Week 6

Abstract Representation Theory

6.1 The Center of the Group Algebra

10/30:

- Plan for this week.
  - Today: Briefly discuss a very important concept called the **center**.
  - Wednesday: Do algebraic numbers.
  - Friday: Burnside's theorem.
- **Center** (of a group): The set of all elements of a group G that commute with every other element in G. *Denoted by* $\boldsymbol{Z(G)}$. *Given by*

$$Z(G) = \{g \in G \mid xgx^{-1} = g \ \forall \ x \in G\}$$

  - Note: $Z(G)$ is a subgroup of G.
- The center is one of the most important concepts in all of representation theory.
  - Example: Let A be an abelian group, such as $Z(G)$. Then all its irreps are 1D.
    - See Section 1.3 of Fulton and Harris (2004) for an explanation.
  - Normally, the center of a group is too small to be interesting.
    - However, $Z(\mathbb{C}[G])$ *is* large enough to be interesting.
- **Center** (of an algebra): The set of all elements of an algebra A that commute with every other element in A. *Denoted by* $\boldsymbol{Z(A)}$. *Given by*

$$Z(A) = \{a \in A \mid xa = ax \ \forall \ x \in A\}$$

- Proposition: If A is an algebra over $\mathbb{C}$, M is an irreducible left A-module, and $\rho : A \to \mathrm{End}(M)$ is a corresponding representation, then $x \in Z(A)$ implies that $\rho(x) = \lambda I$, i.e., $\rho(x)$ is a *scalar matrix*.

  Proof. Let $x \in Z(A)$ be arbitrary. Then for all $a \in A$, we know that $\rho(x)\rho(a) = \rho(a)\rho(x)$. Thus, $\rho(x)$ is a morphism of A-modules. Consequently, since M is irreducible (also known as *simple*), Schur's Lemma for associative algebras implies that $\mathrm{Hom}_A(M, M)$ is a division algebra over $\mathbb{C}$. But since $\mathbb{C}$ is the only division algebra over $\mathbb{C}$, we have that $\mathrm{Hom}_A(M, M) \cong \mathbb{C}$. From here, it readily follows that $\rho(x)$ is equal to some λI. $\square$

- Consequence: If M is reducible, we can reduce it into component scalar representations.
- Consequence: If G is an abelian group, then every irrep V is 1-dimensional.

- Additionally, $\mathbb{C}[G]$ is commutative and hence $\mathbb{C}[G] = Z(\mathbb{C}[G])$.
- Then if V is an arbitrary representation, V is equal to the direct sum of one dimensional irreducible representations for all g. Hence, $\rho_V(g) = \lambda I$. Could the λ's not be different for the various irreps??

- We now try to compute $Z(\mathbb{C}[G])$.
  - Facts:

$$Z(A_1 \oplus A_2) = Z(A_1) \oplus Z(A_2) \qquad\qquad Z(M_n(\mathbb{C})) = \text{span}(I) \cong \mathbb{C}$$

  - These facts coupled with the fact that G is a finite group (hence $\mathbb{C}[G] \cong M_{n_1}(\mathbb{C}) \oplus \cdots \oplus M_{n_k}(\mathbb{C})$ where k is the number of conjugacy classes in G by the example from last Wednesday's class) yield

$$\begin{aligned}
Z(\mathbb{C}[G]) &\cong Z(M_{n_1}(\mathbb{C}) \oplus \cdots \oplus M_{n_k}(\mathbb{C})) \\
&\cong \underbrace{\mathbb{C} \oplus \cdots \oplus \mathbb{C}}_{k \text{ times}} \\
&= \mathbb{C}^k
\end{aligned}$$

- Let $C_1, \dots, C_k$ be conjugacy classes in G. Then we may define

$$e_i = \sum_{g \in C_i} g$$

  for each $i = 1, \dots, k$.
  - Example: In S_3 the three e_i's are $\{e, (12) + (13) + (23), (123) + (132)\}$.
- Claim: $Z(G) = \langle e_1, \dots, e_k \rangle$, that is, the e_i commute with every element of G expressed as $1g \in \mathbb{C}[G]$.

