Introduction to Representation Theory - Week 8 - Algebraic Integers and Burnside's Theorem

Antonio León Villares

November 2023

Contents

Based on the notes by Konstantin Ardakov, Section 7

1 Algebraic Integers

1.1 Definition: Algebraic Numbers and Algebraic Integers

Let $z \in \mathbb{C}$. Then:

1. *z is an **algebraic number** if:*

$$\exists f \in \mathbb{Q}[t] \ : \ f(z) = 0$$

   *The set of all **algebraic numbers** is $\overline{\mathbb{Q}}$.*

2. *z is an **algebraic integer** if:*

$$\exists f \in \mathbb{Z}[t] \ : \ f(z) = 0$$

   *and f is **monic** (its **leading coefficient** is 1).*
   *The set of all **algebraic integers** is $\mathbb{A}$*

(Definition 7.1)

1.1.1 Examples: Algebraic Integers

- every **integer** $a \in \mathbb{Z}$ is an **algebraic integer**, as it satisfies $t - a = 0$
- every n**th root of unity** ω is an **algebraic integer**, as it satisfies $t^n - 1 = 0$
- if $z \in \mathbb{C}$ is an **algebraic number**, there exists some $m \in \mathbb{Z}$ such that mz is an **algebraic integer**. In particular, suppose that:

$$\sum_{i=1}^{d} \alpha_i z^i = 0$$

  Then, if:

$$\alpha_i = \frac{a_i}{b_i}$$

  (where $a_i, b_i \in \mathbb{Z}$ are **coprime**), then if we let:

$$m = \text{lcm}(b_1, \ldots, b_d)$$

  we have that:

$$0 = m^{d+1} \sum_{i=0}^{d} \alpha_i z^i = \sum_{i=1}^{d} \alpha_i m^{d-i} (mz)^i$$

  and:

$$\alpha_i m^{d-i} \in \mathbb{Z}$$

  since $\forall i \in [0, d]$ b_i will divide m^{d-i}

- we have that:

$$\alpha \in \mathbb{Z} \iff \alpha \in \mathbb{Q} \text{ is an } \textbf{algebraic integer}$$

In other words:

$$\mathbb{Q} \cap \mathbb{A} = \mathbb{Z}$$

If $\alpha \in \mathbb{Z}$, then it is trivially a rational algebraic integer. On the other hand, if α is a rational algebraic integer, there exist **coprime** $r, s \in \mathbb{Z}$ such that:

$$\alpha = \frac{r}{s} \in \mathbb{Q}$$

and:

$$\exists a_i \in \mathbb{Z} \ : \ 0 = \sum_{i=0}^{n} a_i \left(\frac{r}{s}\right)^i \implies -r^n = \sum_{i=0}^{n-1} a_i r^i s^{n-i}$$

Since s divides the LHS, it must divide the RHS; but r, s being coprime implies that $s = \pm 1$ (since their only common divisor will be 1), so $\alpha = r/s = r \in \mathbb{Z}$

1.2 Algebraic Integers as a Ring

1.2.1 Proposition: Preserving Subgroups Leads to Algebraic Integers

*Let M be a **finitely generated subgroup** of $(\mathbb{C}, +)$. Then:*

$$\{z \in \mathbb{C} \mid zM \subseteq M\} \subset \mathbb{A}$$

(Proposition 7.4)

Proof. Let $z \in \mathbb{C}$ be such that for any finitely generated additive subgroup of $\mathbb{C}$ M we have that:

$$zM \subseteq M$$

Let

$$V = \{v_1, \ldots, v_d\}$$

be a generating set for M. Then, since $zM \subseteq M$, we have that:

$$\forall v_i \in V, \exists u_{ij} \in \mathbb{Z} \ : \ zv_i = \sum_{j=1}^{d} u_{ij} v_j$$

(without loss of generality we can always assume that the v_i have been picked so that the u_{ij} are integers).

