LINEAR ALGEBRA AND GROUP THEORY

TEO BANICA

ABSTRACT. This is an introduction to linear algebra and group theory. We first present the key concepts and results of linear algebra and matrix theory, namely the determinant, the diagonalization procedure, and more. We discuss then the structure of the various groups of matrices $G \subset U_N$, with algebraic and probabilistic results.

CONTENTS

2010 *Mathematics Subject Classification.* 15A03.
Key words and phrases. Complex matrix, Unitary group.

Introduction

Linear algebra is concerned with the study of arrays of numbers, also called matrices. Here is well-known example of such a matrix, depending on a number $t \in \mathbb{R}$:

$$R_t = \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix}$$

In case you do not know about R_t, here is the thing. The idea is that the points in the plane $\mathbb{R}^2$ can be represented as vectors $\binom{x}{y}$, with $x \in \mathbb{R}$ standing for the horizontal coordinate, and $y \in \mathbb{R}$ standing for the vertical coordinate.

The point now is that the various 2×2 matrices, such as the above one, "act" on such vectors, according to the following formula:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$$

So, let us try now to see if a very basic action that we know, namely the counterclockwise rotation of angle $t \in \mathbb{R}$, can be expressed in this way. We will see that this is indeed the case, and that the matrix of this rotation is precisely the above matrix R_t.

It is easy to get lost into computations here, and the trick is to "guess" the associated matrix, via its action on the basic coordinate vectors $\binom{1}{0}$ and $\binom{0}{1}$.

To be more precise, a quick picture shows that we must have:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos t \\ \sin t \end{pmatrix}$$

Also, by paying attention to positives and negatives, we must have:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -\sin t \\ \cos t \end{pmatrix}$$

Guessing now the matrix is not complicated, because the first equation gives us in fact the first column, $\binom{a}{c}$, and the second equation gives us the second column, $\binom{b}{d}$.

Thus, we can just put together the two vectors that we found, and we obtain our matrix. To be more precise, we obtain the matrix R_t from the beginning, namely:

$$R_t = \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix}$$

Summarizing, we have here some good evidence for the fact that the rotation of angle $t \in \mathbb{R}$ should appear by making this matrix R_t act on the vectors $\binom{x}{y} \in \mathbb{R}^2$.

All this is quite satisfactory, but if we have a potential application in mind, say of engineering type, we must be rock-solid sure about our finding. To be more precise, it remains to check that our matrix R_t rotates in a correct way any vector $\binom{x}{y}$.

This can be done with some trigonometric computations, which are not exactly of trivial type. Fortunately, there is a much simpler way of doing this. Indeed, the rotation of angle t is obviously "linear", in the sense that it maps straight lines into straight lines. And, the main theorem in linear algebra, assuming that you know it already, tells you that linear maps must come from matrices. Thus, with some theory, we are done.

In case you do not know about this theorem, the present book is here for that. We will discuss the basic concepts and results of linear algebra, and with all this knowledge, playing with 2×2 matrices will become as easy as playing with real numbers.

Let us discuss now more advanced aspects, in 3 dimensions.

This is of course the case that we are really interested in, because this is where real life happens. As a first example here, whenever you play a video game on your computer, there are 3D rotations there, in the software, which move your objects.

It goes the same with cars, buildings, and any kind of machinery.

Finding formulae for the rotations in $\mathbb{R}^3$, and any other kind of linear maps that you might need, is not an easy task, and even professionals have big troubles with this.

As an example here, let us take a "random" 3×3 matrix, say:

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 7 & 5 & 4 \\ 1 & 3 & 1 \end{pmatrix}$$

According to the general theory, this matrix produces a linear map $\mathbb{R}^3 \to \mathbb{R}^3$, given by a formula of type $v \to Av$, a bit like in the 2-dimensional case. But, can you visualise this map? Probably not, and this is not surprising: nobody can.

In order to solve this difficulty, let us go back to 2 dimensions, and try to reach to a better level there. With a bit of luck, the new knowledge will apply to 3D as well.

As a first remark, it is better to use complex numbers. Indeed, when thinking of $\mathbb{R}^2$ as being the complex plane $\mathbb{C}$, the formula of the rotation is simply:

$$z \to e^{it} z$$

Thus, we have the following alternative formula for R_t, or rather for the rotation of angle t, regarded now as a 1×1 complex matrix:

$$R_t = (e^{it})$$

Obviously, some magics is going on here. This is actually often the case with the complex numbers, which are quite a tricky thing.

The point now is that we can put on top of this a second remark, which is conceptual as well. The idea indeed is that the rotations can be composed – an operation which is very useful, in practice – and so they form a mathematical object $(G, \cdot)$ called group. Thus, our passage from real to complex corresponds to a certain group equality.

In technical terms, the formula is as follows, with SO_2 standing for "special orthogonal group in 2 dimensions" and with U_1 standing for "unitary group in 1 dimension":

$$SO_2 = U_1$$

This looks very nice and conceptual, and will be our final saying on the subject.

Getting back now to $\mathbb{R}^3$, what we would like to have is a formula for the elements of SO_3. As already explained, there is no hope for that, with bare hands.

However, with some group theory knowledge, that we will explain as well in this book, we can construct a quotient map as follows:

$$SU_2 \to SO_3$$

Thus, in order to solve our problem, it is enough to compute the elements of the group SU_2, and then apply our quotient map.

The computation for SU_2 cannot be difficult, because we are dealing after all with 2×2 matrices. With some knowledge here, the equation for our matrices is:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \bar{d} & -\bar{c} \\ -\bar{b} & \bar{a} \end{pmatrix}$$

Thus, we obtain the following formula for our group:

$$SU_2 = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \;\middle|\; |a|^2 + |b|^2 = 1 \right\}$$

With $a = x + iy$ and $b = z + it$ we have the following alternative formula:

$$SU_2 = \left\{ \begin{pmatrix} x + iy & z + it \\ -z + it & x - iy \end{pmatrix} \;\middle|\; x^2 + y^2 + z^2 + t^2 = 1 \right\}$$

This latter formula is very nice, because the parameters (x, y, z, t) range now over the sphere of space-time. We are probably doing some physics here.

Now by applying the above-mentioned quotient map $SU_2 \to SO_3$, we are led to the following formula, for the arbitrary elements $U \in SO_3$:

$$U = \begin{pmatrix} x^2 + y^2 - z^2 - t^2 & 2(yz - xt) & 2(xz + yt) \\ 2(xt + yz) & x^2 + z^2 - y^2 - t^2 & 2(zt - xy) \\ 2(yt - xz) & 2(xy + zt) & x^2 + t^2 - y^2 - z^2 \end{pmatrix}$$

In short, we are now ready to write 3D game software, or do some engineering.

Even more technically now, for certain applications, especially the "quantum" ones, using rotations "at random" is very useful, provided that we can average them.

We are led in this way to the following kind of questions, of analytic and probabilistic flavor, regarding the various subgroups $G_N \subset U_N$, finite or continuous:

$$\int_{G_N} Tr(U)^k \, dU = ?$$

Even more generally, we are led to general questions of the following type:

$$\int_{G_N} U_{i_1 j_1} \ldots U_{i_k j_k} \, dU = ?$$

The answer here is not trivial, depending on G_N, and involves a lot of interesting mathematics, that we will explain as well, as a final topic of this book.

Let us briefly discuss now, as an introduction to these latter topics, some computations for one of the simplest groups around, namely the symmetric group S_N.

The symmetric group S_N consists by definition of the permutations of a set having N elements, with the composition of the permutations being the group operation:

$$\sigma : \{1, \ldots, N\} \to \{1, \ldots, N\}$$

As a first observation, there are $N!$ such permutations. Indeed, when trying to construct such a permutation $\sigma \in S_N$, the situation is as follows:

– There are N choices for $\sigma(1)$.

– Then, there are $N - 1$ choices for $\sigma(2)$.

– Then, there are $N - 2$ choices for $\sigma(3)$.

$\vdots$

– And so, on up to 2 choices for $\sigma(N - 1)$.

– And we have as well 1 final choice for $\sigma(N)$.

Thus, we have a total of $1 \cdot 2 \ldots (N - 2)(N - 1)N = N!$ choices for our permutation $\sigma \in S_N$, and so the number of elements of S_N follows to be $N!$.

In relation now with our linear algebra questions, the permutations $\sigma \in S_N$ can be thought of as permuting the N coordinate axes of $\mathbb{R}^N$. In abstract terms, we have:

$$S_N \subset O_N$$

To be more precise, the $N \times N$ matrix associated to a permutation $\sigma \in S_N$ is the one having a 1 entry at row $\sigma(i)$ and column i, for any i, and 0 entries elsewhere.

Now let us look at the trace, or sum of diagonal entries, of such a permutation matrix. Since the nonzero diagonal entries come from fixed points, we have:

$$Tr(\sigma) = \#\left\{i \in \{1, \ldots, N\} \middle| \sigma(i) = i\right\}$$

In other words, the conclusion is that the trace of the permutation matrices counts the number of fixed points of the corresponding permutations.

A first question now is that of counting the permutations $\sigma \in S_N$ having no fixed point at all, called derangements. This can be done by a standard method, namely the inclusion-exclusion principle, and we obtain the following number:

$$X = N! - \frac{N!}{1} + \frac{N!}{2} - \frac{N!}{6} + \ldots + (-1)^N \frac{N!}{N!}$$

This looks better if we divide by $N!$. We are led in this way into probability, with the conclusion that the probability for a random $\sigma \in S_N$ to have no fixed points is:

$$P \simeq \frac{1}{e}$$

Now back permutation matrices and their traces, the conclusion is that the equality $Tr = 0$ happens with probability $1/e$, in the $N \to \infty$ limit.

The next question is that of computing the probability for $Tr = k$ to happen, with $k \in \mathbb{N}$ being arbitrary. The answer here, once again obtained via the inclusion-exclusion principle, as a generalization of the above $k = 0$ computation, is as follows:

$$P(Tr = k) \simeq \frac{1}{ek!}$$

In technical terms, the conclusion is that $Tr : S_N \to \mathbb{N}$ becomes Poisson (1), in the $N \to \infty$ limit. This was our first theorem, and many other to follow, in this book.

The present book is organized in 4 parts, as follows:

(1) In sections 1-4 we present the basic concepts and results of linear algebra. The main topics here are the determinant, and the diagonalization procedure.

(2) In sections 5-8 we discuss more advanced aspects, namely applications to analysis, basic spectral theory, and further linear algebra techniques.

(3) In sections 9-12 we review the basic group theory, finite and continuous, and then we start doing some probability computations, in the finite group case.

(4) In sections 13-16 we discuss the structure of the continuous groups of unitary matrices, and we investigate integration problems over them.

Acknowledgements.

I am a professional mathematician, PhD 1996. At some point in my career I was lost inside very abstract mathematics, and I would like to thank Benoît Collins for putting me back on tracks, with probability, numerics, and computer simulations.

Further fun with research came from work with Julien Bichon, Steve Curran, Ion Nechita, Jean-Marc Schlenker, Adam Skalski, Roland Speicher and many others.

Most of this book is based on lecture notes from various classes at Cergy, mainly on linear algebra and probability theory. I would like to thank my students, for their fresh and often uncompromising point of view on these questions, reflected here.

Finally, many thanks go to my cats. There is so much to learn from them, as well.

1. Real matrices

We are interested in what follows in symmetries, rotations, projections and other such transformations, in 2,3 or even more dimensions.

Such transformations appear a bit everywhere, in physics. To be more precise, every physical problem or equation has some "symmetries", and exploiting these symmetries is usually a very useful thing, allowing us to understand the problem or equation.

Normally we should be interested in 3 dimensions, because this is where everyday physics happens. However, if we look at the simplest possible thing "happening", namely a particle moving straight, the situation is more complicated than this.

Indeed, our particle $x \in \mathbb{R}^3$ has as well a direction vector $v \in \mathbb{R}^3$, and so our system is described by the pair $(x, v) \in \mathbb{R}^6$.

