Some stuff about orbital graphs

Johannes Hahn

March 19, 2019

0.1 Definition:
Let $G \curvearrowright \Omega$ be any group action on a set Ω. An orbit of the induced action of G on $\Omega^2 = \Omega \times \Omega$ is called an orbital of the action $G \curvearrowright \Omega$. The number of orbitals is called the rank of the action.
If Γ is any orbital, then the directed graph with vertex set Ω and an edge $\alpha \leftarrow \beta$ iff $(\alpha, \beta) \in \Gamma$ is called an orbital graph of the action.

0.2 Definition:
Let $G \curvearrowright \Omega$ be a transitive action and $\omega \in \Omega$. A G_ω-orbit of this action is called a suborbit. The sizes of the suborbits are called the subdegrees of the action. By transitivity, the subdegrees are independent of $\omega \in \Omega$.

Convention:
For everything that follows, fix a finite, non-empty set Ω and a permutation group $G \leq Sym(\Omega)$. In other words, from now on we consider only faithful permutation actions of G.
Set $n := |\Omega|$, let l be the number of G-orbits on Ω and let r be the rank.
In those cases where $G \curvearrowright \Omega$ is transitive, we will denote the subdegrees by $1 = n_1, n_2, \ldots, n_r$. (We will see in the next theorem that there are in fact exactly r suborbits)

1 Orbital graphs vs. suborbits vs. double cosets – A dictionary

1.1 Theorem and definition (Dictionary theorem)**:**
Let $G \curvearrowright \Omega$ be a group action, $\Omega = Q_1 \sqcup \ldots \sqcup Q_l$ its orbit decomposition, $\omega_i \in Q_i$ fixed orbit-representatives, and $H_i := G_{\omega_i}$ their stabilisers.

a.) There are bijections between the following sets

- $\mathscr{P}(\Omega \times \Omega)^G$, the set of all G-invariant subsets $\Gamma \subseteq \Omega \times \Omega$,
- $\prod_{1 \leq i \leq l} \mathscr{P}(\Omega)^{H_i}$, the set of all l-tuples $(\Delta_1, \ldots, \Delta_l)$ where Δ_i is an H_i-invariant subset of Ω.
- $\prod_{1 \leq i,j \leq l} \mathscr{P}(G)^{H_i \times H_j}$, the set of all $l \times l$-tuples (D_{ij}) where $D_{ij} \subseteq G$ is invariant under left-multiplication by H_i and right-multiplication by H_j.

given in the upper block of table 1.

b.) Moreover, these bijections also translate the properties listed in the rest of table 1.

Proof. It is a tedious, but straight-forward exercise to verify that the given mappings in the first three lines of the table are well-defined, compatible bijections and translate the listed properties as stated. □

1.2 Corollary:
The three sets in the dictionary theorem are posets w.r.t. (component-wise) inclusion and the bijections are order-isomorphisms.
In particular the sets of minimal non-empty elements in these posets, namely

- Ω^2/G, the set of orbitals,
- $\bigsqcup_{i=1}^{l} \Omega/H_i$, the set of suborbits, where we distinguish ${}^{H_i}\omega$ and ${}^{H_j}\omega$ for $i \neq j$ even if H_i and H_j happen to be identical subgroups.
- $\bigsqcup_{1 \leq i,j \leq l} H_i \backslash G / H_j$, the set of double cosets, where we distinguish $H_i y H_j$ and $H'_i y H'_j$ for $(i, j) \neq (i', j')$ even if $H_i = H'_i$ or $H_j = H'_j$.

are mapped bijectively onto each other. Table 2 lists the consequences of the general translations for orbital, suborbits and double-cosets.

$\mathscr{P}(\Omega \times \Omega)^G$	$\prod_{1 \leq i \leq l} \mathscr{P}(\Omega)^{H_i}$	$\prod_{1 \leq i,j \leq l} \mathscr{P}(G)^{H_i \times H_j}$
Γ	$\Delta_i := \Gamma(\omega_i) := \{\, \alpha \mid (\alpha, \omega_i) \in \Gamma \,\}$	$D_{ij} := \{\, y \in G \mid ({}^y\omega_j, \omega_i) \in \Gamma \,\}$
$\bigcup_{\substack{1 \leq i \leq l \\ g \in G}} {}^g(\Delta_i \times \{\, \omega_i \,\})$	(Δ_i)	$D_{ij} := \{\, y \in G \mid {}^y\omega_j \in \Delta_i \,\}$
$\bigcup_{1 \leq i,j \leq l} \{\, ({}^x\omega_j, {}^y\omega_i) \mid y^{-1}x \in D_{ij} \,\}$	$\Delta_i := \bigcup_{1 \leq j \leq l} {}^{D_{ij}}\omega_j$	(D_{ij})
$\{\, (\alpha, \alpha) \mid \alpha \in Q_i \,\}$	$(\emptyset, \ldots, \emptyset, \{\, \omega_i \,\}, \emptyset, \ldots, \emptyset)$	$\mathrm{diag}(\emptyset, \ldots, \emptyset, H_i \emptyset, \ldots, \emptyset)$
Γ^{op}	$\Delta_i^* := \{\, \alpha \mid \exists j, g : \alpha = {}^g\omega_j \wedge {}^{g^{-1}}\omega_j \in \Delta_i \,\}$	$(D^*)_{ij} := D_{ji}^{-1}$
$\lvert \Gamma \cap Q_i \times Q_j \rvert$	$\lvert Q_j \rvert \lvert \Delta_j \cap Q_i \rvert = \lvert Q_i \rvert \lvert \Delta_i^* \cap Q_j \rvert$	$\frac{\lvert G \rvert \lvert D_{ji} \rvert}{\lvert H_i \rvert \lvert H_j \rvert}$
$\Gamma \circ \Gamma'$	$(\Delta \circ \Delta')_i := \{\, \alpha \mid \exists j, g : (\alpha, \omega_j) \in {}^g\Delta_j \times {}^{g^{-1}}\Delta_i' \,\}$	$\left(\bigcup_k D_{ik} D_{kj}' \right)_{i,j=1..l}$
Γ reflexive	$(\{\, \omega_1 \,\}, \ldots, \{\, \omega_l \,\}) \subseteq \Delta$	$\mathrm{diag}(H_1, \ldots, H_l) \subseteq D$
Γ transitive	$\Delta \circ \Delta \subseteq \Delta$	$\forall i, j, k : D_{ij} D_{jk} \subseteq D_{ik}$
Γ symmetric	$\Delta = \Delta^*$	$D_{ij} = D_{ji}^{-1}$
Γ antisymmetric	$\Delta_i \cap \Delta_i^* \subseteq \{\, \omega_i \,\}$	$D_{ij} \cap D_{ji}^{-1} \subseteq H_i$
Γ equiv.relation	Δ_i block	$\forall i : H_i \leq D_{ii} \leq G$ $\forall i, j : D_{ij} = \emptyset \vee \exists g \in G : D_{ii} g = D_{ij} = g D_{jj}$