Now, we can define a matrix $d \times d$ matrix in the integers, whose i, jth entry is:

$$U_{ij} = u_{ij}$$

Then, the equation above can be written in matrix form if we define:

$$\underline{v} = \begin{pmatrix} v_1 \\ \vdots \\ v_d \end{pmatrix} \in \mathbb{Z}^d$$

such that:

$$U\underline{v} = z\underline{v}$$

This then tells us that z is in fact an eigenvalue of U. Define $g(t)$ to be the characteristic polynomial U:

$$g(t) = \det(tI - U)$$

Now, the characteristic polynomial is monic, and since the u_{ij} are integers, g will have integer coefficients. By definition, the eigenvalues of U will be roots of g, so in particular:

$$g(z) = 0$$

which implies that z is an algebraic integer, as required.

□

1.2.2 Theorem: Algebraic Integers are a Subring of $\mathbb{C}$

*The **algebraic integers** $\mathbb{A}$ form a **subring** of $\mathbb{C}$.*
(Theorem 7.3)

Proof. Let $\alpha, \beta \in \mathbb{A}$. To show that $\mathbb{A}$ is a subring of $\mathbb{C}$ we must show it is closed under addition and multiplication:

$$\alpha + \beta \in \mathbb{A} \qquad \alpha\beta \in \mathbb{A}$$

Since α, β are algebraic integers, there exist integers

$$\{a_i\}_{i\in[0,m-1]} \qquad \{b_i\}_{i\in[0,n-1]}$$

such that:

$$\sum_{i=0}^{m-1} a_i\alpha^i = 0 = \sum_{i=0}^{n-1} b_i\beta^i$$

Now, let M be the additive subgroup of $\mathbb{C}$ generated by the set:

$$\{\alpha^i\beta^j \mid i \in [0, m-1], j \in [0, n-1]\}$$

In particular, M contains words/polynomials in the variables α, β (as by definition it is a subring of $\mathbb{C}$ too), so:

$$\alpha + \beta \in M \qquad \alpha\beta \in M$$

Thus

$$(\alpha + \beta)M \subseteq M \qquad (\alpha\beta)M \subseteq M$$

so by Proposition 7.4 above:

$$\alpha + \beta \in \mathbb{A} \qquad \alpha\beta \in \mathbb{A}$$

□

1.3 Algebraic Integers and Character Theory

1.3.1 Lemma: Characters are Algebraic Integers

*Let χ be a **character** of the **finite group** G. Then:*

$$\forall g \in G, \qquad \chi(g) \in \mathbb{A}$$

(Lemma 7.5)

Proof. Since $\chi(g)$ is the trace of the morphism $\rho(g)$, it is a sum of eigenvalues of $\rho(g)$. Now, since G is a finite group:

$$\exists k \in \mathbb{N} \ : \ g^k = e_G \implies (\rho(g))^k = I$$

Thus, if λ is an eigenvalue:

$$(\rho(g))v = \lambda v \implies v = Iv = (\rho(g))^k v = \lambda^k v$$

so $\lambda^k = 1$, and thus, each λ is a root of unity.

In other words, $\chi(g)$ is a sum of roots of unity. But each root of unity is an algebraic integer, and since these form a subring of $\mathbb{C}$ (Theorem 7.3 above), it follows that $\chi(g)$ is an algebraic integer.

□

1.3.2 Lemma: Subring of Group Ring Centre from Conjugacy Class Sums

Recall the definition of conjugacy class sums

*Let G be a **finite group** with **conjugacy classes**:*

$$C_1, \ldots, C_2$$

*Define the **conjugacy class sum** of C_i via:*

$$\widehat{C_i} = \sum_{x \in C_i} x \in kG$$

*That is, $\widehat{C_i}$ is the **formal sum** in kG containing all elements of the conjugacy class C_i.*
(Proposition 3.15)

Let:

- *G be a **finite group***
- *$C_1, \ldots, C_r$ be **conjugacy classes** in G*

*Let S be the **additive subgroup** of $\mathbb{C}G$ generated by the **conjugacy class sums**:*

$$S = \left\langle \widehat{C_1}, \ldots, .\widehat{C_r} \right\rangle_{\mathbb{C}G}$$

*Then, S is a **subring** of the **centre** $Z(\mathbb{C}G)$.*
(Lemma 7.6)