Proof. We will use a bidirectional inclusion proof.
$\underline{\langle e_1, \dots, e_k \rangle \subset Z(G)}$: Let e_i and $x \in G$ be arbitrary. Then

$$\begin{aligned}
xe_ix^{-1} &= \sum_{g \in C_i} xgx^{-1} = \sum_{h \in C_i} h = e_i \\
xe_i &= e_ix
\end{aligned}$$

This naturally extends to any sums and scalar multiples of the e_i's.
$\underline{Z(G) \subset \langle e_1, \dots, e_k \rangle}$: Let $a \in Z(G)$ be arbitrary. As an element of $\mathbb{C}[G]$, we know that $a = \sum a_g g$ for some $a_g \in \mathbb{C}$. Additionally, since $a \in Z(G)$, we have that $xax^{-1} = a$ for all $x \in G$ (that is, $1x \in A$). Combining these last two results, we have that

$$\sum_{g \in G} a_{x^{-1}gx} g = \sum_{g \in G} a_g xgx^{-1} = xax^{-1} = a = \sum_{g \in G} a_g g$$

Comparing like terms in the above equality, we can learn that for all $x \in G$, we have $a_{x^{-1}gx} = a_g$. In other words, all of the a_g's for g's in the same conjugacy class are equal. Therefore, a is of the form $a = \sum_{i=1}^k a_{g_i} e_i$ for $g_i \in C_i$. □

- Thus we get $a_e e + a_{(12)}(12) + a_{(13)}(13) + \cdots$??
- Computing products of the e_i: What if we want to compute $[(12) + (13) + (23)]^2$, for example? We have to multiply *noncommutatively*, so HS formulas are out, but we can still do all nine multiplications and sum them:

$$[(12) + (13) + (23)]^2 = 3e + 3[(123) + (132)]$$

- We now tie this claim back into our discussion of $Z(\mathbb{C}[G])$.
  - $Z(\mathbb{C}[G])$ has basis $e_1, \dots, e_k$[1].
  - Recall that $Z(\mathbb{C}[G]) = \mathbb{C} \oplus \cdots \oplus \mathbb{C}$, with characters $\chi_1, \dots, \chi_k$.
  - Then $f_{\chi_i} = (0, \dots, 0, 1, 0, \dots, 0)$, where the 1 lies in the i^{th} slot.
  - Then we get $f_{\chi_1}, \dots, f_{\chi_k}$ as a basis.
  - It follows that $f_{\chi_i}^2 = f_{\chi_i}$ and $f_{\chi_i} f_{\chi_j} = 0$ for $i \neq j$; this is exactly what it means for a space to be $\mathbb{C} \oplus \cdots \oplus \mathbb{C}$.
  - Both of these spaces (center elements and class functions) have these two interconnected bases, so the spaces are quite similar!
- The center of a group algebra $Z(\mathbb{C}[G])$ can be identified "=" with the space of class functions $\mathbb{C}_{\text{cl}}(G)$ via
$$\sum \varphi(g)g \mapsto [g \to \varphi(g)]$$
where $\varphi(xgx^{-1}) = \varphi(g)$.
  - This isomorphism is an isomorphism of vector spaces, *not* an isomorphism of algebras!
  - However, it still has cool properties.
    - For instance, consider the δ_{C_i}: The functions sending $g \in C_i$ to 1 and $g \notin C_i$ to 0.
    - The isomorphism identifies $e_i \mapsto \delta_{C_i}$.
  - Do we get irreducible characters (our other basis of class functions) when we sum the $\varphi(g)g$'s?
    - We do! What is this??
  - Let's consider another basis χ of irreducibles. The basis is $f_\chi = \frac{d_\chi}{|G|} \sum_{g \in G} \chi(g^{-1})g$, and we send it to χ_{V^*}.
  - Claim:
$$f_{\chi_i} f_{\chi_j} = \begin{cases} f_{\chi_i} & \chi_i = \chi_j \\ 0 & \chi_i \neq \chi_j \end{cases}$$
    - Things that multiply like this are called the **central idempotent**.
  - Thus, general multiplication works as follows.
$$(a_1 f_{\chi_1} + \cdots + a_n f_{\chi_n})(b_1 f_{\chi_1} + \cdots + e_n f_{\chi_n}) = a_1 b_1 f_{\chi_1} + \cdots + a_n b_n f_{\chi_n}$$
  - So if we want to send $a \in Z(G)$ to $\bigoplus^k \mathbb{C}$, we map
$$a = a_1 f_{\chi_1} + \cdots + a_k f_{\chi_k} \mapsto (a_1, \dots, a_k)$$
  - The proof of this claim is really simple because we've already done the computation with the projector on the irrep V_x.
    - So if you want to see $\rho(f_\chi)$, see what it does to the identity: It does $\rho(f_\chi)e = f\chi e = f_\chi$. ρ is regular.
- **Central idempotent**: An element such that $a^2 = a$ and $ax = xa$ for all $x \in A$.
- Two approaches to the same thing: Class functions and the center approach.
  - The great thing about the center: You can understand what it looks like because it is well-defined as a commutative algebra.
  - If something is isomorphic to $\mathbb{C} \oplus \cdots \oplus \mathbb{C}$ as an algebra, then there is another space and basis in which your multiplication looks incredibly simple.

