Matrix representations

jason hanson *

1 Review of linear algebra

1.1 Matrix arithmetic and algebra

Definition 1. *A $m \times n$* **matrix** *is a function $A : \{1, \dots, m\} \times \{1, \dots, n\} \to \mathbb{R}$. We write $A_{ij} \doteq A(i, j)$ for $1 \leq i \leq m$ and $1 \leq j \leq n$.*

It is customary to represent a matrix as a $m \times n$ array of numbers. For example, if A is a 2×3 matrix, we would write

$$A = \begin{pmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \end{pmatrix}.$$

Thus if $A(i, j) \doteq 2i + j$, for $1 \leq i \leq 2$ and $1 \leq j \leq 3$, then $A = \left(\begin{smallmatrix} 3 & 4 & 5 \\ 5 & 6 & 7 \end{smallmatrix}\right)$.

Definition 2. *Suppose A, B are $m \times n$ matrices and $\alpha \in \mathbb{R}$. We define αA and $A + B$ to be the $m \times n$ matrices with*

$$(\alpha A)_{ij} \doteq \alpha A_{ij} \quad \text{and} \quad (A + B)_{ij} \doteq A_{ij} + B_{ij}$$

for $1 \leq i \leq m$ and $1 \leq j \leq n$. Moreover, if C is a $p \times q$ matrix and D is a $q \times r$ matrix, we define CD to be the $p \times r$ matrix with

$$(CD)_{ij} \doteq \sum_{k=1}^{q} C_{ik} D_{kj}.$$

As an example of *scalar multiplication:* $3\left(\begin{smallmatrix} 1 & 0 & 2 \\ 3 & 2 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 3 & 0 & 6 \\ 9 & 6 & 3 \end{smallmatrix}\right)$. For *matrix addition:* $\left(\begin{smallmatrix} 1 & 2 & 1 \\ 0 & 5 & 1 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 2 & 0 & 1 \\ 2 & 1 & 3 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 3 & 2 & 2 \\ 2 & 6 & 4 \end{smallmatrix}\right)$. And for *matrix multiplication:* $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 & 3 \\ 0 & 2 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 2 & 2 & 7 \\ 1 & 2 & 4 \end{smallmatrix}\right)$.

Exercise 1. *Show that for all $\alpha \in \mathbb{R}$, and all $m \times n$ matrices A, B, we have $\alpha(A+B) = \alpha A + \alpha B$. Moreover if C is a $k \times m$ matrix and D is a $n \times p$ matrix, then $C(A+B) = CA + CB$, $(A+B)D = AD + BD$, and $C(BD) = (CB)D$.*

Exercise 2. *Show that the set of all $m \times n$ matrices forms a group under addition. The additive identity in this case is the* zero matrix*: the $m \times n$ matrix whose elements are all zero, and the (additive) inverse of a matrix A is its* negation*: $-A \doteq (-1)A$.*

1.2 Invertibility

The *Kronecker delta* is defined by $\delta_{ij} \doteq 0$ if $i \neq j$, and $\delta_{ii} \doteq 1$, for all integers i, j. With this definition in mind, we define the $n \times n$ *(multiplicative) identity matrix* to be the matrix I, with $I_{ij} = \delta_{ij}$, where $1 \leq i \leq n$ and $1 \leq j \leq n$. E.g., the 2×2 identity matrix is $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

Exercise 3. *Show that for all $m \times n$ matrices A and all $n \times m$ matrices B, we have $AI = A$ and $IB = B$.*

Definition 3. *The $n \times n$ matrix A is* **invertible** *if there exists a $n \times n$ matrix B such that $AB = BA = I$; and in this case we write $A^{-1} \doteq B$. The collection of all $n \times n$ invertible matrices is called the* **general linear group** *of dimension n, and is denoted by* $\mathrm{GL}_n\mathbb{R}$.

Exercise 4. *Suppose A, B, C are $n \times n$ matrices with $AB = I$ and $CA = I$. Show that $B = C$, and hence that A is invertible.*

It follows that the inverse of a matrix is unique. Indeed, if $AB = BA = I$ and $AC = CA = I$, then $B = BI = B(AC) = (BA)C = IC = C$. So the notation A^{-1} for the inverse of a matrix is unambiguous.

