_4. To simplify matters we are also assuming that we have the second row for free: it corresponds to the (irreducible) linear representation of S_n given by the sign, i.e.

$$\rho_2(x)(v) = \mathrm{sign}(x)\, v.$$

The character table of S_4 is

g_i	**1**	(12)	(123)	(1234)	(12)(34)
$\lvert C_G(g_i)\rvert$	24	4	3	4	8
χ_1	1	1	1	1	1
χ_2	1	-1	1	-1	1
χ_3	2	0	-1	0	2
χ_4	3	1	0	-1	-1
χ_5	3	-1	0	1	-1

3.8 The number of linear characters

Recall that a linear character is a character of index 1 and that linear characters are the only characters that are homomorphisms.

In this section the goal is to prove that the number of linear characters of a group divides the order of the group.

Throughout this section $\chi_1, \dots, \chi_k$ will be a complete set of linear characters of a group G (i.e. the set of all the linear characters of G).

Let $D(k, \mathbb{C})$ be the group of diagonal k by k matrices and consider the map $R : G \to D(k, \mathbb{C})$ given by

$$R(g) = \begin{pmatrix} \chi_1(g) & 0 & \cdots & 0 \\ 0 & \chi_2(g) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \chi_k(g) \end{pmatrix}$$

The map R is a homomorphism since each χ_i is. Let $H = \ker(R)$ and let $\hat{G} = \mathrm{Im}(R)$. Then

Lemma 3.37 *$|\hat{G}|$ divides $|G|$.*

Proof: $G/H \cong \mathrm{Im}(R) = \hat{G}$, so $|G| = |H||\hat{G}|$.

∎

Lemma 3.38 *G and $\hat{G}$ have the same number of linear characters.*

Proof: Consider $R : G \to \hat{G} \subseteq D(k, \mathbb{C})$ as before. Define a function

$$L : \{\text{Linear characters of } \hat{G}\} \to \{\text{Linear characters of } G\}$$

by

$$L(\hat{\chi}) = \hat{\chi} \circ R.$$

- L is well defined: since $\hat{\chi}$ and R are homomorphisms, $\hat{\chi} \circ R$ is also a homomorphism from G to $\mathbb{C}$, and therefore it is a linear character (see exercise sheet 5, exercise 6).
- L is injective: suppose that $\hat{\chi} \circ R = \hat{\psi} \circ R$. Let $\hat{g} \in \hat{G}$. Then $\hat{g} = R(g)$ for some $g \in G$ and therefore
$$\hat{\chi}(\hat{g}) = \hat{\chi}(R(g)) = \hat{\chi} \circ R(g) = \hat{\psi} \circ R(g) = \hat{\psi}(R(g)) = \hat{\psi}(\hat{g}).$$
Thus $\hat{\chi} = \hat{\psi}$.
- L is onto: let $\hat{\chi}_j : \hat{g} \to \mathbb{C}$, $1 \le j \le k$, be the character defined by
$$\hat{\chi}_j \left(\begin{pmatrix} z_1 & 0 & \cdots & 0 \\ 0 & z_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 \cdots & z_k \end{pmatrix} \right) = z_j.$$
It is easy to show that $\hat{\chi}_j$ is a homomorphism from $\hat{G}$ to $\mathbb{C}$ and therefore it really is a linear character. In addition, for any $g \in G$ we have
$$(L(\hat{\chi}_j))(g) = \hat{\chi}_j(R(g)) = \hat{\chi}_j \left(\begin{pmatrix} \chi_1(g) & 0 & \cdots & 0 \\ 0 & \chi_2(g) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \chi_k(g) \end{pmatrix} \right) = \chi_j(g).$$

This implies that L is onto.

Therefore L is a bijective function between the set of linear characters of $\hat{G}$ and the set of linear characters of G, which implies that these two sets have the same cardinality.

∎

Theorem 3.39 *The number of linear characters of a group G divides $|G|$.*

Proof: Notice that $\hat{G}$ is abelian since it is a subgroup of the abelian group $D(k, \mathbb{C})$ of diagonal k by k matrices. This implies that all the characters of $\hat{G}$ are linear and therefore $\hat{G}$ has $|\hat{G}|$ linear characters. Then Lemma 3.29 implies that G has $|\hat{G}|$ linear characters and Lemma 3.28 implies that $|\hat{G}|$ divides $|G|$, proving the result.