Proof. To show that S is a subring, it is sufficient to show that the generators $\widehat{C_i}$ satisfy:

$$\forall i, j, \qquad \widehat{C_i} + \widehat{C_j} \in S \qquad \widehat{C_i}\widehat{C_j} \in S$$

Firstly, note that by:

*Let G be a **finite group** with **conjugacy classes**:*

$$C_1, \ldots, C_2$$

Then,

$$\{\widehat{C_1}, \ldots, \widehat{C_2}\}$$

*is a **basis** for $Z(kG)$ as a **vector space**, and thus:*

$$\dim(Z(kG)) = s(G)$$

(Proposition 3.15)

so in particular each $\widehat{C_i}$ is central in $\mathbb{C}G$.

By definition of S (as an additive subgroup), we must ahve that

$$\widehat{C_i} + \widehat{C_j} \in S$$

For the second condition, we can write:

$$\widehat{C_i}\widehat{C_j} = \left(\sum_{x \in C_i} x\right)\left(\sum_{y \in C_j} y\right) = \sum_{i=1}^{r} \sum_{z \in C_k} a_{ijk}(z) z$$

where we've used the fact that conjugacy classes partition G, so in particular:

$$\forall z = xy \in G, \qquad \exists C_k \ : \ z \in C_k$$

What are the coefficients $a_{ijk}(z)$? They count the number of ways in which z can be made as a product of $x \in C_i, y \in C_j$. In other words:

$$a_{ijk}(z) = |\{(x,y) \in C_i \times C_j \mid xy = z\}|$$

But notice, these a_{ijk} are invariant under conjugation:

$$\forall g \in G, \qquad a_{ijk}(g^{-1}zg) = |\{(x,y) \in C_i \times C_j \mid xy = gzg^{-1}\}|$$

since for each (x,y) such that $xy = z$ we have that:

$$(g^{-1}xg)(g^{-1}yz) = g^{-1}xyg = g^{-1}zg$$

and $(g^{-1}xg, g^{-1}yz) \in C_i \times C_j$. Thus:

$$\forall z \in C_k, \qquad a_{ijk}(z) = a_{ijk}(g^{-1}zg)$$

so in particular the a_{ijk} don't depend on the choice of representative, so:

$$\widehat{C_i}\widehat{C_j} = \sum_{i=1}^{r} a_{ijk} \sum_{z \in C_k} z = \sum_{k=1}^{a} a_{ijk}\widehat{C_k} \in S$$

□

1.3.3 Theorem: Conjugacy Class Sums Act Through Algebraic Integers

Let

- G *be a* ***finite group***
- V *be a* ***simple*** $\mathbb{C}G$***-module***

Then, for any $g \in G$*:*

1. *The* ***conjugacy class sum*** $\widehat{g^G}$ *acts on* V *by a* ***scalar****:*

$$\forall v \in V, \qquad \widehat{g^G} \cdot v = \frac{|g^G|\chi_V(g)}{\chi_V(1)} \cdot V$$

where

$$\frac{|g^G|\chi_V(g)}{\chi_V(1)} \in \mathbb{C}$$

2. *The scalar is an* ***algebraic integer***

$$\frac{|g^G|\chi_V(g)}{\chi_V(1)} \in \mathbb{A}$$

(Theorem 7.7)

Proof.

(1)

Recall Schur's Lemma:

> *Suppose k is **algebraically closed**. Let V be a **simple module** over a **finite dimensional** k**-algebra** A.*
> *Then, every A**-module endomorphism** of V is given by the action of some **scalar** $\lambda \in K$, such that:*
>
> $$\mathrm{End}_A(V) = k1_V$$
>
> *(Theorem 3.6)*

Schur's Lemma applies, since by assumption V is simple. Moreover, recall that central elements induce an endomorphism action:

> *Take any $z \in Z(A)$, and define an **endomorphism**:*
>
> $$z_V : V \to V$$
>
> *via:*
>
> $$v \mapsto z \cdot v$$
>
> *We can check that z_V is indeed an **endomorphism**:*
>
> $$\begin{aligned} z_V(a \cdot v) &= z \cdot (a \cdot v) \\ &= (za) \cdot v \\ &= (az) \cdot v \\ &= a \cdot z_V(v) \end{aligned}$$