Table 1: The relationship between G-invariant binary relations between points, H_i-invariant point sets, and H_i-H_j-invariant subsets of G

Orbitals Ω^2/G	Suborbits	double cosets
Γ	$\Delta \in \Omega/H_i$ with $\Delta = \Gamma(\omega_i)$	$H_i y H_j$ with $({}^{y}\omega_j, \omega_i) \in \Gamma$
$\bigcup_{g \in G} {}^{g}(\Delta \times \{\, \omega_i \,\})$	$\Delta \in \Omega/H_i$	$H_i y H_j$ with ${}^{y}\omega_j \in \Delta$
$\{\, ({}^{x}\omega_j, {}^{x'}\omega_i) \mid H_i x'^{-1} x H_j = H_i y H_j \,\}$	${}^{H_i y}\omega_j \in \Omega/H_i$	$H_i y H_j$
(i, j) with $\Gamma \subseteq Q_j \times Q_i$	$\Delta \in \Omega/H_i \wedge \Delta \subseteq Q_j$	$H_i y H_j \in H_i \backslash G / H_j$
$\lvert\Gamma\rvert$	$\lvert Q_i\rvert \lvert\Delta\rvert = \lvert\Delta^*\rvert \lvert Q_j\rvert$	$\lvert G : H_i \cap {}^{y}H_j\rvert = \lvert G : {}^{y^{-1}}H_i \cap H_j\rvert$

Table 2: The relationship between orbitals, suborbits and double-cosets

1.3 Lemma:
Let $G \curvearrowright \Omega$ be transitive, $\omega \in \Omega$ a fixed element and $H := G_\omega$ its stabiliser.
The set of H-invariant subsets of Ω is a monoid w.r.t. $\circ_\omega$, $\{\omega\}$ is the neutral element, $\emptyset$ is a zero element, and $\Delta \mapsto \Delta^*$ is an antiautomorphism of order two of this monoid.
Moreover the monoid is filtered by size of the subsets:

$$\forall \Delta, \Delta' \neq \emptyset : \max\{|\Delta|, |\Delta'|\} \leq |\Delta \circ_\omega \Delta'| \leq |\Delta||\Delta'|$$

Proof. The first few claims all follows from the dictionary theorem after translation into the language of binary relations on Ω. The bounds on the size follow from translating to double cosets. □

1.4 Corollary:
Let $G \curvearrowright \Omega$ be transitive, $\omega \in \Omega$ be fixed, $\Gamma = \Gamma_i \subseteq \Omega^2$ be any orbital, n_i its subdegree, and let HyH be its associated double coset.

a.) Connected components of (Ω, Γ) are automatically strongly connected.

b.) The connected component of ω in (Ω, Γ) is exactly ${}^U\omega$, where $U := \langle H, y\rangle$.

c.) (Ω, Γ) is connected iff $\langle H, y\rangle = G$.

d.) If (Ω, Γ) is connected and the rank is r, then $|\Omega| \leq \frac{n_i^r - 1}{n_i - 1}$.

e.) G acts primitively iff all non-diagonal orbital graphs are connected.

Proof. a. If that were not the case, there would be a connected component $\emptyset \neq C \subseteq \Omega$ which decomposes further $C = X_0 \sqcup \ldots \sqcup X_n$ into strongly connected components. Wlog we number them such that edges from X_i into X_j exist only if $i < j$. Pick any $x_0 \in X_0$, $x_k \in X_k$. Since G is transitive, there would be a $g \in G$ such that ${}^g x_0 = x_k$. In particular ${}^g C = C$, since C is connected component. Hence $\langle g\rangle$ acts as graph automorphisms on C and must permute the strongly connected components. But that means it must map X_0 to X_k which is impossible because the former only only has out-going edges, while the latter only has in-coming edges.

Because of a. we determine the strongly connected components. A direct path $\alpha = \alpha_0 \leftarrow \alpha_1 \leftarrow \ldots \leftarrow \alpha_l = \beta$ exists iff $(\alpha, \beta) \in \Gamma^{\circ l}$, i.e. $\Gamma^\infty := \bigcup_{l \geq 0} \Gamma^{\circ l}$ is the equivalence relation which induces the partition into connected components on Ω.
By our dictionary, this equivalence relation corresponds to the subgroup $H \cup HyH \cup HyHyH \cup \ldots = U$. The component D of ω is the corresponding suborbit $\Gamma^\infty(\omega) = D = {}^U\omega$.

d. follows directly from c. The upper bound for the size follows from the same idea: If (Ω, Γ) is connected and the action has finite rank, then $\Omega^2 = \bigcup_{l \geq 0} \Gamma^{\circ l} = \bigcup_{l=0}^{r-1} \Gamma^{\circ l}$ because the union gets stationary when no new orbitals are added and there are only r of them.

Thus

$$\Omega = \Gamma^{\infty}(\omega) = \bigcup_{l=0}^{r-1} \Gamma^{\circ l}(\omega) = \{\, \omega \,\} \cup \Delta \cup (\Delta \circ_\omega \Delta) \cup (\Delta \circ_\omega \Delta \circ_\omega \Delta) \cup \ldots$$

so that

$$|\Omega| \leq 1 + n_i + n_i^2 + n_i^3 + \ldots + n_i^{r-1} = \frac{n_i^r - 1}{n_i - 1}$$

Note that $n_i > 1$, otherwise Γ would be diagonal and (Ω, Γ) couldn't be connected.

e. follows directly from c. and the fact that G acts primitively on Ω iff H is a maximal subgroup. □

1.5 Remark: This lemma allows for easy identification of at least one block system for the action of G on Ω, namely the connected components of (Ω, Γ). They coincide with the sets ${}^{gU}\omega$.
Moreover: ${}^{U}\omega$ is the smallest possible block containing both ω and ${}^{y}\omega$.

2 The k-closure of a permutation group

2.1 Definition (k-closure)**:**
Let $k \in \mathbb{N}$. The k-closure of G is defined as the largest subgroup $G^{(k)} \subseteq Sym(\Omega)$ that has the same orbits as G on Ω^k, i.e.

$$G^{(k)} := \left\{ \pi \in Sym(\Omega) \;\middle|\; \forall \Gamma \in \Omega^k/G : {}^{\pi}\Gamma = \Gamma \right\}$$

G is called k-closed iff $G = G^{(k)}$ holds.