[1] How did we get from the previous claim to here??

- We might get to **Hopf algebras** at the end of the course (very interesting).
  - Let $\mathbb{C}[G]$ be an associative algebra.
  - Let $\mathbb{C}[G]^*$ be the functions on the group.
  - Then $A \otimes A \to A$ sends $a_1 \otimes a_2 \mapsto a_1 a_2$.
  - When we dualize to get $A^* \otimes A^* \to A^*$, everything gets reversed, so we actually get a **comultiplication** $A \to A \otimes A$ given by $g \mapsto g \otimes g$. These two multiplications together are called a **Hopf algebra**.
  - Knowing that there's something that we can define and understand might help us untangle the knot of all the spaces.
  - This is pretty heavy math, though, so we won't go too deep into it if we get at all.
- Today was the last associative algebra class.
- Going forward: Integral elements, algebraic integers, dimension of the representation divides the order or the group, Burnside's theorem.
- Midterm is heavily computational: Tensor products, character tables, etc. A few simple questions about things.
  - Comparably less associative algebra stuff (maybe just 1 exercise).

6.2 Algebraic Numbers and the Frobenius Divisibility Theorem

11/1:

- Announcements.
  - OH on Zoom today as well; both OH next week will be in person.
- New topic for the next couple of classes (today and Friday at least, possibly Monday as well).
  - Proving two wonderful theorems.
- Theorem 1 (Frobenius divisibility theorem[2]): Let G be a finite group, and let V be an irreducible representation of G over $\mathbb{C}$. Then the degree of V divides the order of G, i.e.,

$$d_V \mid |G|$$

- Theorem 2 (Burnside): If G is a group and $|G| = p^n q^m$, then G is not simple. In fact, G is **solvable**.
  - Seems completely unrelated to Theorem 1, but the methods are similar.
  - The first statement in this theorem is hard and interesting. We will briefly talk about the second one, but it follows form the first by an easy induction.
- Both proofs are based on number theory.
  - As a warm-up to this branch of mathematics, let's talk about the algebraic integers.
- **Algebraic** (number): A number $x \in \mathbb{C}$ for which there exists $a_0, \dots, a_{n-1} \in \mathbb{Q}$ such that

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

- $\bar{\mathbb{Q}}$: The set of all algebraic numbers.
  - So $\mathbb{Q} \subset \bar{\mathbb{Q}} \subset \mathbb{C}$, where $\bar{\mathbb{Q}}$ is the set of all algebraic numbers.
  - π, e are famous examples of numbers that are *not* algebraic.