Hence, since conjugacy class sums are central in $\mathbb{C}G$, it follows that $z = \widehat{g^G}$ acts by a scalar $z_V \in \mathbb{C}$ on every simple $\mathbb{C}G$-module. Thus, we have that:

$$\widehat{g^G} \cdot v = z_V v \implies \sum_{x \in g^G} x \cdot v = z_V v$$

Now, taking the trace of both sides:

$$\mathrm{tr}\left(\sum_{x \in g^G} x \cdot v\right) = \sum_{x \in g^G} \chi_V(x) = |g^G| \chi_V(g)$$

since χ_V is a class function. Similarly:

$$\mathrm{tr}(z_V v) = z_V \dim(V)$$

since the matrix corresponding to a scalar z_V is a diagonal matrix with $\dim(V)$ rows. Hence:

$$|g^G| \chi_V(g) = z_V \dim(V)$$

Using the fact that:

$$\chi_V(1) = \dim(V)$$

we obtain the desired result.

(2)

Let

$$\rho : G \to GL(V)$$

be the representation of G afforded by V. We can extend ρ to a $\mathbb{C}$-algebra homomorphism:

$$\tilde{\rho} : \mathbb{C}G \to \mathrm{End}(V)$$

by defining:

$$\sum_{g \in G} a_g g \overset{\tilde{\rho}}{\mapsto} \sum_{g \in G} a_g \rho(g)$$

If we restrict $\tilde{\rho}$ to the centre $Z(\mathbb{C}G)$, then each $\tilde{\rho}(g)$ corresponds to a scalar in $\mathbb{C}$; this defines a homomorphism:

$$Z(\mathbb{C}G) \to \mathbb{C}$$

which is nothing but the central character of V:

*Let A be a k-**algebra**, and V be an A-**module** where:*

$$\mathrm{End}_A(V) = k1_V$$

*By **Schur's Lemma**, every $z \in Z(A)$ acts on V by **scalar multiplication**. Denote this action/endomorphism via z_V.*

---

*The **central character** of V is the **ring homomorphism**:*

$$\begin{aligned} Z(A) &\to k \\ z &\mapsto z_V \end{aligned}$$

In particular, it thus follows that:

$$\tilde{\rho}(Z(\mathbb{C}G)) \subseteq \mathbb{C}$$

Using Lemma 7.6:

Let:

- *G be a **finite group***
- *$C_1, \ldots, C_r$ be **conjugacy classes** in G*

*Let S be the **additive subgroup** of $\mathbb{C}G$ generated by the **conjugacy class sums**:*

$$S = \left\langle \widehat{C_1}, \ldots, .\widehat{C_r} \right\rangle_{\mathbb{C}G}$$

*Then, S is a **subring** of the **centre** $Z(\mathbb{C}G)$.*
(Lemma 7.6)

since S is a subring of $Z(\mathbb{C}G)$, we must have that:

$$\tilde{\rho}(S) \leq \mathbb{C}$$

is a subring of $\mathbb{C}$, since $\tilde{\rho}$ is a ring homomorphism. In particular:

$$z_V \cdot \tilde{\rho}(S) \subseteq \tilde{\rho}(S)$$

since $z_V \in \tilde{\rho}(S)$. Thus, by Proposition 7.4

> *Let M be a **finitely generated subgroup** of $(\mathbb{C}, +)$. Then:*
>
> $$\{z \in \mathbb{C} \mid zM \subseteq M\} \subset \mathbb{A}$$
>
> *(Proposition 7.4)*

z_V is an algebraic integer, as required.