∎

Summary of character conditions

Let G be a group. Suppose that $\chi_1, \ldots, \chi_k$ is a complete set of irreducible characters of G with degrees $d_1, \ldots, d_k$ respectively.

- $d_1 = 1$ and $\sum_{i=1}^{k} d_i^2 = |G|$.
- $\chi_i(\mathbf{1}) = d_i$.
- $\chi_1(g_i) = 1$.
- $k = \#\{\text{conjugacy classes of } G\} = \dim(\mathbb{C}_{\text{class}} G)$.
- $\#\{\text{linear characters}\}$ divides $|G|$.
- If χ is a linear character and ψ is an irreducible character, then $\chi\psi$ is also an irreducible character.
- Row orthogonality: $\displaystyle\sum_{\ell=1}^{k} \frac{\chi_i(g_\ell)\overline{\chi_j(g_\ell)}}{|C_G(g_\ell)|} = \delta_{ij}$.
- Column orthogonality: $\displaystyle\sum_{\ell=1}^{k} \chi_\ell(g_i)\overline{\chi_\ell(g_j)} = |C_G(g_i)|\, \delta_{ij}$.
- d_i divides $|G|$ (Chapter 4 – not proved yet).
- The only rational values that characters can take are integers (i.e. $chi(g) = 3/4$, for example, is impossible). (Chapter 4 – not proved yet.)

These conditions are very powerful. Some examples:

Example: Suppose that $|G| = p$, p a prime. Let $d_1, d_2, \ldots, d_k$ be the indexes of the irreducible characters, with $d_1 = 1$ corresponding to the trivial character. If one of the d_i is not 1 then it must be p since d_i divides $|G| = p$. This leads to $p = 1 + d_1^2 + \cdots + d_k^2 \geq 1 + p^2$, which is false. Therefore all the d_i are 1 and therefore G is abelian.

Example: Suppose that $|G| = p^2$, p a prime. Ths same argument as before will give $p^2 \geq p^2 + 1$ if one of the d_i is not equal to 1. Therefore all groups of order p^2, p a prime, are abelian.

Example: Let G be a group of index 77. The irreducible representations of G must have indexes that divide 77, so the only possibilities are 1, 7, 11 or 77. Since the sum of the squares of the indexes must equal 77, 11 and 77 are ruled out as possible indexes. If there is an irreducible representation with index 7 (there cannot be two since $7^2+7^2 > 77$), then there would be $77-7^2 = 28$ linear representations. But this is impossible since the number of linear representations divide the order of the group. Thus the only possibility left is that all the irreducible representations of G are linear, and we conclude that all the groups of order 77 are abelian.

Example: Let G be a group of order pq, where p and q are primes and $p < q$ (the case $p = q$ was considered above). Let $d_1, d_2, \ldots, d_k$ be the indexes of the irreducible characters, with $d_1 = 1$ (the trivial character). We have that the d_i can only be 1, p, q or pq. q and pq are ruled out, as in the previous example, because $pq < q^2$ and $pq < (pq)^2$. So the only possibility is that some of the d_i (say the first r of them) are 1 and the rest ($k - r$ of them) are p. We then have the equation

$$pq = \sum_{i=1}^{k} d_i^2 = \sum_{i=1}^{r} d_i^2 + \sum_{i=r+1}^{k} d_i^2 = r + p^2(k - r).$$

Since there are r linear characters, r must be 1, p, q or pq. If $r = pq$ then G is abelian. If r is 1 or q, the left hand side of the equation is divisible by p and the right hand side is not, so this cases are ruled out. If $r = p$ then we have

$$pq = p + p^2(k - p) = p(1 + p(k - p))$$

and therefore

$$q = 1 + p(k - p).$$

In other words, if G is not abelian then $q \equiv 1 \ (\mathrm{mod} p)$.

Summarizing: if G is a group of order pq, where p and q are primes and $p < q$, and if $q \not\equiv 1 \ (\mathrm{mod} p)$, then G is abelian.

Note that there are nonabelian groups of order pq when $q \equiv 1 \ (\mathrm{mod} p)$. An example is S_3, which has order $6 = 2 \cdot 3$.

Chapter 4

Algebraic integers and character values.