[2]There is no agreed-upon name for this result, but Fulton and Harris (2004) call it the "Frobenius divisibility theorem."

- **Algebraic** (integer): An algebraic number for which the corresponding $a_0, \dots, a_{n-1} \in \mathbb{Z}$.
- $\bar{\mathbb{Z}}$: The set of all algebraic integers.
- Examples.
  1. $\sqrt{2} \in \bar{\mathbb{Z}}$.
     - Because $(\sqrt{2})^2 - 2 = 0$.
  2. $\sqrt{3} \in \bar{\mathbb{Z}}$.
  3. $\sqrt{2}/2 \notin \bar{\mathbb{Z}}$.
     - Let $x = \sqrt{2}/2$.
     - We know that $2x^2 - 1 = 0$.
     - Suppose $d(x^n + a_{n-1}x^{n-1} + \cdots + a_0) = (2x^2 - 1)(dx^n + \cdots)$. This is an actual use of Gauss's Lemma from MATH 25800.
     - So $d = 1 \cdot 1$, contradiction.
     - How does this proof work??
- To get a handle on the algebraic integers, we'll prove some basic results (Facts 1-2 below).
- Fact 1: For all $x \in \bar{\mathbb{Q}}$, there exists $d \in \mathbb{N}$ such that $dx \in \bar{\mathbb{Z}}$.

  Proof. Take the polynomial with rational coefficients which is satisfied by x, and then multiply the polynomial by d^n where $d = \operatorname{lcm}(\text{denominators of } a_0, \dots, a_{n-1})$ is the greatest common denominator of all coefficients. This yields the polynomial

  $$(dx)^n + da_{n-1}(dx)^{n-1} + \cdots + d^n a_0 = 0$$

  in dx where each coefficient $d^i a_{n-i}$ is, by the definition of d, now an integer. □

- Fact 2: $\mathbb{Q} \cap \bar{\mathbb{Z}} = \mathbb{Z}$.

  Proof. We will use a bidirectional inclusion proof.
  $\underline{\mathbb{Q} \cap \bar{\mathbb{Z}} \subset \mathbb{Z}}$: Let $x \in \mathbb{Q} \cap \bar{\mathbb{Z}}$ be arbitrary. Since $x \in \mathbb{Q}$, there exist $a \in \mathbb{Z}$, $b \in \mathbb{N}$ with $(|a|, |b|) = 1$ (that is, with a, b coprime) such that $x = a/b$. Since $x \in \bar{\mathbb{Z}}$, there exist $a_0, \dots, a_n \in \mathbb{Z}$ such that

  $$\begin{gathered}\left(\frac{a}{b}\right)^n + a_{n-1}\left(\frac{a}{b}\right)^{n-1} + a_{n-2}\left(\frac{a}{b}\right)^{n-2} + \cdots + a_0 = 0 \\ a^n + a_{n-1}a^{n-1}b + a_{n-2}a^{n-2}b^2 + \cdots + a_0 b^n = 0\end{gathered}$$

  Now suppose for the sake of contradiction that there exists a prime number p dividing b. Then $b = px$ for some $x \in \mathbb{N}$. Consequently,

  $$\begin{gathered}a^n + a_{n-1}a^{n-1}px + a_{n-2}a^{n-2}(px)^2 + \cdots + a_0(px)^n = 0 \\ a^n + p(a_{n-1}a^{n-1}x + a_{n-2}a^{n-2}px^2 + \cdots + a_0 p^{n-1}x^n) = 0 \\ p\underbrace{\left(-a_{n-1}a^{n-1}x - a_{n-2}a^{n-2}px^2 - \cdots - a_0 p^{n-1}x^n\right)}_{y} = a^n\end{gathered}$$

  Thus, since $a^n = py$ (where y is an integer as the sum of products of integers), we have that $p \mid a^n$. It follows that $p \mid a$, since p is prime and raising a to a power doesn't introduce any new primes into its factorization. Consequently, since $p > 1$ as a prime number, there exists a number greater than 1 dividing both a and b. Therefore, $(|a|, |b|) > 1$, a contradiction. It follows that no prime number divides b, and hence, we must have $b = 1$ and $x = a \in \mathbb{Z}$, as desired.