2.2 Remark: Some immediate properties of k-closure include:

- Taking k-closures is idempotent: $(G^{(k)})^{(k)} = G^{(k)}$.
- If $Q_1, \ldots, Q_l$ are the orbits of G on Ω, then $G^{(1)} = Sym(Q_1) \times \cdots \times Sym(Q_l)$. An equally simple and straight forward description of the other $G^{(k)}$, even of $G^{(2)}$ is not available in general.
- If $n := |\Omega|$, then

  $$G = G^{(n)} \leq G^{(n-1)} \leq \ldots \leq G^{(2)} \leq G^{(1)} \leq G^{(0)} = Sym(\Omega)$$

  because the action of G on Ω^k is isomorphic to the action on $\{\, (\alpha, \alpha) \mid \alpha \in \Omega \,\} \times \Omega^{k-1} \subseteq \Omega^{k+1}$.
- In particular if $k \geq 1$, then $G^{(k)}$ has the same orbits as G, has the same fixed points as G and is transitive if and only if G is.

- G is primitive iff $G^{(2)}$ is, because both groups have the same invariant subsets of $\Omega \times \Omega$, in particular they have the same invariant equivalence relations.
- G is k-transitive iff $G^{(k)} = Sym(\Omega)$.

2.3 Lemma (Elementary properties of the k-closure)**:**
Let $G, G_0, G_1 \leq Sym(\Omega)$ be permutation groups and $k \in \mathbb{N}$.

a.) If $G_0 \leq G_1$, then $G_0^{(k)} \leq G_1^{(k)}$.

b.) If $\Omega = \Omega_0 \sqcup \Omega_1$ and $G = G_0 \times G_1$ with $G_i \leq Sym(\Omega_i)$, then $G^{(k)} = G_0^{(k)} \times G_1^{(k)}$.

c.) If $\Omega = \Omega_0 \sqcup \Omega_1$ with disjoint, G-invariant subsets, let $G_{|\Omega_i} \leq Sym(\Omega_i)$ be the permutation group induced by the action of G on Ω_i. Then $G^{(k)} \leq (G_{|\Omega_0})^{(k)} \times (G_{|\Omega_1})^{(k)}$.

Proof. a. Let $g \in G_0^{(k)}$ be arbitrary and let $\Gamma \subseteq \Omega^k$ be G_1-invariant. Because $G_0 \leq G_1$, Γ is also G_0-invariant and therefore ${}^g\Gamma = \Gamma$. Since Γ was arbitrary, $g \in G_1^{(k)}$.

b. Every G_i-orbit $\Gamma \subseteq \Omega_i^k$ is also a $G_0 \times G_1$-orbit so that $(G_0 \times G_1)^{(k)} \leq \bigcap_{\Gamma \in \Omega_i^k/G_i} \mathrm{Aut}(\Omega, \Gamma) = \bigcap_{\Gamma \in \Omega_i^k/G_i} \mathrm{Aut}(\Omega_i, \Gamma) \times Sym(\Omega_{1-i})$ which proves $(G_0 \times G_1)^{(k)} \leq G_0^{(k)} \times G_1^{(k)}$.
Conversely, let $g = g_0 g_1 \in G_0^{(k)} \times G_1^{(k)}$ be arbitrary and $\Gamma \subseteq \Omega^k$ any G-orbit. There are unique $s, t \in \mathbb{N}$ with $s + t = k$ such that, up to reordering of the components in this product (which does not change the stabiliser of Γ), $\Gamma \subseteq \Omega_0^s \times \Omega_1^t$.
Let $\Gamma = {}^G(\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_t)$ for some points $\alpha_1, \ldots, \alpha_s \in \Omega_0$, $\beta_1, \ldots, \beta_t \in \Omega_1$. Then

$$\Gamma = \underbrace{{}^{G_0}(\alpha_1, \ldots, \alpha_s)}_{=:\Gamma_0} \times \underbrace{{}^{G_1}(\beta_1, \ldots, \beta_t)}_{=:\Gamma_1}$$

so that ${}^g\Gamma = {}^{g_0}\Gamma_0 \times {}^{g_1}\Gamma_1$. Because $g_0 \in G_0^{(k)} \leq G_0^{(s)}$ and $g_1 \in G_1^{(k)} \leq G_1^{(t)}$, we find that ${}^g\Gamma = \Gamma_0 \times \Gamma_1 = \Gamma$ so that $g \in G^{(k)}$.

c. follows from combining a. and b. because $G \leq G_{|\Omega_0} \times G_{|\Omega_1}$ holds by construction. □

2.1 The 2-closure - examples and non-examples

2.4 Example:
A regular permutation group is always 2-closed.

Proof. A regular G-set is isomorphic to G itself endowed with left multiplication. The orbitals of this action are given by $\Gamma_h := \{ (x, y) \in G^2 \mid x^{-1}y = h \}$ for $h \in G$ and one can readily verify that the only permutations fixing all the orbitals are the left multiplication maps themselves. □

2.5 Example:
Let $\Omega = \{ 0, 1, \ldots, 2n-1 \}$ with $n \geq 3$, $\Omega_0 = \Omega \cap 2\mathbb{N}$, $\Omega_1 = \Omega \setminus \Omega_0$.
Let $G = \{ \pi_0\pi_1 \mid \pi_i \in Sym(\Omega_i), \mathrm{sgn}(\pi_0) = \mathrm{sgn}(\pi_1) \}.\langle\sigma\rangle$ where $\sigma := \prod_{i\in\Omega_0}(i, i+1)$. This group is transitive, since it contains $Alt(\Omega_0) \times Alt(\Omega_1)$ which is transitive on both sets individually, and it contains at least the permutation σ which switches both sets. Clearly Ω_0 and Ω_1 are blocks for this action so that G is imprimitive.
The stabiliser G_0 cannot switch these blocks. Therefore

$$G_0 = \{ \pi_0\pi_1 \mid \pi_i \in Sym(\Omega_i), \pi_0(0) = 0, \mathrm{sgn}(\pi_0) = \mathrm{sgn}(\pi_1) \}.$$

The suborbits are $\{ 0 \}, \Omega_0 \setminus \{ 0 \}$ and Ω_1. Therefore the subdegrees are 1,$n-1$ and n.
The two non-diagonal orbitals are

$$\Gamma_{n-1} = {}^G(0, 2) = \{ (\alpha, \beta) \mid \alpha \equiv \beta \mod 2 \}$$

$$\Gamma_n = {}^G(0, 1) = \{ (\alpha, \beta) \mid \alpha \not\equiv \beta \mod 2 \}$$

The first orbital graph consists therefore of two disjoint, complete graphs on odd and even numbers. The second graph is the complete bipartite graph $K_{n,n}$.
Both graphs have $(Sym(\Omega_0) \times Sym(\Omega_1)).\langle\sigma\rangle$ as automorphism groups which is therefore the 2-closure of G. We see that G is of index 2 in $G^{(2)}$.