Exercise 5. *Show that* $\mathrm{GL}_n\mathbb{R}$ *is a group under matrix multiplication.*

Exercise 6. *Show that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is invertible if and only if $ad - bc \neq 0$, in which case the inverse is given by $\frac{1}{ad-bc}\left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$.*

Thus $\left(\begin{smallmatrix} 1 & 0 \\ 2 & 0 \end{smallmatrix}\right)$ is not invertible, and so is not an element of $\mathrm{GL}_2\mathbb{R}$. On the other hand, we compute that $\left(\begin{smallmatrix} 1 & 2 \\ 2 & 5 \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} 5 & -2 \\ -2 & 1 \end{smallmatrix}\right)$, so that $\left(\begin{smallmatrix} 1 & 2 \\ 2 & 5 \end{smallmatrix}\right) \in \mathrm{GL}_2\mathbb{R}$ (as well as its inverse).

1.3 Linear maps

Recall that *n–dimensional space* $\mathbb{R}^n$ is the set of all n–tuples $(x_1, \ldots, x_n)$ of real numbers. We may identify elements of $\mathbb{R}^n$ with $n \times 1$ matrices via the prescription

$$(x_1, \ldots, x_n) \mapsto \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Elements $\mathbf{x} \in \mathbb{R}^n$ are called *vectors*; and when we wish to invoke the identification of $\mathbb{R}^n$ with $n \times 1$ matrices, we call $\mathbf{x}$ a *column vector*. Under this identification, we may multiply a vector by a scalar, and we may add two vectors together.

The *standard basis* of $\mathbb{R}^n$ is the collection of vectors $\mathbf{e}_1, \ldots, \mathbf{e}_n$ in $\mathbb{R}^n$, where $\mathbf{e}_j$ is the vector whose k–th component is δ_{jk}. E.g., in $\mathbb{R}^3$, $\mathbf{e}_1 = (1, 0, 0)$, $\mathbf{e}_2 = (0, 1, 0)$, and $\mathbf{e}_3 = (0, 0, 1)$. Every vector in $\mathbb{R}^n$ can be uniquely written as a linear combination of standard basis vectors: if $\mathbf{x} = (x_1, \ldots, x_n)$, then $\mathbf{x} = \sum_{j=1}^n x_j \mathbf{e}_j$.

Definition 4. *A map $\mathbb{R}^n \to \mathbb{R}^m$ is* **linear** *if $f(\alpha\mathbf{x} + \beta\mathbf{y}) = \alpha f(\mathbf{x}) + \beta f(\mathbf{y})$ for all $\alpha \in \mathbb{R}$ and $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$. The* **matrix of** *$f$ is the $m \times n$ matrix M such that $f(\mathbf{e}_i) = \sum_{j=1}^m M_{ji} \mathbf{e}_j$, for $1 \leq i \leq n$.*

For example, consider the map $g : \mathbb{R}^2 \to \mathbb{R}^2$ given by the rule $g(x_1, x_2) \doteq (x_1 + 2x_2, 3x_1 + 4x_2)$. The reader will verify that g is a linear map, and that the matrix of g is given by $M = \left(\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right)$.

Exercise 7. *Suppose M is the matrix of the linear map f. Show that as a column vector, $f(\mathbf{x}) = M\mathbf{x}$ (matrix multiplication).*

Exercise 8. *If A is a $m \times n$ matrix, show that A defines a linear map $g : \mathbb{R}^n \to \mathbb{R}^m$ by $g(x_1, \ldots, x_n) \doteq \sum_{j=1}^m (\sum_{k=1}^n A_{jk} x_k) \mathbf{e}_j$.*

1.4 Change of basis

Definition 5. *A* **basis** *of $\mathbb{R}^n$ is a collection of exactly n vectors $\mathbf{u}_1, \ldots, \mathbf{u}_n$ such that every $\mathbf{x} \in \mathbb{R}^n$ can be expressed as a linear combination of these vectors: $\mathbf{x} = \sum_{j=1}^n \alpha_j \mathbf{u}_j$, where $\alpha_j \in \mathbb{R}$.*

The reader will readily verify that the standard basis $\mathbf{e}_1, \ldots, \mathbf{e}_n$ is indeed a basis (hence its name).