4.1 Algebraic integers

Definition 4.1 *An algebraic integer is a root of a monic polynomial with integer coefficients. (Recall that monic means that its leading coefficient is 1.)*

Examples

- If n is an integer, it is an algebraic integer since it is a root of $z - n$.
- Roots of unity are algebraic integers: they are roots of $z^n - 1$.
- If α is an algebraic integer, so is $\bar{\alpha}$ since roots of polynomials with integer coefficients come in conjugate pairs.

An alternative characterisation of algebraic integers is the following.

Lemma 4.2 *α is an algebraic integer if and only if it is an eigenvalue of a matrix with integer entries.*

Proof:

If α is an eigenvalue of a matrix with integer coefficients then it is a root of the characteristic polynomial of that matrix, which has integer entries.

Conversely, if α is an algebraic integer then it is a root of some polynomial $P(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0$. Since the characteristic polynomial of the matrix

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{n-2} & -a_{n-1} \end{pmatrix}$$

is $(-1)^n P(z)$ (Exercise sheet 9), α is an eigenvalue of this matrix.

■

Algebraic integers share many properties with ordinary integers. For example

Lemma 4.3 *If α and β are algebraic integers then $\alpha + \beta$ and $\alpha\beta$ also are algebraic integers.*

Proof:

Omitted (long and not particularly interesting).

∎

Proposition 4.4 *Character values are algebraic integers. I.e. if χ is a character, then $\chi(g)$ is an algebraic integer for all g.*

Proof:

Clear from the previus theorem and the example above since $\chi(g)$ is a sum of m^{th} roots of unity, where m is the order of g.

∎

Proposition 4.5 *The only algebraic integers that are rational numbers are the ordinary integers. I.e. if $\lambda \in \mathbb{Q}$ is an algebraic integer, then $\lambda \in \mathbb{Z}$.*

Proof:

Write $\lambda = p/q$ where $p, q \in \mathbb{Z}$ and p and $q \neq 0$ are relatively prime. Since λ is an algebraic integer it must be a root of some polynomial $z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0$, where the a_i are integers. Therefore we have

$$\frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + \cdots + a_1\frac{p}{q} + a_0 = 0,$$

and multiplying by q^n,

$$p^n + a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1} + q^n = 0.$$

This implies that q divides p^n, which implies that q divides p and therefore $q = 1$. Hence $p/q \in Z$.

∎

Corollary 4.6 *Character values can never take rational non-integer values. I.e. if $\chi(g) \in \mathbb{Q}$ then $\chi(g) \in \mathbb{Z}$.*

Proof: Clear from the two previous propositions.

∎

4.2 The index of an irreducible representation divides the order of the group

GOAL: Prove that if U is an irreducible representation of a group G then $\dim(U)$ divides $|G|$.

The idea is to prove that $|G|/\dim(U)$ is an algebraic integer and then use Proposition 4.5. But the argument is very slick.

First let us recall some tool that we have used before: Given $f \in \mathbb{C}G$, and given V a representation of G, recall that we had defined the linear map $T_f : V \to V$ by

$$T_f(v) = \sum_{g \in G} f(g)\, g \cdot v.$$

Recall some properties of T_f:

- If $f \in \mathbb{C}_{\text{class}}G$ then $T_f : V \to V$ is G-linear for any representation V.
- If $\rho : G \to GL(V)$ is a representation with character χ then

$$\text{Trace}(T_f) = \sum_{g \in G} f(g)\chi(g).$$

[Since $T_f = \sum_{g \in G} f(g)\rho(g)$.]

In what follows, let $h \in G$ be a fixed element. Consider $\delta_C \in \mathbb{C}G$ given by

$$\delta_C(g) = \begin{cases} 1 & \text{if } \; g \in h^G \\ 0 & \text{if } \; g \notin h^G \end{cases}$$

and consider

$$T_{\delta_C} : \mathbb{C}G \to \mathbb{C}G.$$

Lemma 4.7 *Let $\beta = \{\delta_g : g \in G\}$ be the usual basis of $\mathbb{C}G$. Then the matrix ${}_\beta[T_{\delta_C}]_\beta$ (i.e. the matrix of $T_{\delta_C} : \mathbb{C}G \to \mathbb{C}G$ in the basis β) has integer entries.*

Proof:

$$T_{\delta_C}(\delta_k) = \sum_{g \in G} \delta_C(g)\, g \cdot \delta_k = \sum_{g \in G} \delta_C(g)\, \delta_{gk}.$$

Since $\delta_C(g)$ is either 0 or 1, the matrix of T has only 0's and 1's, and therefore has integer entries. ∎

Now let χ be an irreducible character. Let U be a submodule of $\mathbb{C}G$ whose character is χ (recall that every irreducible G-module is isomorphic to a submodule of $\mathbb{C}G$).