Now if we allow our particle to have an acceleration as well, this acceleration must be described by a further quantity $a \in \mathbb{R}$, and so we end up with a quantity of type $(x, v, a) \in \mathbb{R}^7$, which fully describes our system.

And so on.

In order to understand all this, let us start with 2 dimensions, and leave 3 and more dimensions for later.

As already said, we are interested in symmetries, rotations, projections and other such transformations. Such maps are "affine", in the following sense:

Definition 1.1. *A map $f : \mathbb{R}^2 \to \mathbb{R}^2$ is called*

(1) *Affine, if it maps straight lines to straight lines,*
(2) *Linear, if it maps lines passing through 0 to lines passing through 0,*

with the convention that $\{0\}$ itself is a "degenerate" line.

Here the last convention is there in order for some familiar maps, such as the projections, to be affine in our sense.

Indeed, the projection onto the x axis sends the whole y axis to $\{0\}$, so if we want this projection to be affine, $\{0\}$ itself must be a "line".

Here are some basic examples of symmetries, all being linear in the above sense:

Proposition 1.2. *The symmetry with respect to the horizontal axis is:*

$$\begin{pmatrix}x\\y\end{pmatrix}\to\begin{pmatrix}x\\-y\end{pmatrix}$$

The symmetry with respect to the vertical axis is:

$$\begin{pmatrix}x\\y\end{pmatrix}\to\begin{pmatrix}-x\\y\end{pmatrix}$$

The symmetry with respect to the $x=y$ diagonal is:

$$\begin{pmatrix}x\\y\end{pmatrix}\to\begin{pmatrix}y\\x\end{pmatrix}$$

The symmetry with respect to the $x=-y$ diagonal is:

$$\begin{pmatrix}x\\y\end{pmatrix}\to\begin{pmatrix}-y\\-x\end{pmatrix}$$

Finally, the symmetry with respect to the origin 0 is:

$$\begin{pmatrix}x\\y\end{pmatrix}\to\begin{pmatrix}-x\\-y\end{pmatrix}$$

All these maps are linear, in the above sense.

Proof. The fact that all these maps are linear is clear, because they map lines passing through 0 to lines passing through 0. As for the explicit formulae in the statement, these are clear as well, by drawing pictures for each of the maps involved. □

Here are now some basic examples of rotations, once again all being linear:

Proposition 1.3. *The rotation of angle 0° is the identity, namely:*

$$\begin{pmatrix}x\\y\end{pmatrix}\to\begin{pmatrix}x\\y\end{pmatrix}$$

The rotation of angle 90° is given by:

$$\begin{pmatrix}x\\y\end{pmatrix}\to\begin{pmatrix}-y\\x\end{pmatrix}$$

The rotation of angle 180° is the symmetry with respect to 0:

$$\begin{pmatrix}x\\y\end{pmatrix}\to\begin{pmatrix}-x\\-y\end{pmatrix}$$

As for the rotation of angle 270°, this is given by:

$$\begin{pmatrix}x\\y\end{pmatrix}\to\begin{pmatrix}y\\-x\end{pmatrix}$$

All these maps are linear, in the above sense.

Proof. As before, these rotations are all linear, because they map lines passing through 0 to lines passing through 0. As for the explicit formulae in the statement, these are clear as well, by drawing pictures for each of the maps involved. □

Here are as well some basic examples of projections, once again all being linear:

Proposition 1.4. *The projection on the horizontal axis is:*

$$\begin{pmatrix} x \\ y \end{pmatrix} \to \begin{pmatrix} x \\ 0 \end{pmatrix}$$

The projection on the vertical axis is:

$$\begin{pmatrix} x \\ y \end{pmatrix} \to \begin{pmatrix} 0 \\ y \end{pmatrix}$$

The projection on the $x = y$ diagonal is:

$$\begin{pmatrix} x \\ y \end{pmatrix} \to \frac{1}{2}\begin{pmatrix} x+y \\ x+y \end{pmatrix}$$

The projection on the $x = -y$ diagonal is:

$$\begin{pmatrix} x \\ y \end{pmatrix} \to \frac{1}{2}\begin{pmatrix} x-y \\ y-x \end{pmatrix}$$

Finally, the projection to the origin 0 is:

$$\begin{pmatrix} x \\ y \end{pmatrix} \to \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

All these maps are linear, in the above sense.

Proof. As before, these projections are all linear. As for the formulae in the statement, these are clear as well, by drawing pictures for each of the maps involved. □

Finally, we have as well translations, as follows:

Proposition 1.5. *The translations are exactly the maps of the form*

$$\begin{pmatrix} x \\ y \end{pmatrix} \to \begin{pmatrix} x+p \\ y+q \end{pmatrix}$$

with $p, q \in \mathbb{R}$, and these maps are all affine, in the above sense.

Proof. A translation $f : \mathbb{R}^2 \to \mathbb{R}^2$ is clearly affine, because it maps lines to lines. Also, such a translation is uniquely determined by the following vector:

$$f\begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} p \\ q \end{pmatrix}$$

To be more precise, f must be the map which takes a vector $\binom{x}{y}$, and adds this vector $\binom{p}{q}$ to it. But this gives the formula in the statement. □

Summarizing, we have many interesting examples of linear and affine maps. It is of course possible to get to more complicated things, for instance by taking in Proposition 1.2 and Proposition 1.4 the horizontal axis rotated by an arbitrary angle, and also by using in Proposition 1.3 an arbitary angle as well. We will be back to this later.

Let us develop now some general theory, for the linear and affine maps.

As a first theorem, the linear/affine maps $f : \mathbb{R}^2 \to \mathbb{R}^2$ are fully described by 4/6 parameters, which appear as follows:

Theorem 1.6. *The linear maps $f : \mathbb{R}^2 \to \mathbb{R}^2$ are precisely the maps of type*

$$f\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$$

and the affine maps $f : \mathbb{R}^2 \to \mathbb{R}^2$ are precisely the maps of type

$$f\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix} + \begin{pmatrix} p \\ q \end{pmatrix}$$

with the convention that the vectors in $\mathbb{R}^2$ are written vertically.

Proof. This follows indeed by doing some plane geometry:

(1) A linear map $f : \mathbb{R}^2 \to \mathbb{R}^2$ is uniquely determined by its values on the basic coordinate vectors, namely:

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad , \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

But this gives the result.

(2) As for the affine case, here we have as extra piece of data the vector:

$$\begin{pmatrix} p \\ q \end{pmatrix} = f(0)$$

Indeed, if $f : \mathbb{R}^2 \to \mathbb{R}^2$ is affine, then the following map is linear:

$$f - \begin{pmatrix} p \\ q \end{pmatrix} : \mathbb{R}^2 \to \mathbb{R}^2$$

Thus, we obtain the result. □

There are many examples of such maps, and we will be back to this in a second.

In order to simplify now a bit all this, the idea is to put our parameters a, b, c, d into a matrix, in the following way:

Definition 1.7. *A matrix $A \in M_2(\mathbb{R})$ is an array as follows:*

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

These matrices act on the vectors in the following way,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$$

the rule being "multiply the rows of the matrix by the vector".

The above multiplication formula might seem a bit complicated, at a first glance, but it is not. Here is an example for it:

$$\begin{pmatrix} 1 & 2 \\ 5 & 6 \end{pmatrix} \begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \cdot 3 + 2 \cdot 1 \\ 5 \cdot 3 + 6 \cdot 1 \end{pmatrix} = \begin{pmatrix} 5 \\ 21 \end{pmatrix}$$

As already mentioned, all this comes from our findings from Theorem 1.6. Indeed, with the above multiplication convention, we can turn Theorem 1.6 into something much simpler, and better-looking, as folllows:

Theorem 1.8. *The linear maps $f : \mathbb{R}^2 \to \mathbb{R}^2$ are precisely the maps of type*

$$f(v) = Av$$

and the affine maps $f : \mathbb{R}^2 \to \mathbb{R}^2$ are precisely the maps of type

$$f(v) = Av + w$$

with A being a 2×2 matrix, and with $v, w \in \mathbb{R}^2$ being vectors, written vertically.

Proof. With the above convention for the multiplication of matrices and vectors, the formulae in Theorem 1.6 read:

$$f\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

$$f\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} p \\ q \end{pmatrix}$$

But this is exactly the formula in the statement, with:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad , \quad v = \begin{pmatrix} x \\ y \end{pmatrix} \quad , \quad w = \begin{pmatrix} p \\ q \end{pmatrix}$$

Thus, we have proved our theorem. □

Before going further, let us discuss some examples. There are many interesting linear maps $f : \mathbb{R}^2 \to \mathbb{R}^2$, and we will discuss them gradually. First, we have:

Proposition 1.9. *The symmetry with respect to the horizontal axis is given by:*

$$\begin{pmatrix}1&0\\0&-1\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}x\\-y\end{pmatrix}$$

The symmetry with respect to the vertical axis is given by:

$$\begin{pmatrix}-1&0\\0&1\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}-x\\y\end{pmatrix}$$

The symmetry with respect to the $x=y$ diagonal is given by:

$$\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}y\\x\end{pmatrix}$$

The symmetry with respect to the $x=-y$ diagonal is given by:

$$\begin{pmatrix}0&-1\\-1&0\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}-y\\-x\end{pmatrix}$$

Finally, the symmetry with respect to the origin 0 is given by:

$$\begin{pmatrix}-1&0\\0&-1\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}-x\\-y\end{pmatrix}$$

Proof. All these formulae follow from the formulae in Proposition 1.2 above, by guessing the matrix which does the job, in the obvious way. □

Regarding now the basic rotations, we have here:

Proposition 1.10. *The rotation of angle 0° is given by:*

$$\begin{pmatrix}1&0\\0&1\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}x\\y\end{pmatrix}$$

The rotation of angle 90° is given by:

$$\begin{pmatrix}0&-1\\1&0\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}-y\\x\end{pmatrix}$$

The rotation of angle 180° is given by:

$$\begin{pmatrix}-1&0\\0&-1\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}-x\\-y\end{pmatrix}$$

As for the rotation of angle 270°, this is given by:

$$\begin{pmatrix}0&1\\-1&0\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}y\\-x\end{pmatrix}$$

Proof. As before, all these formulae follow from the formulae in Proposition 1.3 above, by guessing each time the matrix which does the job, in the obvious way. □

Finally, regarding the basic projections, we have here:

Proposition 1.11. *The projection on the horizontal axis is given by:*

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ 0 \end{pmatrix}$$

The projection on the vertical axis is given by:

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ y \end{pmatrix}$$

The projection on the $x = y$ diagonal is given by:

$$\frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \frac{1}{2} \begin{pmatrix} x + y \\ x + y \end{pmatrix}$$

The projection on the $x = -y$ diagonal is given by:

$$\frac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \frac{1}{2} \begin{pmatrix} x - y \\ y - x \end{pmatrix}$$

Finally, the projection to the origin 0 is given by:

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

Proof. As before, all these formulae follow from the formulae in Proposition 1.4 above, by guessing each time the matrix which does the job, in the obvious way. □

Here is now a more bizarre map, which still be understood, however, as being the map which "switches the coordinates, then kills the second one":

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y \\ 0 \end{pmatrix}$$

Even more bizarrely now, here is a certain linear map, whose interpretation is more complicated, and is left to the reader:

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + y \\ 0 \end{pmatrix}$$

And here is another one, which once again, being something geometric, can definitely be understood, at least in theory:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + y \\ y \end{pmatrix}$$

Summarizing, things can escalate quicky, but our linear map formalism is certainly something powerful, and everything can be a priori understood in terms of matrices.

Let us discuss now the computation of the arbitrary rotations.

The answer here, which requires some trigonometry, is as follows:

Theorem 1.12. *The rotation of angle $t \in \mathbb{R}$ is given by the matrix*

$$R_t = \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix}$$

depending on $t \in \mathbb{R}$ taken modulo 2π.