Exercise 9. *Show that* $\mathbf{u}_1, \ldots, \mathbf{u}_n$ *is a basis of* $\mathbb{R}^n$ *if and only if the equation* $\sum_{j=1}^n \beta_j \mathbf{u}_j = \mathbf{0}$*, where* $\beta_j \in \mathbb{R}$*, has* $\beta_1 = \cdots = \beta_n = 0$ *as the only solution.*

Exercise 10. *Show that in the decomposition* $\mathbf{x} = \sum_{j=1}^n \alpha_j \mathbf{u}_j$*, the coefficients* α_j *are unique.*

Given a basis $\mathbf{u}_1, \ldots, \mathbf{u}_n$ of $\mathbb{R}^n$, we may define a $n \times n$ matrix B, whose components B_{ij} are given by the equation $\mathbf{u}_j = \sum_{i=1}^n B_{ij}\mathbf{e}_i$; i.e., B_{ij} is the i–th component of the vector $\mathbf{u}_j$. We call B the **change of basis matrix** that takes us from the standard basis $\mathbf{e}_1, \ldots, \mathbf{e}_n$ to the basis $\mathbf{u}_1, \ldots, \mathbf{u}_n$.

Exercise 11. *Let* A *be the* $n \times n$ *matrix whose components are (uniquely) defined by the equation* $\mathbf{e}_j = \sum_{i=1}^n A_{ij}\mathbf{u}_i$*. Show that* $AB = I$ *and* $BA = I$*.*

It follows that the change of basis matrix B is invertible.

Let us now see how the matrix of a linear map changes when we make a change of basis. We are given a linear map $f : \mathbb{R}^n \to \mathbb{R}^m$ with corresponding $m \times n$ matrix M, in terms of the standard basis; i.e., $f(\mathbf{e}_i) = \sum_{j=1}^m M_{ji}\mathbf{e}_j$, for $1 \leq i \leq n$. Suppose that $\mathbf{u}_1, \ldots, \mathbf{u}_n$ is a basis for $\mathbb{R}^n$ with change of basis matrix B (a $n \times n$ matrix), and that $\mathbf{v}_1, \ldots, \mathbf{v}_m$ is a basis for $\mathbb{R}^m$ with change of basis matrix C (a $m \times m$ matrix). We wish to find the $m \times n$ matrix M' for which $f(\mathbf{u}_i) = \sum_{j=1}^m M'_{ji}\mathbf{v}_j$, for $1 \leq i \leq n$.

Exercise 12. *Show that* $M' = C^{-1}MB$*.*

In particular, for an *endomorphism* of $\mathbb{R}^n$, that is a linear map $f : \mathbb{R}^n \to \mathbb{R}^n$ (in other words, in the case $m = n$, and $\mathbf{v}_i = \mathbf{u}_i$), we have that $M' = B^{-1}MB$. The matrix $B^{-1}MB$ is sometimes called the *conjugate* of M by B; so a change of basis corresponds to conjugation by the change of basis matrix.

1.5 Direct sums

The Cartesian product $\mathbb{R}^p \times \mathbb{R}^q$ consists of ordered pairs of the form $(\mathbf{x}, \mathbf{y})$, where $\mathbf{x} = (x_1, \ldots, x_p)$ and $\mathbf{y} = (y_1, \ldots, y_q)$. Such an ordered pair can be identified with the $(p+q)$–tuple $(x_1, \ldots, x_p, y_1, \ldots, y_q)$; i.e., with an element of $\mathbb{R}^{p+q}$. We make this identification into a formal definition.

Definition 6. *The* **direct sum** *of* $\mathbb{R}^p$ *and* $\mathbb{R}^q$ *is* $\mathbb{R}^p \oplus \mathbb{R}^q \doteq \mathbb{R}^{p+q}$*. Elements of* $\mathbb{R}^p \oplus \mathbb{R}^q$ *are written in the form* $\mathbf{x} \oplus \mathbf{y}$*, where* $\mathbf{x} \in \mathbb{R}^p$ *and* $\mathbf{y} \in \mathbb{R}^p$*.*

That is, $\mathbf{x} \oplus \mathbf{y} = (x_1, \ldots, x_p, y_1, \ldots, y_q)$. It is convenient to let $\mathbf{0}_p$ denote the zero vector in $\mathbb{R}^p$. Thus the zero vector in $\mathbb{R}^p \oplus \mathbb{R}^q$ is $\mathbf{0}_p \oplus \mathbf{0}_q$.