Lemma 4.8 *$T_{\delta_C} u = \lambda\, u$ for all $u \in U$, where*

$$\lambda = |h^G|\, \frac{\chi(h)}{\chi(\mathbf{1})}.$$

Proof: Consider

$$T_{\delta_C}\big|_U : U \to U.$$

Since δ_C is a class function, T_{δ_C} is G-linear and therefore $T_{\delta_C}\big|_U$ is G-linear. Since U is irreducible, Schur's lemma implies that $T_{\delta_C}\big|_U = \lambda\, \text{Id}_U$ for some $\lambda \in \mathbb{C}$.
Take traces in the equality $T_{\delta_C}\big|_U = \lambda\, \text{Id}_U$ to obtain

$$\lambda\, \dim(U) = \sum_{g \in G} \delta_C(g)\, \chi(g) = \sum_{g \in h^G} \chi(g) = |h^G|\, \chi(h),$$

since $\chi(g) = \chi(h)$ for all $g \in h^G$. Since $\dim(U) = \chi(\mathbf{1})$, we finally obtain

$$\lambda = |h^G|\, \frac{\chi(h)}{\chi(\mathbf{1})}.$$

∎

Corollary 4.9 *For $h \in G$ and χ irreducible character,* $\dfrac{|G|\,\chi(h)}{|C_G(h)|\,\chi(\mathbf{1})}$ *is an algebraic integer.*

Proof:

Since $|h^G| = |G|/|C_G(h)|$, the previous lemma implies that $\lambda = \frac{|G|\,\chi(h)}{|C_G(h)|\,\chi(\mathbf{1})}$ is an eigenvalue of T_{δ_C} and therefore an eigenvalue of the matrix ${}_\beta[T_{\delta_C}]_\beta$, which has integer entries by Lemma 4.7. Hence λ is an algebraic integer by Lemma 4.2.

∎

Now we are ready to prove the main theorem of this section.

Theorem 4.10 *If χ is an irreducible character of a group G then $\chi(1)$ divides $|G|$.*

Proof: Let $g_1, \dots, g_k$ be representatives of the conjugacy classes of G. By the last corollary we know that

$$\frac{|G|\,\chi(h)}{|C_G(g_i)|\,\chi(\mathbf{1})}$$

is an algebraic integer for all i. Since $\chi(g_i)$ is an algebraic integer, $\overline{\chi(g_i)}$ also is an algebraic integer for all i, and therefore the expression

$$\sum_{i=1}^{k} \frac{|G|\,\chi(g_i)}{|C_G(g_i)|\,\chi(\mathbf{1})}\,\overline{\chi(g_i)}$$

is also an algebraic integer. But this expression can be written as

$$\frac{|G|}{\chi(\mathbf{1})} \sum_{i=1}^{k} \frac{\chi(g_i)\,\overline{\chi(g_i)}}{|C_G(h)|} = \frac{|G|}{\chi(\mathbf{1})}\langle \chi, \chi \rangle = \frac{|G|}{\chi(\mathbf{1})}.$$

Therefore $|G|/\chi(\mathbf{1})$ is an algebraic integer. Since it is also a rational number, it must be an integer.

This implies that $\chi(\mathbf{1})$ divides $|G|$.

∎

Chapter 5

Burnside's $p^{\alpha}q^{\beta}$ Theorem.

5.1 Algebraic numbers

Definition 5.1 *An algebraic number is a root of a monic polynomial with rational coefficients. (Recall that monic means that its leading coefficient is 1.)*

Notation:

- $\mathbb{Z}[z]$ are polynomials in z with coefficients in $\mathbb{Z}$.
- $\mathbb{Q}[z]$ are polynomials in z with coefficients in $\mathbb{Q}$.

Lemma 5.2 *If α is an algebraic number then there exists a unique monic polynomial $p \in \mathbb{Q}[z]$ with smallest degree such that $p(\alpha) = 0$ and*

(i). *If $r \in \mathbb{Q}[z]$ satisfies $r(\alpha) = 0$ then there is $s \in \mathbb{Q}[z]$ such that $r = p\,s$.*

(ii). *p is irreducible, i.e. there are no polynomials with degree less than the degree of p whose product is p.*

p is called the minimal polynomial *of α.*

Proof:
Exercise sheet 10.