□

1.3.4 Corollary: Dimension of Group Ring Module Divides Group Order

> *If V is a **simple** $\mathbb{C}G$**-module**, then $\dim(V)$ **divides** $|G|$.*
> *(Corollary 7.8)*

Proof. By row orthogonality of the character table, we have that:

$$\langle \chi_V, \chi_V \rangle = 1$$

Define a complete set of representatives for the conjugacy classes of G to be:

$$g_1, \ldots, g_r$$

Then, we have that:

$$\begin{aligned} 1 &= \langle \chi_V, \chi_V \rangle \\ &= \frac{1}{|G|} \sum_{g \in G} \overline{\chi_V(g)} \chi_V(g) \\ &= \frac{1}{|G|} \sum_{i=1}^{r} |g_i^G| \chi_V(g_i^{-1}) \chi_V(g_i) \\ \implies \frac{|G|}{\chi_V(1)} &= \sum_{i=1}^{r} \chi_V(g_i^{-1}) \frac{|g_i^G| \chi_V(g_i)}{\chi_V(1)} \end{aligned}$$

Here we've used the fact that:

$$\chi_V(g^{-1}) = \overline{\chi_V(g)}$$

*This follows from the fact that if ρ is the representation afforded by V, then the **eigenvalues** of $\rho(g^{-1})$ are the inverses of the **eigenvalues** of $\rho(g)$. In particular, if $\rho(g)$ has **eigenvalues** λ_i, then using the fact that these eigenvalues are roots of unity:*

$$\chi_V(g^{-1}) = \mathrm{tr}(\rho(g^{-1})) = \sum \frac{1}{\lambda_i} = \sum \overline{\lambda_i} = \overline{\chi_V(g)}$$

Now, note that for any $i \in [1, r]$:

- $\chi_V(g_i^{-1}) \in \mathbb{A}$, since characters are roots of unity, and roots of unity are algebraic integers
- $\frac{|g_i^G|\chi_V(g_i)}{\chi_V(1)} \in \mathbb{A}$, by Theorem 7.7, part 2

Since $\mathbb{A}$ is a ring (Theorem 7.3), it is closed under addition and multiplication, which in particular implies that:

$$\frac{|G|}{\chi_V(1)} = \frac{|G|}{\dim(V)} \in \mathbb{A}$$

This is a rational number, and since $\mathbb{Q} \cap \mathbb{A} = \mathbb{Z}$, in particular:

$$\frac{|G|}{\dim(V)} \in \mathbb{Z}$$

so as required $\dim(V)$ must divide $|G|$.

□

2 Burnside's Theorem

2.1 Sylow's Theorems

2.1.1 Definition: Sylow p-Subgroup

*Let G be a **finite** group, and let p be a **prime** such that:*

$$|G| = p^\alpha m$$

where $p \nmid m$.
*A **Sylow p-subgroup** of G is a **subgroup** $P \leq G$ such that:*

$$|P| = p^\alpha$$

(Definition 7.10)

2.1.2 Theorem: Sylow Theorems

*Let G be a **finite group**, and let p be a **prime** such that:*

$$|G| = p^\alpha m$$

where $p \nmid m$.

Then:

1. *G contains **at least** one **Sylow p-subgroup***
2. *If P_1, P_2 are **Sylow p-subgroups** of G:*

$$\forall g \in G, \qquad gP_1g^{-1} = P_2$$

3. *Let n_p be the number of **Sylow p-subgroups** of G. Then:*

   (a)

$$n_p \equiv 1 \pmod{p}$$

   (b)

$$n_p \mid m = \frac{|G|}{p^\alpha}$$

2.2 Towards Burnside's Theorem

2.2.1 Lemma: Order of Conjugacy Classes from Central Sylow Subgroup Elements

*Let G be a **finite group** such that:*

$$|G| = p^\alpha q^\beta$$

where:

- *p, q are **distinct primes***
- *$\alpha, \beta \geq 1$*

*If $P \leq G$ is a **Sylow p-subgroup**, and $g \in Z(P)$, then:*

$$\exists m \in \mathbb{N} \ : \ |g^G| = q^m$$

(Lemma 7.12)

Proof. Since $g \in Z(P)$, in particular the centraliser (set of all elements of G which commute with g) must contain P as a subgroup:

$$P \leq C_G(g)$$

In particular, by Lagrange's Theorem, it follows that $|P|$ divides $|C_G(g)|$:

$$|C_G(g)/P| = \frac{|C_G(g)|}{|P|}$$

Moreover, by the Orbit-Stabilizer Theorem, we know that:

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

Lastly, again by Lagrange's Theorem:

$$|G/P| = \frac{|G|}{|P|} = q^\beta$$

In particular:

$$\frac{|G/P|}{|G/C_G(g)|} = \frac{q^\beta}{|g^G|} = \frac{|C_G(g)||G|}{|G||P|} = \frac{|C_G(g)|}{|P|} \in \mathbb{N}$$

In particular, this implies that $|g^G|$ divides q^β, and since q is prime, this is true if and only if $|g^G|$ is itself a power of q.