Proof. The rotation being linear, it must correspond to a certain matrix, as follows:

$$R_t = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

We can guess this matrix, via its action on the basic coordinate vectors $\binom{1}{0}$ and $\binom{0}{1}$. A quick picture shows that we must have:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos t \\ \sin t \end{pmatrix}$$

Also, by paying attention to positives and negatives, we must have:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -\sin t \\ \cos t \end{pmatrix}$$

Guessing now the matrix is not complicated, because the first equation gives us in fact the first column, and the second equation gives us the second column:

$$\begin{pmatrix} a \\ c \end{pmatrix} = \begin{pmatrix} \cos t \\ \sin t \end{pmatrix}$$

$$\begin{pmatrix} b \\ d \end{pmatrix} = \begin{pmatrix} -\sin t \\ \cos t \end{pmatrix}$$

Thus, we can just put together these two vectors, and we obtain our matrix. □

It is possible to write down as well formulae for the arbitrary symmetries, and arbitrary projections, in 2 dimensions. We will be back to this.

In order to formulate now our second theorem, dealing with compositions of maps, let us make the following multiplication convention, between matrices and matrices:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} ap + br & aq + bs \\ cp + dr & cq + ds \end{pmatrix}$$

This might look a bit complicated at first, but the idea is once again very simple, namely "multiply the rows of the first matrix by the columns of the second matrix".

With this convention, we have the following result:

Theorem 1.13. *If we denote by $f_A : \mathbb{R}^2 \to \mathbb{R}^2$ the linear map associated to a matrix A, given by the formula*

$$f_A(v) = Av$$

then we have the following multiplication formula:

$$f_A f_B = f_{AB}$$

In other words, the composition of linear maps corresponds to the multiplication of the corresponding matrices.

Proof. We want to show that we have the following formula, valid for any two matrices $A, B \in M_2(\mathbb{R})$, and any vector $v \in \mathbb{R}^2$:

$$A(Bv) = (AB)v$$

For this purpose, let us write our matrices and vector as follows:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad , \quad B = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \quad , \quad v = \begin{pmatrix} x \\ y \end{pmatrix}$$

The formula that we want to prove becomes:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \left[\begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \right] = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} \right] \begin{pmatrix} x \\ y \end{pmatrix}$$

But this is the same as saying that:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} px + qy \\ rx + sy \end{pmatrix} = \begin{pmatrix} ap + br & aq + bs \\ cp + dr & cq + ds \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

And this latter formula does hold indeed, because on both sides we get:

$$\begin{pmatrix} apx + aqy + brx + bsy \\ cpx + cqy + drx + dsy \end{pmatrix}$$

Thus, we have proved the result. □

The above result is something quite powerful, fully justifying our matrix formalism for the linear maps. We will be back to this later, with some concrete applications.

As a verification for the above result, let us compose two rotations. The computation here is as follows, yieding a rotation, as it should, and of the correct angle:

$$\begin{aligned}
& R_sR_t\\
= \ & \begin{pmatrix}\cos s & -\sin s\\ \sin s & \cos s\end{pmatrix}\begin{pmatrix}\cos t & -\sin t\\ \sin t & \cos t\end{pmatrix}\\
= \ & \begin{pmatrix}\cos s\cos t-\sin s\sin t & -\cos s\sin t-\sin t\cos s\\ \sin s\cos t+\cos s\sin t & -\sin s\sin t+\cos s\cos t\end{pmatrix}\\
= \ & \begin{pmatrix}\cos(s+t) & -\sin(s+t)\\ \sin(s+t) & \cos(s+t)\end{pmatrix}\\
= \ & R_{s+t}
\end{aligned}$$

This verification is quite interesting, because we can see here the power of linear algebra. Indeed, the theory that we have so far beats a lot of non-trivial trigonometry.

We will be back to more applications to 2 dimensions later on.

We are ready now to pass to 3 dimensions. The idea is to select what we know in 2 dimensions, nice looking results only, and generalize to 3 dimensions. We obtain:

Theorem 1.14. *Consider a map $f:\mathbb{R}^3\to\mathbb{R}^3$.*

(1) *f is linear, sending lines through 0 to lines through 0, precisely when it is of the form*

$$f(v)=Av$$

with A being a certain 3×3 matrix.

(2) *f is affine, sending lines to lines, precisely when it is of the form*

$$f(v)=Av+w$$

with A being a certain 3×3 matrix, and $w\in\mathbb{R}^3$ being a vector.

In addition, we have a formula of type

$$f_Af_B=f_{AB}$$

similar to the 2D one.

Proof. Here (1) and (2) can be proved exactly as in the 2D case, with the multiplication convention being as usual, "multiply the rows of the matrix by the vector":

$$\begin{pmatrix}a & b & c\\ d & e & f\\ g & h & i\end{pmatrix}\begin{pmatrix}x\\ y\\ z\end{pmatrix}=\begin{pmatrix}ax+by+cz\\ dx+ey+fz\\ gx+hy+iz\end{pmatrix}$$

As for the last assertion, once again the idea in 2D applies, with the same product rule, "multiply the rows of the first matrix by the columns of the second matrix":

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \begin{pmatrix} p & q & r \\ s & t & u \\ v & w & x \end{pmatrix}$$

$$= \begin{pmatrix} ap+bs+cv & aq+bt+cw & ar+bu+cx \\ dp+es+fv & dq+et+fw & dr+eu+fx \\ gp+hs+iv & gq+ht+iw & gr+hu+ix \end{pmatrix}$$

Thus, we have proved our theorem. Of course, we are going a bit fast here, and some verifications are missing, but we will extend this to N dimensions anyway. □

There are many other things that can be said about 3 dimensions, and we will be back to this, gradually, in what follows.

We are now ready to discuss 4 and more dimensions.

Before doing so, let us point out however that the maps $f : \mathbb{R}^3 \to \mathbb{R}^2$, or $f : \mathbb{R} \to \mathbb{R}^2$, and so on, are not covered by our results. Since there are many interesting such maps, say obtained by projecting and then rotating, and so on, we will be interested here is the maps $f : \mathbb{R}^N \to \mathbb{R}^M$.

A bit of thinking suggests that such maps should come from the $M \times N$ matrices. Indeed, this is what happens at $M = N = 2$ and $M = N = 3$, of course. But this happens as well at $M = 1$, because a linear map $f : \mathbb{R} \to \mathbb{R}^N$ can only be something of the form $f(\lambda) = \lambda v$, with $v \in \mathbb{R}^N$. But $v \in \mathbb{R}^N$ means that v is a $N \times 1$ matrix.

So let us start with the product rule for such matrices, that we will need all the time:

Definition 1.15. *We can multiply the $M \times N$ matrices with $N \times K$ matrices,*

$$\begin{pmatrix} a_{11} & \dots & a_{1N} \\ \vdots & & \vdots \\ a_{M1} & \dots & a_{MN} \end{pmatrix} \begin{pmatrix} b_{11} & \dots & b_{1K} \\ \vdots & & \vdots \\ b_{N1} & \dots & b_{NK} \end{pmatrix}$$

the product being given by the following formula,

$$\begin{pmatrix} a_{11}b_{11} + \ldots + a_{1N}b_{N1} & \ldots\ldots & a_{11}b_{1K} + \ldots + a_{1N}b_{NK} \\ \vdots & & \vdots \\ \vdots & & \vdots \\ a_{M1}b_{11} + \ldots + a_{MN}b_{N1} & \ldots\ldots & a_{M1}b_{1K} + \ldots + a_{MN}b_{NK} \end{pmatrix}$$

obtained via the usual rule "multiply rows by columns".

Observe that this generalizes all the multiplication rules given so far. So, we can simply forget all the rules that we previously learned, and simply memorize this one.

In case this looks hard to memorize, here is a simpler formula, using algebraic notation for the matrices, along with some consequences coming from it:

Proposition 1.16. *The matrix multiplication is given by the following formula:*

$$(AB)_{ij} = \sum_k A_{ik}B_{kj}$$

In addition, we have the following general formula, valid for any A, B, C,

$$(AB)C = A(BC)$$

provided of course that the sizes of our matrices A, B, C fit.

Proof. The first formula is just a shorthand for the formula in Definition 1.15. As for the second formula, this follows from it. Indeed, we have:

$$\begin{aligned}((AB)C)_{ij} &= \sum_k (AB)_{ik}C_{kj}\\ &= \sum_{kl} A_{il}B_{lk}C_{kj}\end{aligned}$$

On the other hand, we have as well:

$$\begin{aligned}(A(BC))_{ij} &= \sum_l A_{il}(BC)_{lj}\\ &= \sum_{kl} A_{il}B_{lk}C_{kj}\end{aligned}$$

Thus, we have proved our result. □

We can now talk about linear maps, as follows:

Theorem 1.17. *Consider a map $f : \mathbb{R}^N \to \mathbb{R}^M$.*

(1) *f is linear, sending lines through 0 to lines through 0, precisely when it is of the form*

$$f(v) = Av$$

with A being a certain $M \times N$ matrix.

(2) *f is affine, sending lines to lines, precisely when it is of the form*

$$f(v) = Av + w$$

with A being a certain $M \times N$ matrix, and $w \in \mathbb{R}^M$ being a vector.

In addition, we have $f_A f_B = f_{AB}$, whenever the sizes fit.

Proof. We already know that this happens indeed at $M = N = 2$, and at $M = N = 3$ as well. In general, the proof is similar, by doing some computations. □

Summarizing, the general theory goes exactly as in 2 dimensions.

As a first example here, we have the identity matrix:

$$\begin{pmatrix} 1 & \ldots & \ldots \\ \vdots & \ddots & \vdots \\ \ldots & \ldots & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix}$$

We have as well the null matrix:

$$\begin{pmatrix} 0 & \ldots & \ldots \\ \vdots & \ddots & \vdots \\ \ldots & \ldots & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

There are many other trivial examples.

Here is now an important result, providing us with many examples:

Proposition 1.18. *The diagonal matrices act as follows:*

$$\begin{pmatrix} \lambda_1 & \ldots & \ldots \\ \vdots & \ddots & \vdots \\ \ldots & \ldots & \lambda_N \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix} = \begin{pmatrix} \lambda_1 x_1 \\ \vdots \\ \lambda_N x_N \end{pmatrix}$$

Proof. This is clear, indeed. □

Another interesting example is the flat matrix, which is as follows:

$$\mathbb{I} = \begin{pmatrix} 1 & \ldots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \ldots & 1 \end{pmatrix}$$

This matrix acts in the following way:

$$\begin{pmatrix} 1 & \ldots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \ldots & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix} = \begin{pmatrix} x_1 + \ldots + x_N \\ \vdots \\ x_1 + \ldots + x_N \end{pmatrix}$$

This latter formula is best written as follows:

$$\frac{1}{N} \begin{pmatrix} 1 & \ldots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \ldots & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix} = \frac{x_1 + \ldots + x_N}{N} \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$$

This suggests to make the following normalization:

$$P=\frac{1}{N}\begin{pmatrix}1&\ldots&1\\ \vdots&\ddots&\vdots\\ 1&\ldots&1\end{pmatrix}$$

Indeed, a bit of thinking tells us that P must be the projection on the all-1 vector. We will be back later to this, with a more detailed result.

Let us develop now some general theory for the linear maps, by using the fact that these are the same thing as the matrices.

We first have the following result:

Theorem 1.19. *A linear map $f:\mathbb{R}^N\to\mathbb{R}^N$, written as*

$$f(v)=Av$$

is invertible precisely when A is invertible, and in this case we have:

$$f^{-1}(v)=A^{-1}v$$

Proof. This is standard, coming from the following formula:

$$f_Af_B(v)=f_{AB}(v)$$

Indeed, this gives all the assertions. □

In view of the above result, an interesting question is that of inverting the square matrices. In general, this is something which is quite complicated.

In the simplest case, in 2 dimensions, the result is as follows:

Theorem 1.20. *We have the following inversion formula, for the 2×2 matrices:*

$$\begin{pmatrix}a&b\\ c&d\end{pmatrix}^{-1}=\frac{1}{ad-bc}\begin{pmatrix}d&-b\\ -c&a\end{pmatrix}$$

When $ad-bc=0$, the matrix is not invertible.