∎

Definition 5.3 *Let α be an algebraic number and let p be its minimal polynomial. The roots of p are called the* conjugates *of α.*

Examples:

- Any algebraic integer α is an algebraic number: if α is a root of a monic polynomial with integer coefficients then, since $\mathbb{Z} \subset \mathbb{Q}$, α is a root of a monic polynomial with rational coefficients.
- Every rational α is an algebraic number: it is a root of $z - \alpha \in \mathbb{Q}[z]$. (This shows that there are strictly more algebraic numbers than algebraic integers, as one should expect.)

- In fact, if α is an algebraic integer, its minimal polynomial lies in $\mathbb{Z}[z]$ (Exercise sheet 10).

We will use the following fact that we state without proof.

Lemma 5.4 *(Some properties of algebraic numbers.)*

(i). *If α and β are algebraic numbers then so is $\alpha+\beta$. Each conjugate to $\alpha+\beta$ is of the form $\alpha'+\beta'$, where α' is conjugate to α and β' is conjugate to β.*

(ii). *If α is an algebraic number and $r \in \mathbb{Q}$, then $r\alpha$ is also an algebraic number and all the conjugates of $r\alpha$ are of the form $r\alpha'$, where α' is conjugate to α.*

Proof:

(i). Omitted.

(ii). Exercise sheet 10.

■

5.2 More on character values

Lemma 5.5 *Let $\rho : G \to GL(V)$ be a representation with character χ, and let $g \in G$. Then*

(i). $\left|\dfrac{\chi(g)}{\chi(\mathbf{1})}\right| \leq 1$, *with equality if and only if $\rho(g) = \lambda\, Id_V$ for some $\lambda \in \mathbb{C}$.*

(ii). *If* $0 < \left|\dfrac{\chi(g)}{\chi(\mathbf{1})}\right| < 1$ *then* $\dfrac{\chi(g)}{\chi(\mathbf{1})}$ *is not an algebraic integer.*

Proof:

(i). This was done in exercise sheet 6, exercise 5. Let us recall the proof. First recall the triangle inequality for complex numbers: if $z_1, \ldots, z_n$ are complex numbers then

$$|z_1 + \cdots + z_n| \leq |z_1| + \cdots + |z_n|,$$

with equality if and only if all the z_i are positive real multiples of each other (or in other words, all z_i have the same argument as complex numbers).

Recall that given $g \in G$, there is a basis of V such that the matrix of $\rho(g)$ in this basis is

$$\begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}$$

where the λ_i are mth roots of unity , with m being the order of g.

Now $\chi(g) = \mathrm{Trace}(\rho(g)) = \lambda_1 + \cdots + \lambda_n$, and $|\lambda_i| = 1$ for all i. Therefore,

$$|\chi(g)| = |\lambda_1 + \cdots + \lambda_n| \leq |\lambda_1| + \cdots + |\lambda_n| = 1 + \cdots + 1 = n = \chi(\mathbf{1}).$$

If equality holds, then all the λ_i have the same argument (by the triangle inequality); they also have the same norm ($= 1$), and therefore they all have the same value, which we call λ. This implies that the matrix of $\rho(g)$ is $\lambda\, I_n$, and therefore $\rho(g) = \lambda\, Id_V$.

(ii). Suppose that $\chi(g)/\chi(\mathbf{1}) < 1$ and that $\chi(g)/\chi(\mathbf{1})$ is an algebraic integer. We will prove that $\chi(g)/\chi(\mathbf{1}) = 0$.

Write $\alpha = \chi(g)/\chi(\mathbf{1})$. Since α is an algebraic integer, it is, in particular, an algebraic number (see the examples after Definition 5.3). Let $p = z^k + a_{k-1}z^{k-1} + \cdots + a_1 z + a_0$ be the minimal polynomial of α. Then it follows also from the examples after Definition 5.3 that $a_0, \ldots, a_{n-1}$ are integers.

Note also that, writing $\chi(g) = \lambda_1 + \cdots + \lambda_n$ as above, the λ_i are algebraic integers (since they are roots of unity). Since $\chi(\mathbf{1}) = n$ we have that $1/\chi(\mathbf{1}) \in \mathbb{Q}$, and therefore, using Lemma 5.4 (ii), that $\lambda_i/\chi(\mathbf{1})$ is an algebraic number. Thus we have that

$$\alpha = \frac{\lambda_1}{\chi(\mathbf{1})} + \cdots + \frac{\lambda_n}{\chi(\mathbf{1})}$$

is an algebraic number with minimal polynomial p.