□

2.2.2 Lemma: Algebraic Integer from Roots of Unity

This makes me so happy: we get to combine Representation Theory with Galois Theory. As a recap, consider my notes on Galois Theory.

Let

$$\xi_1, \ldots, \xi_n$$

be ***roots of unity****, and define:*

$$\alpha = \frac{\xi_1 + \ldots + \xi_n}{n}$$

Now, suppose that α is an ***algebraic integer*** *($\alpha \in \mathbb{A}$). Then either:*

$$\alpha = 0 \qquad or \qquad \alpha = \xi_1 = \ldots = \xi_n$$

(Lemma 7.14)

Proof. Without loss of generality, we may assume that there exists some primitive kth root of unity ω, such that:

$$\forall i \in [1, n], \qquad \xi_i \in \mathbb{Q}(\omega)$$

Let:

$$\mathcal{G} = \mathrm{Gal}(\mathbb{Q}(\omega) : \mathbb{Q})$$

Define the *norm* of α as the value:

$$a = \prod_{\sigma \in \mathcal{G}} \sigma(\alpha)$$

By definition of the Galois Group, any $\sigma \in \mathcal{G}$ will permute the roots of unity, so:

$$\forall j \in [1, n], \sigma \in \mathcal{G} \qquad |\sigma(\xi_j)| = 1$$

Moreover, as an automorphism over $\mathbb{Q}$:

$$|\sigma(\alpha)| = \frac{1}{n} \left| \sum_{j=1}^{n} \sigma(\xi_j) \right| \leq \frac{1}{n} \sum_{j=1}^{n} |\sigma(\xi_j)| = 1$$

by the Triangle Inequality. Hence:

$$|a| = \prod_{\sigma \in \mathcal{G}} |\sigma(\alpha)| \leq 1$$

On the other hand, again by definition of the Galois Group as a an automorphism, any action of $\mathcal{G}$ on a fixes a (since applying autmorphisms repeatedly sends each ξ_j to a distinct root, and the norm is symmetric with respect to these roots). But then:

$$a \in Fix(\mathcal{G}) \iff a \in \mathbb{Q}$$

by definition of the fixed set.

By hypothesis, $\alpha \in \mathbb{A}$, so $\sigma(\alpha) \in \mathbb{A}$ for any $\sigma \in \mathcal{G}$ and since algebraic integers form a ring (Theorem 7.3), i t follows that $a \in \mathbb{A}$ too. This then forces:

$$a \in \mathbb{Z}$$

Alongside the restriction $|a| \leq 1$, this implies that:

$$a \in \{-1, 0, 1\}$$

If $a = 0$, then at least one of the $\sigma(\alpha)$ is 0; but σ is an automorphism over $\mathbb{Q}$, which forces $\alpha = 0$.

Otherwise, $|a| = 1$, which forces:

$$\left| \sum_{j=1}^{n} \sigma(\xi_j) \right| = n \iff \left| \sum_{j=1}^{n} \xi_j \right| = n$$

Now, we proceed by induction. If $n = 1$, the result is clear. Assume that for $n = k$, we have:

$$\left| \sum_{j=1}^{k} \xi_j \right| = k$$

implies that all the ξ_j are equal. Now consider $k + 1$ roots of unity such that:

$$\left| \sum_{j=1}^{k+1} \xi_j \right| = k + 1$$

Then:

$$|k + \xi_{k+1}| = k + 1$$

By the Triangle Inequality:

$$|k\xi_1 + \xi_{k+1}| \leq k + 1$$

Thus, if $\xi_{k+1} \neq \xi_1$, we must have:

$$|k\xi_1 + \xi_{k+1}| < k + 1$$

which contradicts the initial assumption. Thus, $\xi_{k+1} = \xi_1$, and all the roots of unity are equal. In other words:

$$|a| = 1 \implies \alpha = \xi_1 = \ldots = \xi_n$$

□

2.2.3 Theorem: Simple Groups from Conjugacy Class Size

> *Let G be a **finite group**. Suppose that $g \in G$ is a **non-central** group element, such that $|g^G|$ is **not a prime power**. Then, G is **not simple** (if has a **non-trivial** normal subgroup).*
> *That is, if for any non-central $g \in G$ we have that $|g^G|$ is a **prime power**, then G contains a **non-trivial** normal subgroup.*
> *(Theorem 7.13)*

Proof. Let G have r conjugacy classes, and let

$$\mathbb{1}, \rho_2, \ldots, \rho_r$$

be the irreducible ($\mathbb{C}$-linear) representations of G (i.e the simple $\mathbb{C}G$ modules).

Assume that the Theorem is false, and that for some non-central element g with $|g^G|$ a prime power, G is simple. Then, since the kernel of a representation is always a normal subgroup, we must have that:

$$\ker(\rho_i) = \{e_G\} \qquad or \qquad \ker(\rho_i) = G$$

But since these are all irreducible, non-isomorphic representations, and $\mathbb{1}$ is the unique representation with kernel G, it must be the case that:

$$\forall i \in [2, r], \qquad \ker(\rho_i) = \{e_G\}$$

In particular, each representation ρ_i is injective, so by the First Isomorphism Theorem (or simple logic):

$$G/\ker(\rho_i) \cong \text{im}(\rho_i) \implies G \cong \rho_i(G)$$

Moreover, the image of a representation is a subgroup:

$$\rho_i(G) \leq \text{GL}_{n_i}(\mathbb{C})$$

Now, $\text{GL}_{n_i}(\mathbb{C})$ is not simple: it has a non-trivial centre C, given by the diagonal matrices with entries in $\mathbb{C}^\times$. In particular, this implies that:

$$\rho_i(G) \cap C$$

is a central subgroup of $\rho_i(G)$. But then, since $\rho_i(G) \cong G$, and G is simple, this forces:

$$\rho_i(G) \cap C = \{\rho_i(e_G)\}$$

so it must be trivial (since clearly $\rho_i(G) \cap C \neq \rho_i(G)$, as otherwise we'd have that G is a central subgroup of itself, and thus, G is abelian, which contradicts the fact that G is simple).

Hence, the proof reduces to finding some $g_j \in G$ such that $\rho_i(g_j)$ acts a scalar multiple of the identity:

$$\rho_i(g_j)(g_j) = \alpha I, \qquad \alpha \in \mathbb{C}^\times$$

as this then implies a contradiction of the fact that

$$\rho_i(G) \cap C = \{\rho_i(e_G)\}$$

Now, consider the non-central element g, such that $|g|^G$ is some power of a prime q. Using column orthogonality:

*Let G be a **finite group**, and let*

$$\chi_1, \ldots, \chi_R$$

*be **irreducible characters** of G.*

If $g, h \in G$, then:

$$\sum_{i=1}^{R} \overline{\chi_i(g)}\chi_i(h) = \begin{cases} |C_G(g)|, & g^G = h^G \\ 0, & otherwise \end{cases}$$

---

*In other words, taking the **dot product** of **columns** in the **character table** will always be 0.*
(Theorem 5.23)

with the first column and the column associated to g^G (and letting χ_i be the character associated to representation ρ_i):

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

Now, does q divide all of the $\chi_i(1)$? If it did, then:

$$-\frac{1}{q} = \sum_{i=2}^{r} \left(\frac{\chi_i(1)}{q}\right) \chi_i(g)$$

Under the assumption that q divides each $\chi_i(1)$, the RHS is a linear combination of algebraic integers, so it must be an algebraic integer. But since $q \geq 2$, $-\frac{1}{q} \notin \mathbb{A}$ (the only rational algebraic integers are the integers themselves). This implies that:

- $$\exists i \in [2, r] \ : \ q \not| \chi_i(1)$$
- for said i, $\chi_i(g) \neq 0$ (since otherwise whether q divides $\chi_i(1)$ or not wouldn't matter)

Finally, we bring it all together. Let:

$$|g^G| = q^\beta, \qquad \beta > 0$$

Since $q \not| \chi_i(1)$, in particular:

$$\gcd(|g^G|, \chi_i(1)) = 1$$

since only q divides $|g^G|$. Hence, by Bezout's Lemma:

$$\exists a, b \in \mathbb{Z} \ : \ a\chi_i(i) + b|g^G| = 1$$

This implies that:

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

The LHS is again a linear combination of algebraic integers (using Theorem 7.7, part 2 and Lemma 7.5), and since algebraic integers form a ring, this implies that:

$$\frac{\chi_i(g)}{\chi_i(1)} \in \mathbb{A}$$

Now, $\chi_i(1)$ gives the dimension n_i of the $\mathbb{C}G$-module represented by ρ_i. Moreover, $\chi_i(g)$ is a sum of n_i eigenvalues of $\rho_i(g)$, and these eigenvalues are all roots of unity, say ξ_j^i. Since by assumption $\chi_i(g) \neq 0$, we thus have that:

$$\frac{1}{n_i}\sum_{j=1}^{n_i} \xi_j^i \neq 0$$

Hence, using

> *Let*
>
> $$\xi_1, \ldots, \xi_n$$
>
> *be* ***roots of unity****, and define:*
>
> $$\alpha = \frac{\xi_1 + \ldots + \xi_n}{n}$$
>
> *Now, suppose that α is an* ***algebraic integer*** *($\alpha \in \mathbb{A}$). Then either:*
>
> $$\alpha = 0 \qquad or \qquad \alpha = \xi_1 = \ldots = \xi_n$$
>
> *(Lemma 7.14)*

it follows that each of the eigenvalues of ρ_i are all the same, say χ. In particular, this then means that:

$$\rho_i(g) = \xi I$$

But this contradicts the fact that:

$$\rho_i(G) \cap C = \{\rho_i(e_G)\}$$

since $\xi I \in C$ is clearly a central element. Hence, it follows by contradiction that if g is a non-central element of G, with $|g^G| = q^\beta$ for some prime p, that G can't be simple, as required.

□

2.2.4 Theorem: Burnside's Theorem

*Let G be a **finite, non-abelian group** of order $p^\alpha q^\beta$, where p, q are **primes**. Then, G is **not simple**.*
(Theorem 7.9)

We may assume that $\alpha, \beta \geq 1$.
*Otherwise, $|G| = p^n$ implies that G has a **non-trivial centre**, by the previous Group Theory course.*
*If $|G|$ is **prime**, then it will be **cyclic**, and so, **abelian** so Burnside's Theorem doesn't apply to them).*

Proof. ---

By Sylow I, G has a Sylow p-subgroup, call it P. Since $\alpha \geq a$, P is a non-trivial p-group, so it has a non-trivial centre, $Z(P)$ (again, by this theorem). Hence, we can always find a non-trivial central element $g \in Z(P)$.

If $g \in Z(G)$ aswell, then $\langle g \rangle$ defines a non-trivial, proper normal subgroup of G, in which case we are done.

Otherwise, g isn't central in G, in which case by

*Let G be a **finite group** such that:*

$$|G| = p^\alpha q^\beta$$

where:

- *p, q are **distinct primes***
- *$\alpha, \beta \geq 1$*

*If $P \leq G$ is a **Sylow p-subgroup**, and $g \in Z(P)$, then:*

$$\exists m \in \mathbb{N} \ : \ |g^G| = q^m$$

(Lemma 7.12)

we have that $|g^G|$ is a prime power, which by:

*Let G be a **finite group**. Suppose that $g \in G$ is a **non-central** group element, such that $|g^G|$ is **not a prime power**. Then, G is **not simple** (if has a **non-trivial** normal subgroup).*
*That is, if for any non-central $g \in G$ we have that $|g^G|$ is a **prime power**, then G contains a **non-trivial** normal subgroup.*
(Theorem 7.13)

implies that G isn't simple.

□