  $\underline{\mathbb{Z} \subset \mathbb{Q} \cap \bar{\mathbb{Z}}}$: Let $x \in \mathbb{Z}$ be arbitrary. Then $x = x/1 \in \mathbb{Q}$. Additionally, choosing $a_0 = -x$, we have $x + a_0 = 0$. Thus, $x \in \bar{\mathbb{Z}}$. Combining these two results yields $x \in \mathbb{Q} \cap \bar{\mathbb{Z}}$, as desired. □

- We now look at the natural problem to which an algebraic integer is always the solution.
- Fact 3: Let $A \in M_{n\times n}(\mathbb{Z})$. If λ is an eigenvalue of A, then $\lambda \in \bar{\mathbb{Z}}$. More simply, $Av = \lambda v$ implies that $\lambda \in \bar{\mathbb{Z}}$.

  Proof. To prove that $\lambda \in \bar{\mathbb{Z}}$, it will suffice to find a monic polynomial P with integer coefficients such that $P(\lambda) = 0$. Let χ_A be the characteristic polynomial of A. As a characteristic polynomial, χ_A is monic. Additionally, since A is a matrix over the integers, the coefficients of χ_A will all be integers. Lastly, since $Av = \lambda v$, we know that $\chi_A(\lambda) = 0$. $\square$

- Lemma: The converse of Fact 3 is true. That is, if $\lambda \in \bar{\mathbb{Z}}$, then there exists $A \in M_{n\times n}(\mathbb{Z})$ and $v \in \mathbb{C}^n$[3] such that $Av = \lambda v$.
  - $\lambda \in \bar{\mathbb{Z}}$ implies $\lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_0 = 0$. This implies that there exists $A \in M_{n\times n}(\mathbb{Z})$ such that $\chi_A(\lambda) =$ this polynomial $= 0$. Rudenko leaves it as an exercise to find this A.
- We now use the above to give a cryptic proof of an interesting fact.
- Fact 4: $\bar{\mathbb{Z}}$ is a ring. That is, if $x, y \in \bar{\mathbb{Z}}$, then $x + y, xy \in \bar{\mathbb{Z}}$.

  Proof. Since $x, y \in \bar{\mathbb{Z}}$, the lemma implies that there exist A, B, v, w such that

  $$Av = xv \qquad\qquad Bw = yw$$

  Note that A can be of dimension $n \times n$ and B of dimension $m \times m$, i.e., they need not be the same dimension. Now how do we find a matrix for which the sum $x + y$ and product xy are eigenvalues? We use the tensor/Kronecker product to start! In particular,

  $$(A \otimes B)(v \otimes w) = xy(v \otimes w)$$

  For sum, we take $A \otimes I_m + I_n \otimes B$ so that

  $$(A \otimes I_m + I_n \otimes B)(v \otimes w) = xv \otimes w + v \otimes yw = (x + y)v \otimes w$$

  It follows by the two lines above and Fact 3 that $xy, x + y \in \bar{\mathbb{Z}}$, as desired. $\square$