Lemma 5.4 (i) and (ii) now imply that all the conjugates of α (i.e. the roots of p) are of the form

$$\alpha' = \frac{\lambda'_1}{\chi(\mathbf{1})} + \cdots + \frac{\lambda'_n}{\chi(\mathbf{1})},$$

where λ'_i are conjugates to λ_i.

The minimal polynomial of λ_i has the form $z^\ell - 1$ for some ℓ since λ_i is a root of unity. Therefore, all the conjugates of λ_i are roots of unity and therefore they have norm 1. This implies that if α' is a root of p then

$$|\alpha'| = \left|\frac{\lambda'_1}{\chi(\mathbf{1})} + \cdots + \frac{\lambda'_n}{\chi(\mathbf{1})}\right| \leq \left|\frac{\lambda'_1}{\chi(\mathbf{1})}\right| + \cdots + \left|\frac{\lambda'_n}{\chi(\mathbf{1})}\right| = \frac{1}{n} + \cdots + \frac{1}{n} = 1.$$

The product of all the roots of p is equal to the constant coefficient (i.e. a_0). Therefore $|a_0| < 1$ since $|\alpha'| \leq 1$ for all the roots of p and $|\alpha| < 1$. Since a_0 is an integer, we must have $a_0 = 0$. This implies that the polynomial z divides p. Since p is monic and irreducible, $p(z) = z$, which implies that $\alpha := \chi(g)/\chi(\mathbf{1}) = 0$.

∎

5.3 Some applications to the study of simple groups

Definition 5.6 *A group G is called* simple *if its only normal subgrups are G itself and $\{\mathbf{1}\}$.*

Why are simple groups important? They can be thought of as the 'building blocks' of finite groups. In other words, if one is able to classify all simple groups (this has been kind of done; it is called the 'enormous theorem' and is so enormous that nobody is completely convinced that it is correct) then one can essentially 'construct' all possible finite groups.

The following are two theorems deal with the problem of recognising finite simple groups. They are extremely difficult to prove without the use of representation theory, but not so much with the tools that we have learned in this course. Note however: proofs are tricky!

Theorem 5.7 *Let p be a prime and let $r \geq 1$. If G is a finite group with a conjugacy class of order p^r then G is not simple.*

Proof: Let $g \in G$ with $|g^G| = p^r$. Since $|g^G| = p^r > 1$, this implies that $g \neq Z(G)$ and therefore G not abelian and $g \neq \mathbf{1}$.

Let $\chi_1, \ldots, \chi_k$ be the irreducible characters of G with χ_1 being the trivial character as usual. Use the column orthogonality relations to obtain

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

Since $\chi_1(g) = \chi_1(\mathbf{1}) = 1$, we have

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

or, dividing by p,

$$\sum_{i=2}^{k} \frac{\chi_i(g)\chi_i(\mathbf{1})}{p} = -\frac{1}{p}.$$

The number $1/p$ is NOT an algebraic integer since it is in $\mathbb{Q}$ and not in $\mathbb{Z}$ (see Proposition 4.5). This implies that, for some $i > 1$,

$$\frac{\chi_i(g)\chi_i(\mathbf{1})}{p} \text{ is not an algebraic integer.}$$

(If $\chi_i(g)\chi_i(\mathbf{1})/p$ were algebraic integers for all i, so would their sum be.)

This implies that $\chi_i(g) \neq 0$ (since 0 is an algebraic integer); also, since $\chi_i(g)$ is an algebraic integer by Proposition 4.4, we must have that $\chi_i(\mathbf{1})/p$ is NOT an algebraic integer. In particular, p cannot divide $\chi_i(\mathbf{1})$.