2.6 Example (Rank ≤ 4)**:**
If G is 2-transitive, then $G^{(2)} = Sym(\Omega)$. Thus essentially all 2-transitive groups are not 2-closed.

If G has rank 3, then $G^{(2)} = \mathrm{Aut}(\Omega, \Gamma)$ for both of the two non-diagonal orbitals, because they are complementary graphs and therefore have identical automorphism groups.

If G has rank 4 and one orbit Γ that is not self-paired, then $G^{(2)} = \mathrm{Aut}(\Omega, \Gamma)$ as well, because $\mathrm{Aut}(\Omega, \Gamma) = \mathrm{Aut}(\Omega, \Gamma^{op})$ so that the automorphism group already stabilises two of the four orbitals. It also stabilises the diagonal for trivial reasons so that the fourth one also must be stabilised.

2.7 Corollary (Size estimates)**:**
$|G^{(2)}|$ divides $\prod_{i=1}^{l}|Q_i| \prod_{\Delta\in Q_i/H_i}|\Delta|!$

Proof. Using the notation in lemma 2.3, we find $G^{(2)} \leq (G_{|Q_1})^{(2)} \times \ldots \times (G_{|Q_l})^{(2)}$.
Therefore we can assume that G is transitive. Set $\omega = \omega_1$, $H = H_1$, and let $\Delta_1, \ldots, \Delta_r$ be the H-orbits on Ω. Then $G = |G : H||H| = |\Omega||H|$. And because $H \leq H^{(1)} = Sym(\Delta_1) \times \ldots \times Sym(\Delta_r)$, we find that $|H|$ divides $\prod_{\Delta\in\Omega/H}|\Delta|!$ which proves the lemma. $\square$

2.8 Remark: This bound is rarely sharp, because H is rarely 1-closed. And even if that is the case, then the inclusion $G^{(2)} \leq (G_{|Q_1})^{(2)} \times \ldots \times (G_{|Q_l})^{(2)}$ can still be strict.

2.9 Theorem:
Cyclic permutation groups are 2-closed.

Proof. Let $G = \langle\sigma\rangle \leq Sym(n)$ and $\sigma = \sigma_1 \cdots \sigma_l$ the cycle decomposition of σ. We argue by induction on l. For $l = 0$ there is nothing to prove. If $l = 1$ then G acts regular on its non-trivial orbit and is therefore 2-closed.
By the previous lemma $G^{(2)} \leq \langle\sigma_1 \cdots \sigma_{l-1}\rangle^{(2)} \times \langle\sigma_l\rangle^{(2)}$. By the induction hypothesis and because $\langle\sigma_l\rangle$ acts regularly on its non-trivial orbit, we find $G^{(2)} \leq \langle\sigma_1 \cdots \sigma_{l-1}\rangle \times \langle\sigma_l\rangle$.
Let $g = (\sigma_1 \cdots \sigma_{l-1})^a \sigma_l^b \in G^{(2)}$ be arbitrary with $a, b \in \mathbb{Z}$. We want to show $g \in G$. By replacing g by $\sigma^{-a}g$, we can assume wlog that $a = 0$. Then $g \in G$ is equivalent to $b \equiv 0 \mod ord(\sigma_1 \cdots \sigma_{l-1})$ which is equivalent to $\forall i < l : b \equiv 0 \mod ord(\sigma_i)$.
Number the non-trivial orbits of G according to the cycles $Q_1, \ldots, Q_l$ and pick any pair $(\alpha, \beta) \in Q_i \times Q_l$ for some $1 \leq i < l$ and let $\Gamma := {}^G(\alpha, \beta)$ its orbital. Wlog we can assume $i = 1$, $\alpha = 0$, $\sigma_1 = (0, 1, 2, \ldots, k-1)$, $\beta = k$ and $\sigma_l = (k, k+1, k+2, \ldots, k+m-1)$ so that $ord(\sigma_1) = k$ and $ord(\sigma_l) = m$.
Because g is a power of σ_l it fixes the point 0. The pairs of the form $(0, \gamma)$ which are contained in Γ are all given by ${}^{\sigma^{sk}}(0, \beta) = (0, {}^{\sigma_l^{sk}}k) = (0, k + (sk \mod m))$ for $s \in \mathbb{Z}$, i.e. they correspond bijectively to elements of the subgroup $T := \langle k + m\mathbb{Z}\rangle \leq \mathbb{Z}/m$. Since we could replace b by any $b + tm$ without changing g, we only have to show that $b + m\mathbb{Z}$ is contained in this subgroup.
Since $g \in G^{(2)}$ is a graph automorphism of (Ω, Γ) and fixes the point 0, it must also map these edges amongst themselves. In particular ${}^g k = k + (sk \mod m)$ for some $s \in \mathbb{Z}$. But since $g = \sigma_l^b$, this is only possible if $b + m\mathbb{Z} \in \langle k + m\mathbb{Z}\rangle$ which is exactly what we wanted to prove. $\square$

3 Orbital graphs vs. representation theory

3.1 Definition:
Now let $V := \mathbb{K}^\Omega$ be the $\mathbb{K}$-vector space with basis Ω. This vector space is naturally a $\mathbb{K}G$-module by extending the action of G on the basis elements linearly to the whole space.
We will identify $\mathrm{End}_{\mathbb{K}}(V)$ with the space $\mathbb{K}^{\Omega\times\Omega}$ of matrices indexed by $\Omega \times \Omega$. We will also identify $Sym(\Omega)$ with the group of permutation matrices.

3.2 Theorem and definition:
For $\Gamma \subseteq \Omega^2$ define the matrix $X_\Gamma \in \mathbb{K}^{\Omega\times\Omega}$ as follows:

$$(X_\Gamma)_{\alpha\beta} := \begin{cases} 1 & \text{if } (\alpha, \beta) \in \Gamma \\ 0 & \text{otherwise} \end{cases}$$

With this notation, the set $\{ X_\Gamma \mid \Gamma \subseteq \Omega^2 \text{ orbital} \}$ is a $\mathbb{K}$-basis of $\mathrm{End}_{\mathbb{K}G}(V)$. The structure constants w.r.t. this basis, i.e. the numbers d_{ij}^k such that

$$X_{\Gamma_i} \cdot X_{\Gamma_j} = \sum_k d_{ij}^k X_{\Gamma_k},$$

are given by $d_{ij}^k := |\{\, \beta \in \Omega \mid (\alpha, \beta) \in \Gamma_i \wedge (\beta, \gamma) \in \Gamma_j \,\}|$ where (α, γ) is any element of Γ_k.