- Notes on the above proof.
  - Types of proofs.
    - This is a nonstandard proof from Etingof et al. (2011).
    - The old proof from the 1800s uses symmetric stuff. It goes something like this:
      - Let $x = x_1, \dots, x_n$ and $y = y_1, \dots, y_m$, and take $\prod_{i,j=1}^{n,m}(t - x_i - y_j)$. Then we observe symmetric polynomials.
      - We'll cover a lot more of this stuff later.
    - There is also one more (more abstract) proof using modules.
  - Like algebraic integers form a ring, algebraic numbers form a field.
- So, cool... but why are algebraic integers relevant to us?
  - Observe that if G is a group and χ_V is a character, then for all $g \in G$, we have $\chi_V(g) \in \bar{\mathbb{Z}}$!
  - Why would this be the case?
    - Recall that since $g^n = e$, $\chi(g) = \operatorname{tr}(\rho(g)) = \varepsilon_1 + \cdots + \varepsilon_n$ where the ε_i are n^{th} roots of unity.
    - Each root of unity is an algebraic integer under the polynomial $x^n - 1 = 0$.
    - Thus, by inducting on Fact 4, the sum $\varepsilon_1 + \cdots + \varepsilon_n \in \bar{\mathbb{Z}}$.

[3] Where does v lie?? Is it $\mathbb{Z}^n$ or something, or are there no restrictions as I suspect?

- Fact 5: Let $C := \{g_1, \dots, g_s\}$ be a conjugacy class of G, and let $e_C := g_1 + \cdots + g_s \in \mathbb{Z}[G] \subset \mathbb{C}[G]$. Then there exist $a_0, \dots, a_{n-1} \in \mathbb{Z}$ such that

$$e_C^n + a_{n-1}e_C^{n-1} + \cdots + a_0 = 0$$

Proof. Define $L_{e_C} : \mathbb{Z}[G] \to \mathbb{Z}[G]$ by $a \mapsto e_C a$. Thus, L_{e_C} has eigenvalue e_C and matrix representation

$$L_{e_C} = \begin{array}{c} \\ g_1 \\ \vdots \\ g_n \end{array} \begin{array}{c} \begin{matrix} g_1 & \cdots & g_n \end{matrix} \\ \begin{pmatrix} & & \\ & & \\ & & \end{pmatrix} \end{array} \in M_{n\times n}(\mathbb{Z})$$

Therefore, by an argument analogous to that used in Fact 3, the desired $a_0, \dots, a_{n-1} \in \mathbb{Z}$ exist. □

- Example to illustrate the above argument: Consider $C = \{(12), (13), (23)\} \subset S_3$.
  - Then $e_C = (12) + (13) + (23)$.
  - Label the elements of S_3 as follows.

$$S_3 = \{\underbrace{e}_{g_1}, \underbrace{(12)}_{g_2}, \underbrace{(13)}_{g_3}, \underbrace{(23)}_{g_4}, \underbrace{(123)}_{g_5}, \underbrace{(132)}_{g_6}\}$$

  - Then the matrix of L_{e_C} is given by the following.

$$L_{e_C} = \begin{array}{c|cccccc} & e & (12) & (13) & (23) & (123) & (132) \\ \hline e & 0 & 1 & 1 & 1 & 0 & 0 \\ (12) & 1 & 0 & 0 & 0 & 1 & 1 \\ (13) & 1 & 0 & 0 & 0 & 1 & 1 \\ (23) & 1 & 0 & 0 & 0 & 1 & 1 \\ (123) & 0 & 1 & 1 & 1 & 0 & 0 \\ (132) & 0 & 1 & 1 & 1 & 0 & 0 \end{array}$$

    - Notice how, for example, representing e as $(1, 0, 0, 0, 0, 0)$ yields

$$L_{e_C}e = (0, 1, 1, 1, 0, 0) = (12) + (13) + (23) = e_C$$

    as expected.
  - We can then calculate that the characteristic polynomial $\chi_{L_{e_C}}$ of L_{e_C} is

$$\chi_{L_{e_C}}(\lambda) = \det(L_{e_C} - \lambda I) = \lambda^6 - 9\lambda^4$$

  - This yields

$$a_0 = 0 \qquad a_1 = 0 \qquad a_2 = 0 \qquad a_3 = 0 \qquad a_4 = -9 \qquad a_5 = 0$$

    as the desired coefficients.
  - Sanity check: We can confirm that

$$\begin{aligned} e_C^6 - 9e_C^4 &= e_C^4(e_C^2 - 9) \\ &= (9[e + (123) + (132)])(3[e + (123) + (132)] - 9) \\ &= 27[e + (123) + (132)]^2 - 81[e + (123) + (132)] \\ &= 81[e + (123) + (132)] - 81[e + (123) + (132)] \\ &= 0 \end{aligned}$$