Proof. As a first observation, when $ad-bc=0$ we must have, for some $\lambda\in\mathbb{R}$:

$$b=\lambda a$$

$$d=\lambda c$$

Thus our matrix must be of the following special type:

$$\begin{pmatrix}a&b\\ c&d\end{pmatrix}=\begin{pmatrix}a&\lambda a\\ a&\lambda c\end{pmatrix}$$

Thus in this case the columns are proportional, and so the matrix is not invertible.

When $ad-bc\neq 0$, let us look for an inversion formula of the following type:

$$\begin{pmatrix}a&b\\c&d\end{pmatrix}^{-1}=\frac{1}{ad-bc}\begin{pmatrix}*&*\\*&*\end{pmatrix}$$

We must therefore solve the following equations:

$$\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}*&*\\*&*\end{pmatrix}=\begin{pmatrix}ad-bc&0\\0&ad-bc\end{pmatrix}$$

The obvious solution here is as follows:

$$\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}d&-b\\-c&a\end{pmatrix}=\begin{pmatrix}ad-bc&0\\0&ad-bc\end{pmatrix}$$

Thus, we are led to the formula in the statement. □

The 3×3 matrices can be inverted as well, but this is something more complicated. We will be back to this, later on.

The idea indeed is that the inversion problem needs, before everything, a certain function $\det:M_N(\mathbb{R})\to\mathbb{R}$ having the property that $\det A\neq 0$ precisely when A is invertible. In 2 dimensions this is the function used in the above proof, namely:

$$\det\begin{pmatrix}a&b\\c&d\end{pmatrix}=ad-bc$$

In general, however, the construction of det is something quite complicated, that we will discuss later on, in section 2 below, after lots of geometric preliminaries.

As an important definition now, we have:

Definition 1.21. *Let A be a square matrix. When the condition*

$$Av=\lambda v$$

is satisfied we say that:

(1) *v is an eigenvector of A.*
(2) *λ is an eigenvalue of A.*

We say that A is diagonalizable when it has a basis of eigenvectors.

When A is diagonalizable, in that basis we can write:

$$A=\begin{pmatrix}\lambda_1&&\\&\ddots&\\&&\lambda_N\end{pmatrix}$$

In general, this means that we have a formula as follows, with D diagonal:

$$A=PDP^{-1}$$

We have many examples here. We have the following result:

Theorem 1.22. *If the matrix has N distinct eigenvalues, it is diagonalizable.*

Proof. This looks quite clear from definitions, because in each of the N directions of the eigenvectors, the matrix must multiply by a certain scalar.

However, the point is that of showing that these N directions do not "overlap", and this comes from the fact that the corresponding eigenvalues are different. □

Here are now a few basic examples:

Proposition 1.23. *The following matrices, which correspond to the symmetries with respect to the $x = y$ and $x = -y$ axes,*

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$$

and the following matrices, which correspond to the projections on these 2 same axes,

$$\frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

$$\frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$$

are all diagonalizable.

Proof. Everything here is clear from the definition of the eigenvalues and eigenvectors, with no need for any matrix computations, or any computations in general. □

Here are as well a few counterexamples:

Proposition 1.24. *The rotation of angle $t \in [0, 2\pi)$, given by the formula*

$$R_t = \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix}$$

is not diagonalizable for $t \neq 0, \pi$. Also, the matrix

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

is not diagonalizable as well, and this for different reasons.

Proof. The rotations of angle $t \neq 0, \pi$ clearly cannot have eigenvectors. As a comment here, however, we will see later on that these rotations have complex eigenvectors.

Regarding now the second matrix, this acts as follows:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y \\ 0 \end{pmatrix}$$

Thus the eigenvector/eigenvalue equation $Av = \lambda v$ reads:

$$\begin{pmatrix} y \\ 0 \end{pmatrix} = \begin{pmatrix} \lambda x \\ \lambda y \end{pmatrix}$$

For $\lambda \neq 0$ we must have $y = 0$, and so $x = 0$ as well, so we have no nontrivial eigenvectors.

As for the case $\lambda = 0$, here we must have $y = 0$, and so the eigenvectors here are the vectors of the form $\begin{pmatrix} x \\ 0 \end{pmatrix}$. Thus our matrix is not diagonalizable, as stated. □

Let us discuss now the general 2D case.

We have here the following result:

Theorem 1.25. *Diagonalization of the 2×2 matrices.*

Proof. This is quite technical, and is our main result here. We must solve:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \lambda \begin{pmatrix} x \\ y \end{pmatrix}$$

Thus, we have the following system of equations:

$$\begin{cases} ax + by &= \lambda x \\ cx + dy &= \lambda y \end{cases}$$

We obtain from this the following formula:

$$\lambda^2 - (a + d)\lambda + (ad - bc) = 0$$

We have several cases here. Full discussion. □

There are many matrices which are not diagonalizable, and this for various reasons. For some, we would need complex numbers. For some others, there is not fix.

Let us get now to higher dimensions. In order to discuss some interesting examples of matrices, and their diagonalization, we will need the following standard fact:

Theorem 1.26. *Consider the scalar product on $\mathbb{R}^N$, given by:*

$$< x, y >= \sum_i x_i y_i$$

We have then the following formula, valid for any vectors x, y and any matrix A,

$$< Ax, y >=< x, A^t y >$$

with A^t being the transpose matrix.

Proof. By linearity, it is enough to prove the above formula on the standard basis vectors $e_1, \ldots, e_N$ of $\mathbb{R}^N$. Thus, we want to prove that for any i, j we have:

$$< Ae_j, e_i >=< e_j, A^t e_i >$$

The scalar product being symmetric, this is the same as proving that:

$$< Ae_j, e_i >=< A^t e_i, e_j >$$

On the other hand, for any matrix M we have the following formula:

$$M_{ij} =< Me_j, e_i >$$

Thus, the formula to be proved simply reads:

$$A_{ij} = (A^t)_{ji}$$

But this precisely the definition of A^t, and we are done. □

With this, we can develop some theory. We first have:

Proposition 1.27. *The linear maps $f : \mathbb{R}^N \to \mathbb{R}^N$ which are projections, in the sense that*

$$f^2 = f$$

are those associated to the matrices $P \in M_N(\mathbb{R})$ satisfying:

$$P^2 = P$$

These latter matrices are diagonalizable, with eigenvalues $0, 1$. Conversely, each matrix with eigenvalues $0, 1$ corresponds to a projection.

Proof. The first assertion follows from the general multiplication formula $f_A f_B = f_{AB}$ for linear maps, because with $f = f_P$ we have:

$$\begin{aligned} & f_P^2 = f_P \\ \iff \quad & f_{P^2} = f_P \\ \iff \quad & P^2 = P \end{aligned}$$

Regarding the diagonalization assertion, this is clear by taking a basis of $Im(f)$, which consists of 1-eigenvectors, and then completing with 0-eigenvectors.

Finally, the converse is clear as well, because in the basis where the matrix is diagonal, the action is by multipliying by 0 or 1, so it is a projection. □

In the scalar product context now, we have:

Theorem 1.28. *The orthogonal projections are the matrices satisfying:*

$$P^2 = P = P^t$$

These projections are diagonalizable, with eigenvalues $0, 1$.

Proof. We use the result in Proposition 1.27. In practice, we must take the condition $P^2 = P$ found there, and add to it the condition coming from the fact that P is orthogonal, as a projection. But this condition can be written and processed as follows:

$$\begin{aligned} & < Px - Py, Px - x >= 0 \\ \iff & < x - y, P^tPx - P^tx >= 0 \\ \iff & P^tPx - P^tx = 0 \\ \iff & P^tP - P^t = 0 \end{aligned}$$

Thus we must have $P^t = P^tP$. Now observe that by conjugating, we obtain:

$$\begin{aligned} P &= (P^tP)^t \\ &= P^t(P^t)^t \\ &= P^tP \end{aligned}$$

Now by comparing with the original relation, $P^t = P^tP$, we conclude that:

$$P = P^t$$

Thus, we have shown that any orthogonal projection must satisfy:

$$P^2 = P = P^t$$

Conversely now, assuming $P^2 = P = P^t$, we know from Proposition 1.27 that P is a projection, and the above condition, namely $P^t = P^tP$, is satisfied as well.

Thus, we are led to the conclusion in the statement. □

Here is now a key computation of such projections:

Theorem 1.29. *The rank* 1 *projections are given by the formula*

$$P_x = \frac{1}{||x||^2}(x_ix_j)_{ij}$$

where the constant, namely

$$||x|| = \sqrt{\sum_i x_i^2}$$

is the length of the vector.

Proof. Consider a vector $y \in \mathbb{R}^N$. Its projection on $\mathbb{R}x$ must be a certain multiple of x, and we are led in this way to the following formula:

$$\begin{aligned} P_xy &= \frac{< y, x >}{< x, x >}\, x \\ &= \frac{1}{||x||^2} < y, x > x \end{aligned}$$

With this in hand, we can now compute the entries of P_x, as follows:

$$\begin{aligned}(P_x)_{ij} &= < P_x e_j, e_i > \\ &= \frac{1}{||x||^2} < e_j, x >< x, e_i > \\ &= \frac{x_j x_i}{||x||^2}\end{aligned}$$

Thus, we are led to the formula in the statement. □

As an application, we have the following result:

Proposition 1.30. *In 2 dimensions, the rank 1 projections, which are the projections on the Ox axis rotated by an angle $t \in [0, \pi)$, are given by the following formula:*

$$P_t = \begin{pmatrix} \cos^2 t & \cos t \sin t \\ \cos t \sin t & \sin^2 t \end{pmatrix}$$

Together with the following two matrices, which are the rank 0 and 2 projections in $\mathbb{R}^2$,

$$0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$1 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

these are all the projections in 2 dimensions.

Proof. The first assertion follows from the general formula in Theorem 1.29, by plugging in the following vector, depending on a parameter $t \in [0, \pi)$:

$$x = \begin{pmatrix} \cos t \\ \sin t \end{pmatrix}$$

As for the second assertion, this is clear from the first one, because outside rank 1 we can only have rank 0 or rank 2, corresponding to the matrices in the statement. □

Here is another interesting application, this time in N dimensions:

Proposition 1.31. *The projection on the all-1 vector $\xi \in \mathbb{R}^N$ is*

$$P_\xi = \frac{1}{N} \begin{pmatrix} 1 & \ldots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \ldots & 1 \end{pmatrix}$$

d with the all-1 matrix on the right being called the flat matrix.

Proof. As already pointed out in the discussion following Proposition 1.18 above, the matrix in the statement acts in the following way:

$$P_\xi \begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix} = \frac{x_1 + \ldots + x_N}{N} \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$$

Thus P_ξ is indeed a projection onto $\mathbb{R}\xi$, and the fact that this projection is indeed the orthogonal one follows either by a direct orthogonality computation, or by using the general formula in Theorem 1.29 above, by plugging in the all-1 vector ξ. □

Before going further, we should make a comment about diagonalization. In the context of general projections, what differentiates the arbitrary ones, from Proposition 1.27, from the orthogonal ones, from Theorem 1.28, is the fact that the latter can be diagonalized via an orthogonal transformation of $\mathbb{R}^N$. We will be back to this in a moment.

As for the rank 1 projections, here are there many ways of diagonalizing, some of them being better than the other. We will see later on, in section 3 below, that even in the simplest case, of the projections from Proposition 1.31, this is something quite tricky, and that in order to get to fully satisfactory results, we must use complex numbers.

Let us discuss now, as a final topic of this preliminary section, the isometries of $\mathbb{R}^N$. We have here the following general result:

Theorem 1.32. *The linear maps $f : \mathbb{R}^N \to \mathbb{R}^N$ which are isometries, in the sense that they preserve scalar products, or distances, are those coming from matrices satisfying:*

$$U^t = U^{-1}$$

These latter matrices are called orthogonal, and they form a set $O_N \subset M_N(\mathbb{R})$ which is stable under taking compositions, and inverses.

Proof. The first assertion follows by doing some computations based on the formula in Theorem 1.26 above, in the spirit of those from the proof of Theorem 1.28.