Exercise 13. *Show that if $\mathbf{u}_1, \ldots, \mathbf{u}_p$ is a basis for $\mathbb{R}^p$ and $\mathbf{v}_1, \ldots, \mathbf{v}_q$ is a basis for $\mathbb{R}^q$, then $\mathbf{u}_1 \oplus \mathbf{0}_q, \ldots, \mathbf{u}_p \oplus \mathbf{0}_q$, $\mathbf{0}_p \oplus \mathbf{v}_1, \ldots, \mathbf{0}_p \oplus \mathbf{v}_q$ is a basis for $\mathbb{R}^p \oplus \mathbb{R}^q$.*

Definition 7. *Let $f : \mathbb{R}^n \to \mathbb{R}^m$ and $g : \mathbb{R}^t \to \mathbb{R}^s$ be linear maps. We define $f \oplus g : \mathbb{R}^n \oplus \mathbb{R}^t \to \mathbb{R}^m \oplus \mathbb{R}^s$ by $(f \oplus g)(\mathbf{x} \oplus \mathbf{y}) \doteq f(\mathbf{x}) \oplus g(\mathbf{y})$.*

The matrix of the direct sum of two linear maps is a matrix in *block diagonal* form. Specifically, if A is the $m \times n$ matrix of f, and B is the $s \times t$ matrix of g, then

$$A \oplus B = \begin{pmatrix} A & 0_{mt} \\ 0_{sn} & B \end{pmatrix}$$

is the $(m+s) \times (n+t)$ matrix of $f \oplus g$, where 0_{sn} denotes the $s \times n$ matrix of zeros. Such a matrix is called a *block diagonal* matrix. For example, if $A = \left(\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 5 & 6 \end{smallmatrix}\right)$, then $A \oplus B = \left(\begin{smallmatrix} 1 & 2 & 0 & 0 \\ 3 & 4 & 0 & 0 \\ 0 & 0 & 5 & 6 \end{smallmatrix}\right)$.

1.6 Inner product

Definition 8. *The* **inner product** *of $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$ is $\mathbf{u} \cdot \mathbf{v} \doteq \sum_{j=1}^n u_j v_j$, where $\mathbf{u} = (u_1, \ldots, u_n)$ and $\mathbf{v} = (v_1, \ldots, v_n)$. The vectors $\mathbf{u}, \mathbf{v}$ are* **orthogonal** *if $\mathbf{u} \cdot \mathbf{v} = 0$. The* **length** *of $\mathbf{u}$ is $|\mathbf{u}| \doteq \sqrt{\mathbf{u} \cdot \mathbf{v}}$.*

Exercise 14. *Show that the inner product is symmetric and linear each argument: (i) $\mathbf{u} \cdot \mathbf{v} = \mathbf{v} \cdot \mathbf{u}$, (ii) $(\alpha\mathbf{u} + \beta\mathbf{u}') \cdot \mathbf{v} = \alpha(\mathbf{u} \cdot \mathbf{v}) + \beta(\mathbf{u}' \cdot \mathbf{v})$, and (iii) $\mathbf{u} \cdot (\alpha\mathbf{v} + \beta\mathbf{v}') = \alpha(\mathbf{u} \cdot \mathbf{v}) + \beta(\mathbf{u} \cdot \mathbf{v}')$.*

Definition 9. *The* **transpose** *of a $m \times n$ matrix A is the $n \times m$ matrix A^T with $(A^T)_{ij} \doteq A_{ji}$. If $f : \mathbb{R}^n \to \mathbb{R}^m$ is a linear map with matrix A, then the* **adjoint** *of f is the linear map $f^T : \mathbb{R}^m \to \mathbb{R}^n$ whose matrix is A^T.*

Exercise 15. *Show that as column vectors $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$, $\mathbf{u} \cdot \mathbf{v} = \mathbf{u}^T\mathbf{v}$.*

Exercise 16. *Let $g : \mathbb{R}^m \to \mathbb{R}^n$ be a linear map. Show that $f(\mathbf{u}) \cdot \mathbf{v} = \mathbf{u} \cdot g(\mathbf{v})$ for all $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$ if and only if $g = f^T$.*

That is, $f(\mathbf{u}) \cdot \mathbf{v} = \mathbf{u} \cdot f^T(\mathbf{v})$ for all $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$, and this equation uniquely defines the adjoint f^T of f.

Definition 10. *A linear map $f : \mathbb{R}^n \to \mathbb{R}^n$ is* **orthogonal** *if $f(\mathbf{u}) \cdot f(\mathbf{v}) = \mathbf{u} \cdot \mathbf{v}$ for all $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$. A matrix A is* **orthogonal** *if $A^T A = AA^T = I$.*

In particular, an orthogonal map preserves length: $|f(\mathbf{u})| = |\mathbf{u}|$. Note that an orthogonal matrix is necessarily invertible.