Hence $p^r = |g^G|$ and $\chi_i(\mathbf{1})$ are relatively prime, and therefore we can find numbers $a, b \in \mathbb{Z}$ such that

$$a\,|g^G| + b\,\chi_i(\mathbf{1}) = 1.$$

Multiply over by $\chi_i(g)/\chi_i(\mathbf{1})$ and use the equation $|g^G| = |G|/|C_G(g)|$ (Proposition 3.23). We obtain

$$a\,\frac{|G|}{|C_G(g)|}\,\frac{\chi_i(g)}{\chi(\mathbf{1})} + b\,\chi_i(g) = \frac{\chi_i(g)}{\chi_i(\mathbf{1})}.$$

We know that

$$a\,\frac{|G|}{|C_G(g)|}\,\frac{\chi_i(g)}{\chi_i(\mathbf{1})}$$

is an algebraic integer (see Corollary 4.9) and that $b\,\chi_i(g)$ also is (Proposition 4.4), so the left hand side is an algebraic integer, and therefore $\chi_i(g)/\chi_i(\mathbf{1})$ must be an algebraic integer, and is not zero since $\chi_i(g) \neq 0$.

Thus, since $\chi_i(g)/\chi_i(\mathbf{1})$ is a nonzero algebraic integer, Lemma 5.5 (i) and (ii) imply

$$\left|\frac{\chi_i(g)}{\chi_i(\mathbf{1})}\right| = 1.$$

Let $\rho_i : G \to GL(U_i)$ be the representation corresponding to the character χ_i. Then Lemma 5.5 (i) implies

$$\rho_i(g) = \lambda\,\mathrm{Id}_{U_i}.$$

Consider $K = \ker(\rho_i)$. K is a normal subgroup of G since it is the kernel of a homomorphism. Let us analyse K.

- $K \neq G$. Otherwise ρ_i would be the trivial representation, and it is not by assumption (since $i > 1$).
- $K \neq \{\mathbf{1}\}$: suppose that $K = \{\mathbf{1}\}$. Then ρ_i is injective, which implies that, for all $h \in G$,

  $$\rho_i(gh) = \rho_i(g) \circ \rho_i(h) = (\lambda \operatorname{Id}_{U_i}) \circ \rho_i(h) = \rho_i(h) \circ (\lambda \operatorname{Id}_{U_i}) = \rho_i(h) \circ \rho_i(g) = \rho_i(hg).$$

  Injectivity of ρ_i then implies then that $gh = hg$ for all $h \in G$. Thus, $g \in Z(G)$, which is a contradiction.

Therefore there is only a possibility: K is a normal subgroup that is not G or $\{\mathbf{1}\}$. This implies that G is not simple.

∎

The following is the famous Burnside's $p^\alpha q^\beta$ theorem. It was proved by Burnside in 1897 and until 1972 there was no proof of this theorem that did not make use of representation theoretic tools.

Before stating the theorem, recall Sylow's Theorem:

Theorem (particular case of Sylow 1). If G is a group of order $r^n s$, with r prime and r and s relatively prime, then G has a subgroup of order r^n.

Now we state the last theorem of this course.

Theorem 5.8 *Let p and q be prime and let α and β be nonnegative integers with $\alpha + \beta \geq 2$. If G is a group of order $p^\alpha q^\beta$ then G is not simple.*

Proof:

If either α or β is 0 then G has order the power of a prime. Using exercise sheet 7, exercise 6 (i), we must have that G is either abelian or has $Z(G)$ as a nontrivial normal subgroup. In either case, G is not simple. (If G abelian of order p^α with $\alpha \geq 2$ then G has a subgroup, which is necessarily normal, of order p, and so it is not simple.)

So suppose that $\alpha > 0$ and $\beta > 0$. Use Sylow's theorem stated above to get a subgroup Q of order q^β. Note first that if G is abelian then Q is normal and nontrivial, so G is not simple.

By exercise sheet 7, exercise 6 (i), $Z(Q) \neq \{\mathbf{1}\}$, so let $g \in Z(Q)$ such that $g \neq \mathbf{1}$. We then have

$$qgq^{-1} = g$$

for all $q \in Q$, which implies that $Q < C_G(g)$, and therefore $q^\beta = |Q|$ divides $|C_G(g)|$.

Thus, $|C_G(g)| = p^r q^\beta$ for some nonnegative r and therefore $|g^G| = |G|/|C_G(g)| = p^{\alpha - r}$.

- If $\alpha - r \geq 1$ then we can apply Theorem 5.7 to conclude that G is not simple.
- If $\alpha - r = 0$ then $|g^G| = 1$ which implies that $\mathbf{1} \neq g \in Z(G)$ and so either G abelian or $Z(G)$ is a nontrivial normal subgroup. In either case, G is not simple.

∎