As for the second assertion, this is clear from definitions. □

As a basic illustration here, we have:

Theorem 1.33. *The rotations in the plane, given by the formula*

$$R_t = \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix}$$

are isometries. The symmetries in the plane, given by formula

$$S_t = \begin{pmatrix} \cos t & \sin t \\ \sin t & -\cos t \end{pmatrix}$$

are isometries as well. These are all the isometries in 2 dimensions.

Proof. We already know that R_t is the rotation of angle t. As for S_t, this is the symmetry with respect to the Ox axis rotated by $t/2 \in \mathbb{R}$. This gives the result. □

We will be back to O_N, which is a so-called group, and is actually one of the most important examples of groups, on several occasions, in what follows.

2. The determinant

We have seen in the previous section that most of the interesting maps $f : \mathbb{R}^N \to \mathbb{R}^N$ that we know, such as rotations, symmetries and projections, are linear, and so can be written in the following form, with $A \in M_N(\mathbb{R})$ being a square matrix:

$$f(v) = Av$$

In this section we develop more general theory, more advanced this time, for the linear maps $f : \mathbb{R}^N \to \mathbb{R}^N$, written in the above form, in terms of a matrix $A \in M_N(\mathbb{R})$.

To be more precise, we will investigate here the following theoretical question, which is of particular importance: which linear maps $f(v) = Av$ are invertible?

This is quite a tricky problem, so let us first recall what we know so far about it, from section 1 above. First, at the level of the basic examples we have:

Proposition 2.1. *The basic linear maps are as follows:*

(1) *The rotation R_t is invertible, its inverse being R_{-t}.*
(2) *Any symmetry S is invertible, with $S^{-1} = S$.*
(3) *The projections $P \neq 1$ are not invertible.*

Proof. All this is clear from definitions, as follows:

(1) This is obvious, because rotating by an angle $t \in \mathbb{R}$, and then rotating backwards by the same angle, amounts in doing nothing.

(2) Once again this is obvious, because a symmetry S is somehow by definition a linear transformation satisfying $S^2 = id$, and so $S^{-1} = S$.

(3) This is clear too, because when our projection P is non-degenerate, in the sense that $P \neq 1$, we are certainly losing information when applying it. □

Observe that the above results do not use matrix theory of any kind.

In general, however, we have to use matrices, and we have here:

Theorem 2.2. *A linear map $f : \mathbb{R}^N \to \mathbb{R}^N$, written as*

$$f(v) = Av$$

is invertible precisely when A is invertible, and in this case we have:

$$f^{-1}(v) = A^{-1}v$$

Proof. This is something that we already know, coming from the following formula:

$$f_A f_B(v) = f_{AB}(v)$$

Indeed, this gives all the assertions. □

In view of the above result, we are led to the question of inverting the square matrices $A \in M_N(\mathbb{R})$. In general, this is something which is quite complicated.

In the simplest case, in 2 dimensions, the result is as follows:

Theorem 2.3. *We have the following inversion formula, for the 2×2 matrices:*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

When $ad - bc = 0$, the matrix is not invertible.

Proof. This is something that we already know, the idea being as follows:

(1) In order for our matrix $A \in M_2(\mathbb{R})$ to be invertible, its column vectors $\binom{a}{c}$ and $\binom{b}{d}$ must be not proportional, and this amounts in saying that we have:

$$ad - bc \neq 0$$

(2) Now by assuming that this condition holds, the trick is to look for a matrix $M \in M_2(\mathbb{R})$ satisfying $AM = (ad - bc)1_2$, so that our inverse is:

$$A^{-1} = \frac{1}{ad - bc} M$$

But this leads to the formula in the statement. □

Summarizing, we have so far some results, and notably Theorem 2.3 above, which is something quite tricky.

In order to deal now with the inversion problem in general, for the arbitrary matrices $A \in M_N(\mathbb{R})$, we will use the method coming from Theorem 2.3 above.

To be more precise, if we write $A = (v_1, \ldots, v_N)$, with $v_1, \ldots, v_N \in \mathbb{R}^N$ being the columns of A, then we know from the general results from section 1 that, in order for A to be invertible, the vectors $v_1, \ldots, v_N$ must be linearly independent.

Thus, following (1) in the proof of Theorem 2.3, we are led into the question of understanding when a family of vectors $v_1, \ldots, v_N \in \mathbb{R}^N$ are linearly independent.

In order to deal with this latter question, let us introduce the following notion:

Definition 2.4. *Associated to any vectors $v_1, \ldots, v_N \in \mathbb{R}^N$ is the volume*

$$\det{}^+(v_1 \ldots v_N) = vol < v_1, \ldots, v_N >$$

of the parallelepiped made by these vectors.

In other words, we have constructed here a function $\det^+ : M_N(\mathbb{R}) \to \mathbb{R}_+$, having the property that $A \in M_N(\mathbb{R})$ is invertible precisely when:

$$\det^+(A) > 0$$

We will see later, after fully understanding how this function works, that this will ultimately lead to a solution of our inversion problem.

As a first observation now, in 1 dimension we recover in this way the absolute value of the real numbers:

$$\det^+(a) = |a|$$

In 2 dimensions now, the computation is non-trivial, and we have the following result, making the link with our main result so far, namely Theorem 2.3 above:

Theorem 2.5. *In 2 dimensions we have the following formula,*

$$\det^+ \begin{pmatrix} a & b \\ c & d \end{pmatrix} = |ad - bc|$$

with $\det^+ : M_2(\mathbb{R}) \to \mathbb{R}_+$ *being the function constructed above.*

Proof. This follows from an elementary geometry computation.

To be more precise, we must show that the area of the parallelogram formed by $\binom{a}{c}, \binom{b}{d}$ equals the quantity $|ad - bc|$, which is a difference of areas of two rectangles.

But this can be done by drawing the parallelogram, along with the vertical lines at a, b, and the horizontal lines at c, d, and then:

(1) Either computing the lenghts of all segments appearing on the picture, by using the Thales theorem, and then the area of the parallelogram, by dividing it into triangles, and then using the usual $A = bh/2$ formula for the area of the triangles.

(2) Or solving the problem in "puzzle" style, without algebraic computations, by suitably chopping the parallelogram, along the vertical and horizontal lines, and then rearranging and modifying the pieces as to cover the difference of the two rectangles.

There is as well an alternative proof, which is somewhat hybrid between the above two ones, consisting in deforming the parallelogram, via linear transformations which keep the area constant, into a rectangle, and then computing the area of this rectangle. □

All this is very nice, but we can see that our theory has a flaw, because in 1 dimension a is certainly a better quantity than $|a|$, and in 2 dimensions, $ad - bc$ is certainly a better quantity than $|ad - bc|$.

To be more precise, the signed quantities have for instance good additivity properties, and so can be effectively computed, while the unsigned ones do not have such properties, and are therefore much harder to compute.

So, let us upgrade now our theory, by constructing a function of type:

$$\det : M_N(\mathbb{R}) \to \mathbb{R}$$

For this purpose, we just need a sign. And this sign can be introduced as follows:

Definition 2.6. *A system of vectors $v_1, \ldots, v_N \in \mathbb{R}^N$ is called:*

(1) *Oriented, if one can continuously pass from the standard basis to it.*
(2) *Unoriented, otherwise.*

The associated sign is $+$ in the oriented case, and $-$ in the unoriented case.

As a basic example, in 1 dimension the sign is the usual one:

$$sgn(a) = \begin{cases} + & \text{if } a > 0 \\ - & \text{if } a < 0 \end{cases}$$

In 2 dimensions now, the explicit formula of the sign is as follows:

Proposition 2.7. *We have the following formula, valid for any 2 vectors in $\mathbb{R}^2$,*

$$sgn\left[\begin{pmatrix} a \\ c \end{pmatrix}, \begin{pmatrix} b \\ d \end{pmatrix}\right] = sgn(ad - bc)$$

with the two sign functions being those defined above, in 2 and 1 dimensions.

Proof. According to our definitions, the sign of $\binom{a}{c}, \binom{b}{d}$ is $+$ when these vectors come in this order with respect to the counterclockwise rotation, and is $-$ otherwise.

Thus, when assuming $a, b, c, d > 0$ for simplifying, we are left with comparing the angles having the numbers c/a and d/b as tangents, and we obtain in this way:

$$sgn\left[\begin{pmatrix} a \\ c \end{pmatrix}, \begin{pmatrix} b \\ d \end{pmatrix}\right] = \begin{cases} + & \text{if } \frac{c}{a} < \frac{d}{b} \\ - & \text{if } \frac{c}{a} > \frac{d}{b} \end{cases}$$

But this gives the formula in the statement. The proof in general is similar. □

At the level of the general results now, we have:

Proposition 2.8. *The orientation of a system of vectors changes as follows:*

(1) *If we switch the sign of a vector, the associated sign switches.*
(2) *If we permute two vectors, the associated sign switches as well.*

Proof. This is indeed clear from definitions. □

One interesting question is about permuting the whole basis. We will see later on that the corresponding sign is the "signature" of the corresponding permutation.

With the above notion in hand, we can now formulate:

Definition 2.9. *The determinant of $v_1, \ldots, v_N \in \mathbb{R}^N$ is the signed volume*

$$\det(v_1 \ldots v_N) = \pm vol < v_1, \ldots, v_N >$$

of the parallelepiped made by these vectors.

In matrix terms, the determinant of a matrix $A \in M_N(\mathbb{R})$ is the signed volume of the parallelepiped $< v_1, \ldots, v_N >$ made by its column vectors.

In the matrix context, we will often use the symbol $|.|$ instead of det:

$$|A| = \det A$$

Let us try now to compute the determinant. In 1 dimension we have of course $\det a = a$, because the absolute value fits, and so does the sign:

$$\begin{aligned} \det a &= sgn(a) \times |a| \\ &= a \end{aligned}$$

In 2 dimensions now, we have the following result:

Theorem 2.10. *In 2 dimensions we have the following formula,*

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$$

with $|.| = \det$ being the determinant function constructed above.

Proof. According to our definition, to the computation from Theorem 2.5, and to sign formula from Proposition 2.7, the determinant of a 2×2 matrix is given by:

$$\begin{aligned} & \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ = \ & sgn \left[\begin{pmatrix} a \\ c \end{pmatrix}, \begin{pmatrix} b \\ d \end{pmatrix} \right] \times \det{}^+ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ = \ & sgn \left[\begin{pmatrix} a \\ c \end{pmatrix}, \begin{pmatrix} b \\ d \end{pmatrix} \right] \times |ad - bc| \\ = \ & sgn(ad - bc) \times |ad - bc| \\ = \ & ad - bc \end{aligned}$$

Thus, we have obtained the formula in the statement. □

We will be back to more formulae of this type, in 3 dimensions and more, later on, after developing some general theory, allowing us to compute the determinant.

In order to discuss now arbitrary dimensions, we will need a number of theoretical results.

Here is a first series of formulae, coming straight from the definitions:

Theorem 2.11. *The determinant has the following properties:*

(1) *When multiplying by scalars, the determinant gets multiplied as well:*

$$\det(\lambda_1 v_1, \ldots, \lambda_N v_N) = \lambda_1 \ldots \lambda_N \det(v_1, \ldots, v_N)$$

(2) *When permuting two columns, the determinant changes the sign:*

$$\det(\ldots, v, \ldots, w, \ldots) = -\det(\ldots, w, \ldots, v, \ldots)$$

(3) *The determinant* $\det(e_1, \ldots, e_N)$ *of the standard basis of* $\mathbb{R}^N$ *is* 1.

Proof. All this is clear from definitions, as follows:

(1) This follows from definitions, and from Proposition 2.8 (1).

(2) This follows as well from definitions, and from Proposition 2.8 (2).

(3) This is clear from our definition of the determinant. □

As an application of the above result, we have:

Theorem 2.12. *The determinant of a diagonal matrix is given by:*

$$\begin{vmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_N \end{vmatrix} = \lambda_1 \ldots \lambda_N$$

That is, we obtain the product of diagonal entries, or of eigenvalues.