- We will now prove Theorem 1. First, we restate it.
- Theorem 1 (Frobenius divisibility theorem): Let G be a finite group, and let V be an irreducible representation of G over $\mathbb{C}$. Then the degree of V divides the order of G, i.e.,

$$d_V \mid |G|$$

Proof. We begin with four definitions: Let $C := \{g_1, \dots, g_s\} \subset G$ be a conjugacy class of G, let $\mathbb{Z}[G] \subset \mathbb{C}[G]$ be a **group ring**, let $e_C := g_1 + \cdots + g_s \in \mathbb{Z}[G]$, and let $\rho : G \to GL(V)$ be the group homomorphism associated with the irreducible representation V.

With our notation set, let's look at how $\rho(g_1 + \cdots + g_s)$ acts on V. Since $g_1 + \cdots + g_s \in Z(\mathbb{C}[G])$, the proposition from Monday's class implies that

$$\rho(g_1 + \cdots + g_s) = \lambda I_{d_V}$$

Taking the trace of both sides of the above equation, we obtain the following. Note that in the below equations, $\chi(C)$ denotes $\chi(g_i)$ for any $g_i \in C$; all $\chi(g_i)$ are equal because χ is a class function.

$$\begin{aligned} \operatorname{tr}(\rho(g_1 + \cdots + g_s)) &= \operatorname{tr}(\lambda I_{d_V}) \\ \operatorname{tr}(\rho(g_1)) + \cdots + \operatorname{tr}(\rho(g_s)) &= \lambda \operatorname{tr}(I_{d_V}) \\ \sum_{i=1}^{s} \chi(C) &= \lambda d_V \\ |C|\chi(C) &= \lambda d_V \end{aligned}$$

It follows by a simple algebraic rearrangement that

$$\frac{|C|\chi(C)}{d_V} = \lambda$$

We can now prove that $\lambda \in \bar{\mathbb{Z}}$ via Fact 4. Let $v \neq 0$. Then

$$\begin{aligned} 0 &= \rho(0)v \\ &= \rho(e_C^n + a_{n-1}e_C^{n-1} + \cdots + a_0)v \\ &= [\rho(e_C)^n + a_{n-1}\rho(e_C)^{n-1} + \cdots + a_0]v \\ &= \underbrace{(\lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_0)}_{0} v \end{aligned}$$

Now recall that by the first orthogonality relation, we have that

$$\sum_C |C|\chi(C)\overline{\chi(C)} = |G|$$

It follows by dividing through by d_V that

$$\frac{|G|}{d_V} = \sum_C \frac{|C|\chi(C)}{d_V} \cdot \overline{\chi(C)}$$

But $|C|\chi(C)/d_V = \lambda \in \bar{\mathbb{Z}}$ by the above and $\overline{\chi(C)} \in \bar{\mathbb{Z}}$ by the earlier note about roots of unity, so by Fact 4, the whole sum of products $|G|/d_V \in \bar{\mathbb{Z}}$. Naturally, $|G|/d_V \in \mathbb{Q}$ as well. Consequently, $|G|/d_V \in \bar{\mathbb{Z}} \cap \mathbb{Q}$, so by Fact 2, $|G|/d_V \in \mathbb{Z}$. Therefore, we must have $d_V \mid |G|$. ☐

- Notes on the above proof.
  - In this course, we will not talk to much about integral elements; those will be the focus of Rudenko's next course, Algebraic Geometry.

- Definitely take some time to think through this proof before next class! It's short, but quite subtle. Next class's will be much much harder.
- Rudenko will not be here for next Friday's midterm; someone else will be proctoring, though.
- Next week's HW will be a preparational HW.