Exercise 17. *Show that f is orthogonal if and only if the matrix of f is orthogonal.*

Exercise 18. *Show that f is orthogonal if and only if preserves length.*

2 Linear representations

As we have mentioned, the general linear group $\mathrm{GL}_n\mathbb{R}$, which is the set of all invertible $n \times n$ matrices, is a group under matrix multiplication; the identity is the $n \times n$ identity matrix I.

Definition 11. *A* **(linear) representation** *of the group G is a group homomorphism $\rho : G \to \mathrm{GL}_n\mathbb{R}$; the* **dimension** *of the representation is n. If $\rho(g)$ is an orthogonal matrix for each $g \in G$, then ρ is said to be an* **orthogonal representation**.

That is, for each group element g, we assign to it a matrix $\rho(g)$, and for any $g_1, g_2 \in G$, $\rho(g_1 g_2) = \rho(g_1)\rho(g_2)$. In other words, multiplication in G exactly corresponds under ρ to matrix multiplication. Observe that we must have $\rho(e) = I$.

As an example, consider the cyclic group with four elements: $C_4 = \langle \gamma \mid \gamma^4 = e \rangle = \{e, \gamma, \gamma^2, \gamma^3\}$. Define the map $\rho : C_4 \to \mathrm{GL}_2\mathbb{R}$ by

$$\rho(e) \doteq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \rho(\gamma) \doteq \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \rho(\gamma^2) \doteq \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \rho(\gamma^3) \doteq \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

One verifies that ρ is a homomorphism. Indeed, $\rho(\gamma)^4 = I$, and $\rho(\gamma^k) = \rho(\gamma)^k$ for $k = 1, 2, 3$. In fact, ρ is seen to to be an orthogonal representation of C_4 of dimension 2. Geometrically, the matrix $\rho(\gamma)$ rotates a vector $\mathbf{u}$ by 90° clockwise about the origin.

Exercise 19. *Suppose $\rho : G \to \mathrm{GL}_n\mathbb{R}$ is a linear representation and $M \in \mathrm{GL}_n\mathbb{R}$. Define $\rho^M : G \to \mathrm{GL}_n\mathbb{R}$ by $\rho^M(g) \doteq M\rho(g)M^{-1}$. Show that ρ^M is a linear representation of G.*

Exercise 20. *Show that if $\rho : G \to \mathrm{GL}_n\mathbb{R}$ is an orthogonal representation and M is an orthogonal matrix, then ρ^M is an orthogonal representation.*

We have seen that conjugation by an invertible matrix corresponds to a change of basis. Thus the matrix $\rho^M(g)$ defines the same linear map as $\rho(g)$, but under a change of basis. For this reason, we will view the representations ρ and ρ^M as essentially defining the same representation.

Definition 12. *Two linear representations $\rho, \sigma : G \to \mathrm{GL}_n\mathbb{R}$ are* **isomorphic** *if $\sigma = \rho^M$ for some $M \in \mathrm{GL}_n\mathbb{R}$. In this case we write $\rho \cong \sigma$.*

For example, the previous (orthogonal) representation ρ of C_4 is isomorphic to the representation $\sigma : C_4 \to \mathrm{GL}_2\mathbb{R}$, where

$$\sigma(e) = I, \sigma(\gamma) \doteq \begin{pmatrix} -3 & 5 \\ -2 & 3 \end{pmatrix}, \sigma(\gamma^2) \doteq \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \sigma(\gamma^3) \doteq \begin{pmatrix} 3 & -5 \\ 2 & -3 \end{pmatrix}.$$

Indeed $\sigma = \rho^M$, where $M = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)$. Note however that σ is not orthogonal (since M is not).

3 Irreducibility

Definition 13. *The* **direct sum** *of linear representations $\sigma : G \to \mathrm{GL}_p\mathbb{R}$ and $\tau : G \to \mathrm{GL}_q\mathbb{R}$ is the linear representation $\sigma \oplus \tau : G \to \mathrm{GL}_{p+q}\mathbb{R}$ defined by $(\sigma \oplus \tau)(g) \doteq \sigma(g) \oplus \tau(g)$. A linear representation is* **reducible** *if is isomorphic to a direct sum of linear representations of positive dimension. A linear representation that is is not reducible is said to be* **irreducible**.