3.3 Remark: In other words: X_Γ is the adjacency matrix of the directed graph (Ω, Γ). In particular: The automorphism group of (Ω, Γ) is the group of those permutations which centralise X_Γ, i.e. $Sym(n) \cap C(X_\Gamma)$.

3.4 Remark: Note that the right hand side in the definition of d_{ij}^k really is independent of the choice of the element $(\alpha, \gamma) \in \Gamma_k$, because G acts transitively on Γ_k.

Proof of the theorem. Writing out the defining condition

$$X \in \mathrm{End}_{\mathbb{K}G}(V) \iff \forall g \in G : gXg^{-1} = X$$

in components shows that every $\mathbb{K}G$-linear endomorphism is indeed a linear combination of the X_Γ where Γ is a G-orbit on Ω^2. The X_Γ are linearly independent, because the orbitals are disjoint, and therefore they are a basis.
The formula for the structure constants similarly follows by writing out the definition of matrix multiplication in this case. □

3.5 Lemma and definition (Support of matrices)**:**
The support of a matrix $X \in \mathbb{K}^{\Omega \times \Omega}$ is defined as

$$\mathrm{supp}(X) := \{\, (\alpha, \beta) \in \Omega \times \Omega \mid X_{\alpha\beta} \neq 0 \,\}$$

supp is a homomorphism of semirings $(\mathbb{N}^{\Omega \times \Omega}, +, \cdot) \to (\mathscr{P}(\Omega \times \Omega), \cup, \circ)$ that is $Sym(n)$-equivariant. In particular it maps matrices centralised by G to G-invariant subsets.

Proof. trivial. □

3.6 Theorem:
Let $\Gamma \subseteq \Omega^2$ be G-invariant. Let $d \in \mathbb{N}$ be the degree of the minimal polynomial of $X_\Gamma \in \mathrm{End}_{\mathbb{Q}G}(V)$ and let δ be the maximum of the directed diameters of the connected components of (Ω, Γ), i.e.

$$\delta := \max_{C \text{ component}} \min \{\, l \in \mathbb{N} \mid \forall \alpha, \beta \in C \exists \text{dir.path } \alpha = \alpha_0 \leftarrow \ldots \leftarrow \alpha_k = \beta \text{ with } k \leq l \,\}$$

With these notations:

$$\delta < d \leq r$$

Proof. The inequality $d \leq r$ follows immediately from $\dim \mathrm{End}_{\mathbb{Q}G}(V) = r$. Thus we only have to prove the other one.
Let Γ_0 be the diagonal (which may a proper union of orbitals if G does not act transitively) and set $\widetilde{\Gamma} := \Gamma \cup \Gamma_0$. This is the support of $X_\Gamma + 1$, because X_{Γ_0} is the identity

matrix. Note that $\widetilde{\Gamma}^{\circ s} \subseteq \widetilde{\Gamma}^{\circ(s+1)}$ for all $s \in \mathbb{N}$ and if equality holds for some $s \in \mathbb{N}$, then $\widetilde{\Gamma}^{\circ s} = \widetilde{\Gamma}^{\circ t}$ for all $t \geq s$.
Now it is easy to see that δ is the number of steps in this chain with proper inclusions, i.e.

$$\Gamma_0 = \widetilde{\Gamma}^{\circ 0} \subsetneq \widetilde{\Gamma} \subsetneq \widetilde{\Gamma}^{\circ 2} \subsetneq \ldots \subsetneq \widetilde{\Gamma}^{\circ \delta} = \widetilde{\Gamma}^{\circ(\delta+1)} = \widetilde{\Gamma}^{\circ(\delta+2)} = \ldots$$

Thus $1, X_\Gamma + 1, ..., (X_\Gamma + 1)^\delta$ are linearly independent, because the support of these elements is strictly increasing. Therefore the minimal polynomial of $X_\Gamma + 1$ has at least degree $\delta + 1$ and the minimal polynomial of X_Γ has the same degree. □

3.7 Remark: Using the notation in the proof, the differences $\Gamma_s := \widetilde{\Gamma}^{\circ s} \setminus \widetilde{\Gamma}^{\circ(s-1)}$ contains exactly those pairs (α, β) that can be connected by a directed path of length s, not by a path of length $\leq s - 1$, i.e. the directed distance from β to α equals s.
It is clear that the automorphism group of the graph (Ω, Γ) fixes these sets. But we can say more: The automorphism group also stabilises each part of the partition $\Gamma_s = A_1 \sqcup A_2 \sqcup \ldots$ where A_k is the set of (α, β) of directed distance s which are connected by exactly k directed paths of length s.
Γ_s is exactly the piece by which the support grows when going from $(X_\Gamma + 1)^{s-1}$ to $(X_\Gamma + 1)^s$. A quick calculations shows that

$$(X_\Gamma + 1)^s - (X_\Gamma + 1)^{s-1} = \sum_{k \in \mathbb{N}} k X_{A_k}$$

This is an algebraic analogue of the combinatorial consideration above: The automorphism group of (Ω, Γ) centralises X_Γ and therefore also centralises the left hand side of the equation. Since it only permutes the entries of the matrix, the set of entries with a given value must be invariant under all graph automorphisms.

3.1 Computing the 2-closure

3.8 Theorem (2-closure in terms of endomorphism algebras)**:**
$G^{(2)} = Sym(\Omega) \cap C(\mathrm{End}_{\mathbb{K}G}(V))$.

Proof. Let $G^{(2)}$ be the 2-closure of G. By definition $\pi \in Sym(\Omega)$ is in $G^{(2)}$ if and only if $\pi X_\Gamma \pi^{-1} = X_\Gamma$ for all $\Gamma \in \Omega^2/G$. But the X_Γ are a $\mathbb{K}$-basis of the endomorphism algebra. Therefore π is in the 2-closure iff it is a permutation matrix and an element of the centraliser of the endomorphism ring of the $\mathbb{K}G$-module V. □

3.9 Lemma (2-closure in terms of linear algebra)**:**
$G^{(2)} = Sym(\Omega) \cap \mathrm{span}_{\mathbb{K}}(G)$. In particular, G is 2-closed if no permutation matrix outside of G is a linear combination of elements of G.