Proof. The formula in the statement is clear by using the rules (1) and (3) in Theorem 2.11 above, which in matrix terms give:

$$\begin{vmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_N \end{vmatrix} = \lambda_1 \ldots \lambda_N \begin{vmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{vmatrix}$$
$$= \lambda_1 \ldots \lambda_N$$

As for the last assertion, this is rather a remark. □

We will see in a moment that, more generally, the determinant of any diagonalizable matrix is the product of its eigenvalues.

In order to reach to more advanced theory, let us adopt now the linear map point of view. In this setting, the definition of the determinant reformulates as follows:

Theorem 2.13. *Given a linear map, written as* $f(v) = Av$*, its "inflation coefficient", obtained as the signed volume of the image of the unit cube, is given by:*

$$I_f = \det A$$

More generally, I_f *is the inflation ratio of any parallelepiped in* $\mathbb{R}^N$*, via the transformation* f*. In particular* f *is invertible precisely when* $\det A \neq 0$.

Proof. The only non-trivial thing here is that the inflation coefficient I_f, as defined above, is independent of the choice of the parallelepiped.

But this is a generalization of the Thales theorem, which can be deduced by doing some geometry, and ultimately follows from the Thales theorem itself. □

Summarizing, we have seen so far that the determinant is a quite interesting quantity, regardless of the viewpoint, which can be families of vectors, matrices, or linear maps.

As a first application of the above linear map viewpoint, we have:

Theorem 2.14. *We have the following formula,*

$$\det(AB) = \det A \cdot \det B$$

valid for any matrices A, B. In particular, we have:

$$\det(AB) = \det(BA)$$

Proof. The decomposition formula in the statement follows by using the associated linear maps, which multiply as follows:

$$f_{AB} = f_A f_B$$

Indeed, when computing the determinant, by using the "inflation coefficient" viewpoint from Theorem 2.13, we obtain the same thing on both sides.

As for the formula $\det(AB) = \det(BA)$, this is clear from the first formula. □

As a technical comment, it is possible to define the determinant by other means, but the downside of these alternative methods is that, when using them, Theorem 2.14 becomes something quite opaque. We will be back to this, with more comments, later on.

Getting back now to explicit computations, we have the following key result:

Theorem 2.15. *The determinant of a diagonalizable matrix*

$$A \sim \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_N \end{pmatrix}$$

is the product of its eigenvalues:

$$\det A = \lambda_1 \ldots \lambda_N$$

Proof. This follows from Theorem 2.12, by using either Theorem 2.13, or Theorem 2.14, and more precisely the formula $\det(AB) = \det(BA)$ there.

Indeed, with $A = BDB^{-1}$ and $D = diag(\lambda_1, \ldots, \lambda_N)$ we have:

$$\begin{aligned} & \det A \\ = \ & \det(BDB^{-1}) \\ = \ & \det(DB^{-1}B) \\ = \ & \det D \\ = \ & \lambda_1 \ldots \lambda_N \end{aligned}$$

Thus, we are led to the formula in the statement. □

We will be back later with examples and applications of the above result, and also with a generalization, to the case of upper or lower triangular matrices.

Here are as well some other computations, once again in arbitrary dimensions:

Proposition 2.16. *We have the following results:*

(1) *The determinant of an orthogonal matrix must be* ± 1.

(2) *The determinant of a projection must be* 0 *or* 1.

Proof. The idea here is as follows:

(1) Here the determinant must be ± 1, because the orthogonal matrices map the unit cube to a copy of the unit cube.

(2) Here the determinant is in general 0, because the projections flatten the unit cube, unless we have the identity, where the determinant is 1. □

We will be back with more explicit computations, later on.

In general now, at the theoretical level, we have the following key result:

Theorem 2.17. *The determinant has the additivity property*

$$\begin{aligned} \det(u + v, w_2, \ldots, w_N) &= \det(u, w_2, \ldots, w_N) \\ &+ \det(v, w_2, \ldots, w_N) \end{aligned}$$

valid for any choice of the vectors involved.

Proof. This follows by doing some elementary geometry, in the spirit of the computations in the proof of Theorem 2.5 above:

(1) Either by using the Thales theorem, and then computing the volumes by using basic algebraic formulae.

(2) Or by solving the problem in "puzzle" style, the idea being to cut the parallelepipeds, and then recover them, after soem simple manipulations. □

As a basic application of the above result, we have:

Theorem 2.18. *We have the following results:*

(1) *The determinant of a diagonal matrix is the product of diagonal entries.*
(2) *The same is true for the upper triangular matrices.*
(3) *The same is true for the lower triangular matrices.*

Proof. All this can be deduced by using our various general formulae, as follows:

(1) This is something that we already know, which is elementary:

$$\begin{vmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_N \end{vmatrix} = \lambda_1 \ldots \lambda_N$$

(2) This is follows by using Theorem 2.11 and Theorem 2.17:

$$\begin{vmatrix} \lambda_1 & & * \\ & \ddots & \\ & & \lambda_N \end{vmatrix} = \lambda_1 \ldots \lambda_N$$

(3) This follows as well by using Theorem 2.11 and Theorem 2.17:

$$\begin{vmatrix} \lambda_1 & & \\ & \ddots & \\ * & & \lambda_N \end{vmatrix} = \lambda_1 \ldots \lambda_N$$

To be more precise, Theorem 2.17 reduces the computations (2,3) to (1). □

Summarizing, the rules in Theorem 2.11 and Theorem 2.17 are quite powerful, taken altogether. For future reference, let us record the complete list of these rules:

Theorem 2.19. *The determinant has the following properties:*

(1) *When adding two columns, the determinants get added:*

$$\begin{aligned} \det(u + v, w_2, \ldots, w_N) &= \det(u, w_2, \ldots, w_N) \\ &+ \det(v, w_2, \ldots, w_N) \end{aligned}$$

(2) *When multiplying a column by a scalar, the determinant gets multiplied:*

$$\det(\lambda v_1, v_2 \ldots, v_N) = \lambda \det(v_1, \ldots, v_N)$$

(3) *When permuting two columns, the determinant changes the sign:*

$$\det(\ldots, v, \ldots, w, \ldots) = -\det(\ldots, w, \ldots, v, \ldots)$$

(4) *The determinant* $\det(e_1, \ldots, e_N)$ *of the standard basis of* $\mathbb{R}^N$ *is* 1.

Proof. This follows indeed by putting together Theorem 2.11 and Theorem 2.17. □

As an important theoretical result now, we have:

Theorem 2.20. *The determinant of square matrices is the unique map*

$$\det : M_N(\mathbb{R}) \to \mathbb{R}$$

satisfying the conditions in Theorem 2.19 above.

Proof. This follows indeed by putting the matrix in upper triangular form. □

Here is now an important theoretical result:

Theorem 2.21. *The determinant is subject to the row expansion formula*

$$\begin{aligned}
\begin{vmatrix} a_{11} & \ldots & a_{1N} \\ \vdots & & \vdots \\ a_{N1} & \ldots & a_{NN} \end{vmatrix} &= a_{11} \begin{vmatrix} a_{22} & \ldots & a_{2N} \\ \vdots & & \vdots \\ a_{N2} & \ldots & a_{NN} \end{vmatrix} \\
&- a_{12} \begin{vmatrix} a_{21} & a_{23} & \ldots & a_{2N} \\ \vdots & \vdots & & \vdots \\ a_{N1} & a_{N3} & \ldots & a_{NN} \end{vmatrix} \\
&\vdots \\
&\vdots \\
&+ (-1)^{N+1} a_{1N} \begin{vmatrix} a_{21} & \ldots & a_{2,N-1} \\ \vdots & & \vdots \\ a_{N1} & \ldots & a_{N,N-1} \end{vmatrix}
\end{aligned}$$

and this method fully computes it, by recurrence.

Proof. This follows either by doing some geometric computations, in the spirit of those from the proof of Theorem 2.17 above, or just by using Theorem 2.20.

Indeed, it is clear the formula in the statement, used by recurrence, produces a certain function $\det : M_N(\mathbb{R}) \to \mathbb{R}$, which has the 4 properties in Theorem 2.19. □

We can expand as well over the columns, as follows:

Theorem 2.22. *The determinant is subject to the column expansion formula*

$$\begin{vmatrix} a_{11} & \ldots & a_{1N} \\ \vdots & & \vdots \\ a_{N1} & \ldots & a_{NN} \end{vmatrix} = a_{11} \begin{vmatrix} a_{22} & \ldots & a_{2N} \\ \vdots & & \vdots \\ a_{N2} & \ldots & a_{NN} \end{vmatrix}$$
$$- a_{21} \begin{vmatrix} a_{12} & \ldots & a_{1N} \\ a_{32} & \ldots & a_{3N} \\ \vdots & & \vdots \\ a_{N2} & \ldots & a_{NN} \end{vmatrix}$$
$$\vdots$$
$$\vdots$$
$$+ (-1)^{N+1} a_{N1} \begin{vmatrix} a_{12} & \ldots & a_{1N} \\ \vdots & & \vdots \\ a_{N-1,2} & \ldots & a_{N-1,N} \end{vmatrix}$$

and this method fully computes it, by recurrence.

Proof. Once again, this follows either by doing some geometric computations, in the spirit of those from the proof of Theorem 2.17 above, or just by using Theorem 2.20.

Indeed, it is clear the formula in the statement, used by recurrence, produces a certain function $\det : M_N(\mathbb{R}) \to \mathbb{R}$, which has the 4 properties in Theorem 2.19. □

Summarizing, we have a very efficient way of computing the determinant, which is purely algorithmic.

Finally, we have one more theoretical result, as follows:

Theorem 2.23. *The determinant of the systems of vectors*

$$\det : \mathbb{R}^N \times \ldots \times \mathbb{R}^N \to \mathbb{R}$$

is multilinear, alternate and unital, and unique with these properties.

Proof. Here the properties of det are something that we already know, from the various results established above.

As for the uniqueness assertion, this follows by doing some abstract algebra, with antisymmetric tensors, inspired by Theorem 2.21 and Theorem 2.22 above. □

Summarizing, we have now a full theory for the determinant.

With this technology, we can now prove:

Theorem 2.24. *The determinant of the 3×3 matrices is given by*

$$\begin{vmatrix} a & b & c\\ d & e & f\\ g & h & i\end{vmatrix} = aei+bfg+cdh-ceg-bdi-afh$$

which can be memorized by using Sarrus' triangle method,

$$\begin{aligned}\det &= \begin{pmatrix} * & & \\ & * & \\ & & *\end{pmatrix}+\begin{pmatrix} & * & \\ & & *\\ *& & \end{pmatrix}+\begin{pmatrix} & & *\\ *& & \\ & *& \end{pmatrix}\\ &-\begin{pmatrix} & & *\\ & * & \\ *& & \end{pmatrix}+\begin{pmatrix} & * & \\ *& & \\ & & *\end{pmatrix}+\begin{pmatrix} *& & \\ & & *\\ & *& \end{pmatrix}\end{aligned}$$

"triangles parallel to the diagonal, minus triangles parallel to the antidiagonal".

Proof. Here is the computation, using Theorem 2.21 above:

$$\begin{aligned}&\begin{vmatrix} a & b & c\\ d & e & f\\ g & h & i\end{vmatrix}\\ =\ & a\begin{vmatrix} e & f\\ h & i\end{vmatrix}-b\begin{vmatrix} d & f\\ g & i\end{vmatrix}+c\begin{vmatrix} d & e\\ g & h\end{vmatrix}\\ =\ & a(ei-fh)-b(di-fg)+c(dh-eg)\\ =\ & aei-afh-bdi+bfg+cdh-ceg\\ =\ & aei+bfg+cdh-ceg-bdi-afh\end{aligned}$$

Thus, we obtain the formula in the statement. □

As a first application, let us go back to the inversion problem for the 3×3 matrices, that we left open in section 1 above.