Exercise 21. *Show that the representation ρ of C_4 given in the previous section is irreducible.*

There are two special representations that may be defined for any finite group G. The *trivial representation* $\tau : G \to \mathrm{GL}_1\mathbb{R}$ is the linear representations defined by $\tau(g) \doteq 1$ for all $g \in G$ (note that $\mathrm{GL}_1\mathbb{R}$ is the group of nonzero real numbers). Since this representation is one–dimensional, it is necessarily irreducible.

We also have the *regular representation* $r : G \to \mathrm{GL}_n\mathbb{R}$, where n is the size of G, which is constructed as follows. Choose a bijection $\epsilon : \{1, \ldots, n\} \to G$. We then define $r(g)$ to be the matrix of the linear map defined by the

requirement $r(g)(\mathbf{e}_i) \doteq \mathbf{e}_{\epsilon^{-1}(g\epsilon(i))}$ for $1 \leq i \leq n$. I.e., g will permute the indices of the standard basis vectors $\mathbf{e}_1, \ldots, \mathbf{e}_n$.

For example, let $\epsilon : \{1,2,3,4\} \to C_4$ be the map $\epsilon(i) \doteq \gamma^i$ (so that $\epsilon(4) = \gamma^4 = e$). Then $r(\gamma)(\mathbf{e}_1) = \mathbf{e}_2$, since $\epsilon^{-1}(\gamma\epsilon(1)) = \epsilon^{-1}(\gamma^2) = 2$. Likewise, $r(\gamma)(\mathbf{e}_2) = \mathbf{e}_3$, $r(\gamma)(\mathbf{e}_3) = \mathbf{e}_4$, and $r(\gamma)(\mathbf{e}_4) = \mathbf{e}_1$. Similar computations are made for $r(\gamma^2)$ and $r(\gamma^3)$. It follows that $r(e) = I$, and

$$r(\gamma) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, r(\gamma^2) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, r(\gamma^3) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Note that $r(\gamma^k) = r(\gamma)^k$, so that r is indeed a linear representation.

Exercise 22. *Prove that the regular representation of a group G is an orthogonal linear representation.*

Exercise 23. *Show that the trivial representation is a summand of the regular representation: $r \cong \tau \oplus \sigma$ for some linear representation σ.*

Although it is beyond the scope of these notes, it can be shown that for a given group G, there exists only a finite collection of irreducible nonisomorphic linear representations of G, say $\rho_1, \ldots, \rho_n$. In fact, every irreducible linear representation is a summand of the regular representation. Moreover, every linear representation ρ of G is isomorphic to a direct sum of these irreducible representations: $\rho \cong \rho^{m_1} \oplus \cdots \oplus \rho^{m_n}$, where m_j is the multiplicity of ρ_j: $\rho_j^{m_j} \doteq \rho_j \oplus \cdots \oplus \rho_j$ (m_j summands). This decomposition into irreducibles is unique up to isomorphism and reordering of summands.

As an example, consider the regular representation of C_4 given above. By making a change of basis, the representation can be put into block diagonal form. Indeed,

$$r^M(\gamma) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \quad \text{where} \quad M = \tfrac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{pmatrix}.$$

I.e., $r^M(\gamma) = (1) \oplus \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \oplus (-1)$. Thus, $r^M = \tau \oplus \rho \oplus \mu$, where τ is the trivial representation, ρ is the irreducible two–dimensional representation of C_4 given in the previous section, and μ is the non–trivial irreducible one–dimensional representation given by $\mu(e) \doteq 1$, $\mu(\gamma) \doteq -1$, $\mu(\gamma^2) = 1$, and $\mu(\gamma^3) \doteq 1$.

Definition 14. *A linear representation* $\rho : G \to \mathrm{GL}_n\mathbb{R}$ *is* **faithful** *if it is injective.*

The one–dimensional representations τ and μ of C_4 are not faithful, since $\tau(\gamma) = \tau(e) = 1$, and $\mu(\gamma^2) = \mu(e) = 1$. However, the two–dimensional representation ρ is faithful.

Exercise 24. *The* kernel *of a group homomorphism* $\eta : G \to G'$ *is the set of all elements in* G *that map to the identity in* G'*:* $\ker(\eta) \doteq \{g \mid \eta(g) = e\}$*. Show that* ρ *is faithful if and only if* $\ker(\rho) = \{e\}$*.*

4 References

- *Linear representations of finite groups*, fourth edition, by J. P. Serre; published by Springer–Verlag, 1987; ISBN: 0387901906
- *Matrix groups*, second edition, by Morton Curtis; published by Springer–Verlag, 1984; ISBN: 0387960740.