Maybe remove, not useful at the moment

Proof. Observe that $\mathrm{End}_{\mathbb{K}G}(V)$ is by definition the centraliser algebra of the subalgebra $\mathrm{span}_{\mathbb{K}}(G) \subseteq \mathbb{K}^{\Omega \times \Omega}$.
V is a faithful $\mathbb{K}G$-module and $\mathbb{K}G$ is a symmetric algebra. Therefore V has the double centraliser property so that $C(\mathrm{End}_{\mathbb{K}G}(V)) = C(C(\mathrm{span}_{\mathbb{K}}(G))) = \mathrm{span}_{\mathbb{K}}(G)$. □

3.10 Remark: Let $\Gamma_1, \dots, \Gamma_r$ be the orbitals of G.
We have already seen that

$$G^{(2)} = Sym(n) \cap C(\mathrm{End}_{\mathbb{K}G}(V)) = Sym(n) \cap \bigcap_{i=1}^{r} C(X_{\Gamma_i}) = \bigcap_{i=1}^{r} \mathrm{Aut}(\Omega, \Gamma_i)$$

Since it is expensive to compute all automorphism groups of all orbital graphs and many orbital graphs in fact have the same automorphism group (for example Γ and Γ^{op}), it is desirable to compute as few of these groups as possible. Using that $\mathrm{End}_{\mathbb{K}G}(V)$ is a $*$-algebra, we can ignore some of the orbitals in the computation of the 2-closure.

More precisely: If $g \in Sym(n)$ centralises $X_1, \dots, X_s$, it also centralises the $\mathbb{K}$-algebra generated by $X_1, \dots, X_s$. Therefore it is sufficient to restrict our attention to a set $\{ X_1, \dots, X_s \}$ that generate $\mathrm{End}_{\mathbb{K}G}(V)$.
Since $gXg^{-1} = X \iff gX^tg^{-1} = X^t$, we can further restrict to a set of matrices $X_1, \dots, X_s$ such that $\{ X_1, X_1^t, \dots, X_s, X_s^t \}$ generates $\mathrm{End}_{\mathbb{K}G}(V)$.

Furthermore: Every matrix $X \in \mathbb{K}^{\Omega\times\Omega}$ centralised by $g \in Sym(n)$ defines a collection of G-invariant, disjoint subsets $A_k := \{ (\alpha, \beta) \mid X_{\alpha\beta} = k \}$ for all $k \in \mathbb{K}$. Clearly X decomposes as the sum $\sum_{k\in\mathbb{K}} kX_{A_k}$ in this case and the non-zero summands are even linearly independent because they have disjoint support.

This suggest an algorithm that uses matrix calculations to refine a partition of Ω^2 into G-subsets the hopes of arriving at the orbit-partition at the end. If $\mathrm{Aut}(\Omega, \Gamma_1) \cap \dots \cap \mathrm{Aut}(\Omega, \Gamma_i)$ is already known, then $\mathrm{Aut}(\Omega, \Gamma_1) \cap \dots \cap \mathrm{Aut}(\Omega, \Gamma_i) \cap \mathrm{Aut}(\Omega, \Gamma_{i+1})$ can only be smaller if Γ_{i+1} is not already one of the parts of the partition that is defined by the $*$-algebra generated by $X_{\Gamma_1}, \dots, X_{\Gamma_i}$.

Algorithmus A1 (Computing the two-closure, version 1)**:**
The idea is to maintain a set of “important” orbitals and group the orbitals into two subsets

$$\Omega \times \Omega = \bigsqcup_{\Gamma\in\mathcal{A}} \Gamma \sqcup \bigsqcup_{\Gamma\in\mathcal{B}} \Gamma$$

such that $\mathcal{A}^{op} = \mathcal{A}$, $\mathcal{B}^{op} = \mathcal{B}$ and $\bigcap_{\Gamma \text{ important}} \mathrm{Aut}(\Omega, \Gamma) = \bigcap_{\Gamma\in\mathcal{A}} \mathrm{Aut}(\Omega, \Gamma)$ holds.

The algorithm works as follows:

1.) Initialise the two sets with $\mathcal{A} := \emptyset$ and $\mathcal{B}$ all orbitals. Initialise the set of important orbitals as the empty set.

2.) While $\mathcal{B} \neq \emptyset$ repeat:

   i.) Pick any $\Gamma \in \mathcal{B}$, move Γ and Γ^{op} from $\mathcal{B}$ into $\mathcal{A}$.

      a.) If $\mathcal{B}$ is now empty and $\Gamma = \Gamma^{op}$, then break out of the loop without doing anything else.

      b.) If $\mathcal{B}$ is now empty and $\Gamma \neq \Gamma^{op}$, then break out of the loop, but remember Γ as important.

c.) If $\mathcal{B}$ is still non-empty, then remember Γ as important and carry on with the next steps.

ii.) Set $\mathcal{C} := \emptyset$ and $\mathcal{C}' := \left\{ \Omega^2 \setminus \bigcup_{\Gamma \in \mathcal{A}} \Gamma \right\}$.

While $|\mathcal{C}| < |\mathcal{C}'|$ repeat

a.) Replace $\mathcal{C}$ by $\mathcal{C}'$.

b.) Compute the $\mathbb{K}$-algebra E generated by $\{ X_\Gamma, X_C \mid \Gamma \in \mathcal{A}, C \in \mathcal{C} \}$.

c.) Compute the coarsest partition $\mathcal{C}''$ of $\Omega^2 \setminus \left(\bigsqcup_{\Gamma \in \mathcal{A}} \Gamma \right)$ such that every $X \in E$ is in $\mathrm{span}_{\mathbb{K}} \{ X_\Gamma, X_{C''} \mid \Gamma \in \mathcal{A}, C'' \in \mathcal{C}'' \}$.

d.) Replace $\mathcal{C}'$ by $\mathcal{C}''$.

iii.) Move all Γ from $\mathcal{B}$ into $\mathcal{A}$ that are also parts of the partition $\mathcal{C}$, i.e. replace $(\mathcal{A}, \mathcal{B})$ by $(\mathcal{A} \cup (\mathcal{B} \cap \mathcal{C}), \mathcal{B} \setminus \mathcal{C})$.

3.) Compute $G^{(2)}$ as the intersection $\bigcap_{\Gamma \text{ important}} \mathrm{Aut}(\Omega, \Gamma)$.

3.11 Lemma: a.) Let $\Gamma \subseteq Q_1 \times Q_2$ if a G-orbital such that $\gcd(|Q_1|, |Q_2|) = 1$. Then $\Gamma = Q_1 \times Q_2$ and $\mathrm{Aut}(\Omega, \Gamma) = Sym(Q_1) \times Sym(Q_2) \times Sym(\Omega \setminus (Q_1 \cup Q_2))$.