We can now solve this problem, as follows:

Theorem 2.25. *The inverses of the 3×3 matrices are given by*

$$\begin{pmatrix} a & b & c\\ d & e & f\\ g & h & i\end{pmatrix}^{-1} = \frac{1}{D}\begin{pmatrix} ei-fh & ch-bi & bf-ce\\ fg-di & ai-cg & cd-af\\ dh-eg & bg-ah & ae-bd\end{pmatrix}$$

with D being the determimant. When $D=0$, the matrix is not invertible.

Proof. We can use here the same method as for the 2×2 matrices. To be more precise, in order for the matrix to be invertible, we must have:

$$D\neq 0$$

The trick now is to look for solutions of the following problem:

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \begin{pmatrix} * & * & * \\ * & * & * \\ * & * & * \end{pmatrix} = \begin{pmatrix} D & 0 & 0 \\ 0 & D & 0 \\ 0 & 0 & D \end{pmatrix}$$

We know from Theorem 2.24 above that the determinant is given by:

$$D = aei + bfg + cdh - ceg - bdi - afh$$

But this leads, via some obvious choices, to the following solution:

$$\begin{pmatrix} * & * & * \\ * & * & * \\ * & * & * \end{pmatrix} = \begin{pmatrix} ei - fh & ch - bi & bf - ce \\ fg - di & ai - cg & cd - af \\ dh - eg & bg - ah & ae - bd \end{pmatrix}$$

Thus, by rescaling, we obtain the formula in the statement. □

In fact, we can now fully solve the inversion problem, as follows:

Theorem 2.26. *The inverse of a square matrix, having nonzero determinant,*

$$A = \begin{pmatrix} a_{11} & \ldots & a_{1N} \\ \vdots & & \vdots \\ a_{N1} & \ldots & a_{NN} \end{pmatrix}$$

is given by the following formula,

$$A^{-1} = \frac{1}{\det A} \begin{pmatrix} \det A^{(11)} & -\det A^{(21)} & \det A^{(31)} & \ldots \\ -\det A^{(12)} & \det A^{(22)} & -\det A^{(32)} & \ldots \\ \det A^{(13)} & -\det A^{(23)} & \det A^{(33)} & \ldots \\ \vdots & \vdots & \vdots & \end{pmatrix}$$

where $A^{(ij)}$ is the matrix A, with the i-th row and j-th column removed.

Proof. This follows indeed by using the row expansion formula from Theorem 2.21, which in terms of the matrix A^{-1} in the statement reads $AA^{-1} = 1$. □

In practice, the above result leads to the following algorithm, which is quite easy to memorize, for computing the inverse:

(1) Delete rows and columns, and compute the corresponding determinants.

(2) Transpose, and add checkered signs.

(3) Divide by the determinant.

Observe that this generalizes indeed our computations at $N = 2, 3$.

Let us discuss now the general formula of the determinant, generalizing those that we have at $N = 2, 3$.

In order to formulate our result, we will need:

Definition 2.27. *A permutation of* $\{1, \ldots, N\}$ *is a bijection, as follows:*

$$\sigma : \{1, \ldots, N\} \to \{1, \ldots, N\}$$

The set of such permutations is denoted S_N.

As basic examples, we have permutations of 2,3,4 elements.
These are best denoted as diagrams, going from top to bottom.

Here are some basic properties of the permutations:

Theorem 2.28. *The permutations have the following properties:*

(1) *There are* $N!$ *of them.*
(2) *They are stable by composition, and inversion.*

Proof. All this is standard:

(1) Here we can proceed by recurrence. Indeed, we have:
– N choices for the value of $\sigma(N)$.
– $(N-1)$ choices for the value of $\sigma(N-1)$.
– $(N-2)$ choices for the value of $\sigma(N-2)$.
⋮
⋮
– and so on, up to 1 choice for the value of $\sigma(1)$.
Summing up, the number of choices for a permutation $\sigma \in S_N$ is, as desired:

$$N(N-1)(N-2)\ldots..1 = N!$$

(2) This is clear, indeed. □

We will see later on, in section 7 below, that S_N is a so-called group.

We will need as well:

Theorem 2.29. *Signatures:*

(1) *Defined via inversions.*
(2) *Alternatively, via transpositions.*
(3) *Or via cycle decomposition.*

Proof. This is indeed quite standard. □

We will see later on that the signature is a so-called representation.

We can now formulate a key result, as follows:

Theorem 2.30. *Formula of the determinant,*

$$\det A = \sum_{\sigma\in S_N} \varepsilon(\sigma) A_{1\sigma(1)} \ldots A_{N\sigma(N)}$$

with the signature function being the one introduced above.

Proof. Indeed, when computing the determinant by using the standard rules, we are led into permutations, and into the formula in the statement. □

As a basic example, in 2 dimensions we recover the usual formula:

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$$

In 3 dimensions, we recover the Sarrus formula:

$$\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = aei + bfg + cdh - ceg - bdi - afh$$

Observe that the triangles in the Sarrus formula correspond to the permutations of $\{1, 2, 3\}$, and their signs correspond to the signatures of these permutations:

$$\begin{aligned} \det \;=\; & \begin{pmatrix} * & & \\ & * & \\ & & * \end{pmatrix} + \begin{pmatrix} & * & \\ & & * \\ * & & \end{pmatrix} + \begin{pmatrix} & & * \\ * & & \\ & * & \end{pmatrix} \\ - \; & \begin{pmatrix} & & * \\ & * & \\ * & & \end{pmatrix} + \begin{pmatrix} & * & \\ * & & \\ & & * \end{pmatrix} + \begin{pmatrix} * & & \\ & & * \\ & * & \end{pmatrix} \end{aligned}$$

We will be back to this, with comments and examples.

As a first new application, we have:

Theorem 2.31. *The determinant of a* 4 *dimensions is given by*

$$\begin{vmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{vmatrix} = \ldots$$

with 24 *terms in the sum.*

Proof. This follows indeed from our formula, because we have:

$$\begin{vmatrix} a & b & c & d\\ e & f & g & h\\ i & j & k & l\\ m & n & o & p \end{vmatrix} = a\begin{vmatrix} f & g & h\\ j & k & l\\ n & o & p \end{vmatrix} - b\begin{vmatrix} e & g & h\\ i & k & l\\ m & o & p \end{vmatrix} + c\begin{vmatrix} e & f & h\\ i & j & l\\ m & n & p \end{vmatrix} - d\begin{vmatrix} e & f & g\\ i & j & k\\ m & n & o \end{vmatrix}$$

Thus, we are led to the formula in the statement. □

We will be back to this, with some applications.

We have as well the following theoretical result:

Theorem 2.32. *We have the formula*

$$\det A = \det A^t$$

valid for any square matrix A.

Proof. This follows from the general formula in Theorem 2.30 above. Indeed, when transposing, we obtain:

$$\begin{aligned} \det A^t &= \sum_{\sigma\in S_N} \varepsilon(\sigma)(A^t)_{1\sigma(1)}\ldots(A^t)_{N\sigma(N)}\\ &= \sum_{\sigma\in S_N} \varepsilon(\sigma)A_{\sigma(1)1}\ldots A_{\sigma(N)N}\\ &= \sum_{\sigma\in S_N} \varepsilon(\sigma)A_{1\sigma^{-1}(1)}\ldots A_{N\sigma^{-1}(N)}\\ &= \sum_{\sigma\in S_N} \varepsilon(\sigma^{-1})A_{1\sigma^{-1}(1)}\ldots A_{N\sigma^{-1}(N)}\\ &= \sum_{\sigma\in S_N} \varepsilon(\sigma)A_{1\sigma(1)}\ldots A_{N\sigma(N)}\\ &= \det A \end{aligned}$$

Thus, we are led to the formula in the statement. □

As a comment here, we have seen so far several points of view on the determinant, in terms of families of vectors, or matrices, or linear maps, as well as several techniques for the explicit computation of the determinant. The above formula $\det A = \det A^t$, coming at the end in the present presentation, is perhaps the most subtle one.

Here is now a nice and important example:

Theorem 2.33. *We have the Vandermonde determinant formula*

$$\begin{vmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_N \\ \vdots & \vdots & & \vdots \\ x_1^{N-1} & x_2^{N-1} & \ldots & x_N^{N-1} \end{vmatrix} = \prod_{i>j}(x_i - x_j)$$

valid for any $x_1, \ldots, x_N \in \mathbb{R}$.

Proof. This is indeed routine, by using the basic theory of polynomials.

Indeed, by expanding over the columns, the determinant in question, say D, is a polynomial in the variables $x_1, \ldots, x_N$, having degree $N-1$ in each variable.

Now since $x_i = x_j$ makes D vanish, for any $i \neq j$, we conclude that we must have:

$$D = c\prod_{i>j}(x_i - x_j)$$

As for the constant $c \in \mathbb{R}$, this can be computed by recurrence, and we obtain:

$$c = 1$$

Thus, we are led to the formula in the statement. □

We will be back to this, with some applications.

Let us discuss now some theoretical applications of the determinant.

First, we have the following key statement:

Theorem 2.34. *We have the following results:*

(1) *Caracteristic polynomial.*
(2) *Eigenvalues.*

Proof. This is routine, indeed, by using the following fact:

$$Av = \lambda v \iff (A - \lambda 1_N)v = 0$$

In order for this to hold, we must have:

$$\det(A - \lambda 1_N) = 0$$

Thus, we are led to the conclusion in the statement. □

There are many examples of applications here.

We have the following result:

Theorem 2.35. *The trace is the sum of the eigenvalues.*

Proof. This is clear, indeed. □

In general, the symmetric functions of the eigenvalues are given by some quite complicated formulae. We will be back to this, later on.

We have the following result:

Theorem 2.36. *Diagonalization.*

Proof. This is indeed routine. □

We will be back to this topic, on several occasions.

In practice, in order to apply the above result, we will need:

Theorem 2.37. *Factorization of real polynomials, tricks:*

(1) *For $P \in \mathbb{Z}[X]$, look for integer solutions first.*
(2) *Use the sum and the product of the roots.*
(3) *Use real analysis, and the graph.*
(4) *Other tricks.*

Proof. This is indeed routine. □

Examples, we have:

Theorem 2.38. *Diagonalization in* 3 *dimensions.*

Proof. This is something quite tricky, and there is some discussion here. □

Summarizing, we have a nice theory, but this still does not apply to all the real matrices, such as the rotations, which do not have real eigenvalues.

3. Complex matrices

We have seen in the previous section that the study of the real matrices $A \in M_N(\mathbb{R})$ suggests the use of the complex numbers. Indeed, even simple matrices like the 2×2 ones can, at least in a formal sense, have complex eigenvalues.

In what follows we discuss the theory of the complex matrices $A \in M_N(\mathbb{C})$. We will see that the theory here is much more complete than in the real case.

Also, as an application, we will solve in this way the problems left open in the real case, concerning the diagonalization.

Let us begin with the complex numbers. The definition is as follows:

Definition 3.1. *The complex numbers are variables of the form*

$$x = a + ib$$

which add in the obvious way, and multiply according to the rule:

$$i^2 = -1$$

In other words, we consider variables as above, without bothering for the moment with their precise meaning. Consider now two such complex numbers:

$$x = a + ib$$

$$y = c + id$$

The formulae for the sum and for the product are then as follows:

$$x + y = (a + c) + i(b + d)$$

$$xy = (ac - bd) + i(ad + bc)$$

Observe that we have used here, for the multiplication, the formula $i^2 = -1$:

$$\begin{aligned} xy &= (a + ib)(c + id) \\ &= ac + iad + ibc + i^2bd \\ &= ac + iad + ibc - bd \\ &= (ac - bd) + i(ad + bc) \end{aligned}$$

The advantage of using the complex numbers comes from the fact that the equation $x^2 = 1$ has now a solution, $x = i$. In fact, this equation has two solutions, namely:

$$x = \pm i$$

More generally, we have the following key result, regarding the arbitrary degree 2 equations:

Theorem 3.2. *The complex solutions of $ax^2+bx+c=0$ with $a,b,c\in\mathbb{R}$ are*

$$x_{1,2}=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$$

with the square root of negative numbers $n<0$ being defined as:

$$\sqrt{n}=\pm i\sqrt{-n}$$

Proof. We can write our equation in the following way:

$$\begin{aligned}
& ax^2+bx+c=0\\
\iff\quad & x^2+\frac{b}{a}x+\frac{c}{a}=0\\
\iff\quad & \left(x+\frac{b}{2a}\right)^2-\frac{b^2}{4a^2}+\frac{c}{a}=0\\
\iff\quad & \left(x+\frac{b}{2a}\right)^2=\frac{b^2-4ac}{4a^2}\\
\iff\quad & x+\frac{b}{2a}=\pm\frac{\sqrt{b^2-4ac}}{2a}
\end{aligned}$$

Thus, we are led to the conclusion in the statement. □

We will see later that any degree 2 complex equation has solutions. And that, even more generally, any degree N equation, real or complex, with $N\in\mathbb{N}$, has solutions.