In particular $(G_{|Q_1})^{(2)} \times (G_{|Q_2})^{(2)} \times Sym(\Omega \setminus (Q_1 \cup Q_2)) \leq \mathrm{Aut}(\Omega, \Gamma)$.

b.) $(G_{|Q})^{(2)} = \bigcap_{\substack{\Gamma \in Q^2/G \\ \Gamma \text{ non-diagonal}}} \mathrm{Aut}(Q, \Gamma)$

Algorithmus A2 (Computing the 2-closure, version II)**:**

3.2 Invariant subspaces and reconstruction problems

3.12 Theorem (2-closure in terms of invariant subspaces)**:**
Let $G \leq Sym(\Omega)$ be a permutation group and assume $\mathbb{K} = \mathbb{C}$. Then

$$G^{(2)} = \left\{ \pi \in Sym(\Omega) \;\middle|\; \forall U \leq \mathbb{C}^\Omega : U \ G\text{-invariant} \implies U \ \pi\text{-invariant} \right\}.$$

Proof. We consider the standard scalar product on V defined by declaring Ω to be an orthonormal basis so that V becomes a finite-dimensional Hilbert space.
Then all permutation matrices are unitary. In particular, $\mathrm{span}_{\mathbb{C}}(G) \subseteq \mathbb{C}^{\Omega \times \Omega}$ is closed under taking adjoints and its centraliser $\mathrm{End}_{\mathbb{C}G}(V)$ is also closed under taking adjoints. Both are therefore C^*-algebras. In particular, both are isomorphic to a direct product of matrix rings. It is a consequence of the spectral theorem that $\prod_i \mathbb{C}^{d_i \times d_i}$ is spanned by all the self-adjoint idempotents it contains.

Self-adjoint idempotent matrices correspond bijectively to subspaces by identifying U with the orthogonal projection p_U onto U. A subspace U is G-invariant if G centralises p_U. Therefore

$$\mathrm{End}_{\mathbb{C}G}(V) = \mathrm{span}_{\mathbb{C}}\left\{\, p_U \;\middle|\; U \leq \mathbb{C}^G \; G\text{-invariant} \,\right\}$$

and

$$G^{(2)} = Sym(\Omega) \cap C(\mathrm{End}_{\mathbb{C}G}(V)) = Sym(\Omega) \cap \bigcap_{\substack{U \leq V \\ G\text{-invariant}}} C(p_U)$$

which proves the claim. $\square$

3.13 Definition:
A permutation group $G \leq Sym(\Omega)$ is reconstructible from $\mathcal{X} \subseteq \mathrm{End}_{\mathbb{K}G}(V)$ if

$$G = Sym(\Omega) \cap \bigcap_{X \in \mathcal{X}} C(X).$$

Similarly, we define that G is ...

- ... orbital-graph-reconstructible if G is reconstructible from $\left\{\, X_\Gamma \;\middle|\; \Gamma \in \Omega^2/G \,\right\}$,
- ... strongly orbital-graph-reconstructible from $\Gamma \in \Omega^2/G$ iff it is reconstructible from X_Γ alone,
- ... absolutely orbital-graph-reconstructible iff it is strongly orbital-graph-reconstructible from any non-diagonal orbital $\Gamma \in \Omega^2/G$.
- ... subspace-reconstructible from $\mathcal{U}$, a set of G-invariant subspaces of V, if G is reconstructible from $\{\, p_U \mid U \in \mathcal{U} \,\}$.
- ... subspace-reconstructible over $\mathbb{K}$ if G is reconstructible from the set of all G-invariant subspaces of $\mathbb{K}^\Omega$.
- ... strongly subspace-reconstructible from $U \leq V$ if G is reconstructible from p_U alone,
- ... absolutely subspace-reconstructible over $\mathbb{K}$ if G is strongly subspace-reconstructible from any minimal, non-zero, G-invariant $U \leq \mathbb{K}^\Omega$ which is not $\mathrm{span}_{\mathbb{K}}\{\,(1,1,\ldots,1)\,\}$.

3.14 Corollary:
$G \leq Sym(\Omega)$ is 2-closed iff it is orbital-graph reconstructible iff it is subspace-reconstructible over $\mathbb{C}$.

Proof. The first equivalence follows from the fact that X_Γ is a basis of $\mathrm{End}_{\mathbb{C}G}(V)$. The second is a rephrasing of theorem 3.12. $\square$

3.15 Lemma (Subspace reconstructibility over $\mathbb{C}$ is sufficient)**:**
Let $\mathbb{K} = \mathbb{C}$ and $\mathcal{X} \subseteq \mathrm{End}_{\mathbb{C}G}(V)$ be arbitrary.
Then G is reconstructible from $\mathcal{X}$ iff it is subspace-reconstructible from

$$\{ \mathrm{Eig}_\lambda(\mathfrak{Re}(X)), \mathrm{Eig}_\lambda(\mathfrak{Im}(X)) \mid \lambda \in \mathbb{R}, X \in \mathcal{X} \}.$$

Proof. Permutation matrices are unitary. Therefore $g \in Sym(\Omega)$ centralises X iff it centralises X^*.
$\mathfrak{Re}(X) = \frac{1}{2}(X + X^*)$ and $\mathfrak{Im}(X) = \frac{1}{2i}(X - X^*)$ are self-adjoint matrices with $X = \mathfrak{Re}(X) + i\,\mathfrak{Im}(X)$ and for a self-adjoint matrices Y the spectral theorem shows

$$Y = \sum_{\lambda \in \mathbb{R}} \lambda e_\lambda$$

where $e_\lambda = p_{\mathrm{Eig}_\lambda(Y)}$ is the orthogonal projection onto the λ-eigenspace. Moreover e_λ is a polynomial of Y by Lagrange-interpolation.
Therefore if $g \in GL(V)$ commutes with Y it must commute with all e_λ and vice versa. Thus

$$C(X) = C(X, X^*) = C(\mathfrak{Re}(X), \mathfrak{Im}(X)) = \bigcap_{\lambda \in \mathbb{R}} C(p_{\mathrm{Eig}_\lambda(\mathfrak{Re}(X))}) \cap C(p_{\mathrm{Eig}_\lambda(\mathfrak{Im}(X))})$$

which proves the lemma. $\square$

3.16 Remark: One could use different matrices instead of $\mathfrak{Re}(X)$ and $\mathfrak{Im}(X)$. For example g centralises $X \in GL_n(\mathbb{C})$ iff it centralises the two factors in the polar decomposition $X = UP$ (i.e. U is unitary and P hermitian and positive definite) iff it stabilises their eigenspaces.

3.17 Corollary:
There is a single hermitian matrix $X \in \mathbb{Z}[i]^{\Omega \times \Omega}$ such that

$$G^{(2)} = Sym(n) \cap \bigcap \{ C(p_U) \mid \exists \lambda \in \mathbb{R} : U = Eig_\lambda(X) \}$$

Proof. Let $\Gamma_1, \ldots, \Gamma_s$ be all self-paired orbitals of G and $\Gamma_{s+1}, \ldots, \Gamma_{s+t}$ be such that $\Gamma_{s+1}, \Gamma_{s+1}^{op}, \ldots, \Gamma_{s+t}, \Gamma_{s+t}^{op}$ is a complete list of the non-self-paired orbitals.
Then set

$$X := \sum_{a=1}^{s} a X_{\Gamma_a} + \sum_{b=1}^{t} bi(X_{\Gamma_{s+b}} - X_{\Gamma_{s+b}^{op}})$$

and note that $gXg^{-1} = X \iff \forall \Gamma : gX_\Gamma g^{-1} = X_\Gamma \iff g \in C(\mathrm{End}_{\mathbb{C}G}(V))$. Therefore $G^{(2)}$ is reconstructible from X alone and the previous lemma shows it is reconstructible from the eigenspaces of X. $\square$

3.18 Theorem and definition (More about $\operatorname{End}_{\mathbb{K}G}(V)$ and the intersection algebra)**:** Assume $G \curvearrowright \Omega$ is transitive and $\operatorname{char}(\mathbb{K}) \nmid |G|$. Let $\Gamma_1, \ldots, \Gamma_r$ be a complete list of all orbitals, wlog starting with Γ_1 the diagonal, and let $1 = n_1, \ldots, n_r$ be the corresponding subdegrees, i.e. $n_i := \frac{|\Gamma_i|}{|\Omega|}$. Let $*$ be the permutation of $\{1, \ldots, r\}$ which satisfies $\Gamma_{i^*} = \Gamma_i^{op}$.

a.) $\operatorname{End}_{\mathbb{K}G}(V)$ is a symmetric algebra w.r.t. the trace map. $X_\Gamma^\vee := \frac{1}{|\Gamma|} X_\Gamma^T$ is the dual basis to X_Γ.

b.) The structure constants satisfy

i.) $\forall w, x, y, z \in \{1, \ldots, r\} : \sum_{t=1}^r d_{xt}^w d_{yz}^t = \sum_{t=1}^r d_{xy}^t d_{tz}^w$

ii.) $\forall i, j, k \in \{1, \ldots, r\} : d_{ij}^k = d_{j^* i^*}^{k^*}$.

iii.) $\forall i, j, k \in \{1, \ldots, r\} : n_k d_{ij}^k = n_i d_{kj^*}^i$

iv.) $\forall i, j \in \{1, \ldots, r\} : d_{ij}^1 = \begin{cases} n_i & \text{if } i = j^* \\ 0 & \text{otherwise} \end{cases}$.

c.) Define the matrices $D_k := (\delta_{ij}^k) \in \mathbb{K}^{r \times r}$ by $\delta_{ij}^k := \frac{n_k}{n_i} d_{ij^*}^k$.
With this notation $X_{\Gamma_k} \mapsto D_k$ is an embedding of $\mathbb{K}$-algebras. Its image is called the intersection algebra of V.

Proof. For brevity set $E := \operatorname{End}_{\mathbb{K}G}(V)$.
a. follows from direct computation:

$$\operatorname{tr}(X_\Gamma X_{\Gamma'}^T) = \sum_{\alpha,\beta \in \Omega} (X_\Gamma)_{\alpha\beta} (X_{\Gamma'}^T)_{\beta\alpha} = \sum_{\alpha,\beta} (X_\Gamma)_{\alpha\beta} (X_{\Gamma'})_{\alpha\beta} = \sum_{(\alpha,\beta) \in \Gamma \cap \Gamma'} 1$$

so that $\operatorname{tr}(X_\Gamma X_{\Gamma'}^T) = \begin{cases} |\Gamma| & \text{if } \Gamma' = \Gamma \\ 0 & \text{otherwise} \end{cases}$ which proves that the trace is non-degenerate on E.

b. The first equation is simply the associative law

$$(X_{\Gamma_x} X_{\Gamma_y}) X_{\Gamma_z} = X_{\Gamma_x} (X_{\Gamma_y} X_{\Gamma_z})$$

expanded in the basis X_{Γ_w}.
The second equation follows from the fact that $X \mapsto X^T$ is an anti-automorphism of E that maps X_{Γ_i} to $X_{\Gamma_{i^*}}$.

The third equation follows from a direct computation:

$$\begin{aligned}
d_{ij}^k &= \operatorname{tr}(X_i X_j \cdot X_k^\vee) \overset{a.}{=} \operatorname{tr}(X_i X_j \cdot \tfrac{1}{|\Gamma_k|} X_k^T) \\
&= \tfrac{1}{|\Gamma_k|} \operatorname{tr}(X_j X_k^T X_i) && \operatorname{tr}(AB) = \operatorname{tr}(BA) \\
&= \tfrac{1}{|\Gamma_k|} \operatorname{tr}(X_i^T X_k X_j^T) && \operatorname{tr}(A) = \operatorname{tr}(A^T) \\
&= \tfrac{1}{|\Gamma_k|} \operatorname{tr}(X_k X_j^T X_i^T) && \operatorname{tr}(AB) = \operatorname{tr}(BA) \\
&= \tfrac{|\Gamma_i|}{|\Gamma_k|} \operatorname{tr}(X_k X_{j^*} \cdot \tfrac{1}{|\Gamma_i|} X_i^T) \\
&\overset{a.}{=} \tfrac{|\Gamma_i|}{|\Gamma_k|} d_{kj^*}^i = \tfrac{n_i}{n_k} d_{kj^*}^i
\end{aligned}$$

Cancelling $|\Omega|$ and rearranging proves the third equation.
The fourth equation follows from $(\omega, \omega) \in \Gamma_1$ so that $d_{ij}^1 = |\{ \beta \in \Omega \mid (\omega, \beta) \in \Gamma_i \wedge (\beta, \omega) \in \Gamma_j \}| = \begin{cases} |\Gamma_j(\omega)| & \text{if } \Gamma_i = \Gamma_j^{op} \\ 0 & \text{otherwise} \end{cases} = \begin{cases} n_i & \text{if } i = j^* \\ 0 & \text{otherwise} \end{cases}$.

c. Consider the left regular representation of E, i.e. $\lambda : E \to \operatorname{End}_{\mathbb{K}}(E), x \mapsto (a \mapsto xa)$.
The definition of the structure constants

$$X_{\Gamma_k} X_{\Gamma_j} = \sum_i d_{kj}^i X_{\Gamma_k}$$

together with b.iii. show that D^k is exactly the matrix representing $\lambda(A_k)$ w.r.t. the basis $\{ X_{\Gamma_j} \}$. Therefore $X_{\Gamma_k} \mapsto D_k$ is nothing else than the left regular representation of E. It is therefore an injective algebra homomorphism. $\square$