We can represent the complex numbers in the plane, in the obvious way. The sum is the usual sum. In order to understand the multiplication, however, we must use:

Theorem 3.3. *The complex numbers $z=a+ib$ can be written in polar coordinates,*

$$z=re^{it}$$

with the connecting formulae being

$$a=r\cos t$$

$$b=r\sin t$$

and in the other sense being

$$r=\sqrt{a^2+b^2}$$

$$\tan t=b/a$$

and with r,t being called modulus, and argument.

Proof. This is something deep, requiring advanced trigonometry, and calculus. □

As a consequence of the above, observe that we have:

$$e^{\pi i} = -1$$

Once again this is something deep, based on advanced trigonometry, and calculus.

We can now go back to the addition and multiplication, and we have:

Theorem 3.4. *In polar coordinates, the complex numbers multiply as*

$$re^{it} \cdot r'e^{it'} = rr'e^{i(t+t')}$$

with the arguments t, t' being taken modulo 2π.

Proof. This follows indeed from Theorem 3.3 above. □

As we will soon see, the above multiplication formula is very powerful.

However, observe that in polar coordinates we do not have a simple formula for the sum. Thus, this formalism has its limitations.

We have as well more complicated operations, as follows:

Theorem 3.5. *We have the following operations on the complex numbers, which in polar form are as follows:*

(1) *Inversion:* $(re^{it})^{-1} = r^{-1}e^{-it}$.
(2) *Square roots:* $\sqrt{re^{it}} = \pm\sqrt{r}e^{it/2}$.
(3) *Powers:* $(re^{it})^a = r^a e^{ita}$.

Proof. This is standard, the idea being as follows:
(1) We have indeed the following computation, using Theorem 3.4:

$$\begin{aligned}(re^{it})(r^{-1}e^{-it}) &= rr^{-1} \cdot e^{i(t-t)}\\ &= 1 \cdot 1\\ &= 1\end{aligned}$$

(2) Once again by using Theorem 3.4, we have:

$$\begin{aligned}(\pm\sqrt{r}e^{it/2})^2 &= (\sqrt{r})^2 e^{i(t/2+t/2)}\\ &= re^{it}\end{aligned}$$

(3) Given an arbitrary number $a \in \mathbb{R}$, we can define, as stated:

$$(re^{it})^a = r^a e^{ita}$$

Due to Theorem 3.4, this operation $z \to z^a$ is indeed the correct one. □

With the above results in hand, and notably with the square root formula from Theorem 3.5 (2), we can now go back to the degree 2 equations, and we have:

Theorem 3.6. *The complex solutions of $az^2+bz+c=0$ with $a,b,c\in\mathbb{C}$ are*

$$z_{1,2}=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$$

with the square root of complex numbers being defined as above.

Proof. This is clear, the computations being the same as in the real case. To be more precise, our degree 2 equation can be written as follows:

$$\left(z+\frac{b}{2a}\right)^2=\frac{b^2-4ac}{4a^2}$$

Now since we know from Theorem 3.5 (2) that any complex number has a square root, we are led to the conclusion in the statement. □

We will be back later to polynomial equations, with a proof for the fact that any such equation, of arbitrary degree N, has N complex solutions, counted with multiplicities.

As a last topic regarding the complex numbers, we have:

Theorem 3.7. *The equation $z^N=1$ has N complex solutions, namely*

$$\left\{w^k\Big|k=0,1,\ldots,N-1\right\}\quad:\quad w=e^{2\pi i/N}$$

which are called roots of unity of order N.

Proof. This follows by using Theorem 3.4. Indeed, with $z=re^{it}$ our equation reads:

$$r^Ne^{itN}=1$$

Thus $r=1$, and $t\in[0,2\pi)$ must be a multiple of $2\pi/N$, as stated. □

The roots of unity are very useful variables, and have many interesting properties. Here is a basic such property, to be used many times in what follows:

Theorem 3.8. *The roots of unity have the property*

$$\sum_{k=1}^{N}(w^k)^s=N\delta_{N|s}$$

where on the right we have a Kronecker symbol.

Proof. This follows from the fact that the numbers in the statement form a regular polygon centered at 0. Indeed, the barycenter of this polygon is given by:

$$\frac{1}{N}\sum_{k=1}^{N}(w^k)^s=\delta_{N|s}$$

Thus, we obtain the formula in the statement. □

We will be back to more things regarding the complex numbers, and the roots of unity, later on.

In relation now with linear algebra, our first task is that of extending the results that we know, from the real case, to the complex case.

Let us begin with some very basic results. As in the real case, we have:

Theorem 3.9. *The linear maps $f : \mathbb{C}^N \to \mathbb{C}^M$ are the maps of the form*

$$f(v) = Av$$

with A being a rectangular matrix, $A \in M_{M\times N}(\mathbb{C})$.

Proof. This follows exactly as in the real case.

Indeed, a linear map $f : \mathbb{C}^N \to \mathbb{C}^M$ must send a vector $x \in \mathbb{C}^N$ to a certain vector $f(x) \in \mathbb{C}^M$, all whose components are linear combinations of the components of x. Thus, we can write, for certain complex numbers $a_{ij} \in \mathbb{C}$:

$$f\begin{pmatrix} x_1 \\ \vdots \\ \vdots \\ x_N \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + \ldots + a_{1N}x_N \\ \vdots \\ \vdots \\ a_{M1}x_1 + \ldots + a_{MN}x_N \end{pmatrix}$$

Now the parameters $a_{ij} \in \mathbb{C}$ can be regarded as being the entries of a rectangular matrix, as follows:

$$A \in M_{M\times N}(\mathbb{C})$$

With the usual convention for the rectangular matrix multiplication, the above formula is precisely the one in the statement, namely:

$$f(x) = Ax$$

Thus, we areled to the conclusion in the statement. □

We have as well the following result:

Theorem 3.10. *A linear map $f : \mathbb{C}^N \to \mathbb{C}^M$, written as*

$$f(v) = Av$$

is invertible precisely when A is invertible, and in this case we have:

$$f^{-1}(v) = A^{-1}v$$

Proof. This is indeed standard, as in the real case, coming from:

$$f_A f_B(v) = f_{AB}(v)$$

Indeed, this shows that $f_A f_B = 1$ is equivalent to $AB = 1$. □

With respect to the real case, some subtleties appear at the level of the scalar products, isometries and projections.

The complex theory of the scalar products is as follows:

Theorem 3.11. *Consider the usual scalar product on $\mathbb{C}^N$, namely:*

$$< x, y >= \sum_i x_i \bar{y}_i$$

(1) *We have the following formula, where $(A^*)_{ij} = \bar{A}_{ji}$ is the adjoint matrix:*

$$< Ax, y >=< x, A^* y >$$

(2) *A linear map $f : \mathbb{C}^N \to \mathbb{C}^N$, written as $f(x) = Ux$ with $U \in M_N(\mathbb{C})$, is an isometry precisely when U is unitary, in the sense that:*

$$U^* = U^{-1}$$

(3) *A linear map $f : \mathbb{C}^N \to \mathbb{C}^N$, written as $f(x) = Px$ with $P \in M_N(\mathbb{C})$, is a porojection precisely when P is projection, in the sense that:*

$$P = P^2 = P^*$$

(4) *The formula for the rank 1 projections is as follows:*

$$P_x = \frac{1}{||x||}(x_i \bar{x}_j)_{ij}$$

Proof. We follow the study in the real case:

(1) The formula of the adjoint is indeed as follows:

$$< Ax, y >=< x, A^* y >$$

(2) The condition for the isometries is as follows:

$$U^* = U^{-1}$$

(3) As for the condition for the projections, this is as follows:

$$P = P^2 = P^*$$

(4) The formula of the rank 1 projections is as follows:

$$P_x = \frac{1}{||x||}(x_i \bar{x}_j)_{ij}$$

The proofs are similar to those in the real case. □

The basic examples are similar to those from the real case. We will be back to this, later on, with standard examples, and more advanced examples as well.

We can talk about eigenvalues and eigenvectors, as follows:

Definition 3.12. *Let $A \in M_N(\mathbb{C})$ be a square matrix. When $Av = \lambda v$ we say that:*

(1) *v is an eigenvector of A.*
(2) *λ is an eigenvalue of A.*

We say that A is diagonalizable when it has a basis of eigenvectors.

When A is diagonalizable, in that basis we can write:

$$A = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_N \end{pmatrix}$$

In general, this means that we have a formula as follows, with D diagonal:

$$A = PDP^{-1}$$

Indeed, we can take P to be the matrix formed by the eigenvectors:

$$P = [v_1 \ldots v_N]$$

We have many examples here, similar to those in the real case.

At the theoretical level, we have the following result:

Theorem 3.13. *If the matrix has N distinct eigenvalues, it is diagonalizable.*

Proof. This looks quite clear from definitions, because in each of the N directions of the eigenvectors, the matrix must multiply by a certain scalar.

However, the point is that of showing that these N directions do not "overlap", and this comes from the fact that the corresponding eigenvalues are different. □

The basic examples are similar to those in the real case.

As a first interesting result, we can now diagonalize the rotations in the real plane:

Theorem 3.14. *The rotation of angle $t \in \mathbb{R}$ in the real plane,*

$$R_t = \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix}$$

can be diagonalized over the complex numbers, as follows:

$$R_t = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}\begin{pmatrix} e^{-it} & 0 \\ 0 & e^{it} \end{pmatrix}\begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix}$$

Proof. The rotation of angle $t \in \mathbb{R}$ in the real plane a complex eigenvector, as follows:

$$\begin{aligned} & R_t\begin{pmatrix}1\\ i\end{pmatrix}\\ = & \begin{pmatrix}\cos t - i\sin t\\ \sin t + i\cos t\end{pmatrix}\\ = & e^{-it}\begin{pmatrix}1\\ i\end{pmatrix}\end{aligned}$$

We have as well a second eigenvector, as follows:

$$\begin{aligned} & R_t\begin{pmatrix}1\\ -i\end{pmatrix}\\ = & \begin{pmatrix}\cos t + i\sin t\\ \sin t - i\cos t\end{pmatrix}\\ = & e^{it}\begin{pmatrix}1\\ -i\end{pmatrix}\end{aligned}$$

Thus R_t is diagonalizable over $\mathbb{C}$. To be more precise, we have:

$$R_t = \frac{1}{2}\begin{pmatrix}1 & 1\\ i & -i\end{pmatrix}\begin{pmatrix}e^{-it} & 0\\ 0 & e^{it}\end{pmatrix}\begin{pmatrix}1 & -i\\ 1 & i\end{pmatrix}$$

Thus, we are led to the conclusion in the statement. □

In connection with the above result, observe also that the rotation of angle $t \in \mathbb{R}$ in the real plane can be regarded as a 1×1 complex matrix, as follows:

$$R_t = (e^{it})$$

Summarizing, either way, things are simpler with complex numbers.

We will come back to the diagonalization question for rotations later, after developing the theory of the determinant.

Regarding now the determinant, have we have to follow an abstract approach, due to our lack of intuition with $\mathbb{C}^N$, at $N \geq 2$.

Let us start with the following definition:

Definition 3.15. *The determinant of a complex matrix $A \in M_N(\mathbb{C})$ is given by*

$$\det A = \sum_{\sigma \in S_N} \varepsilon(\sigma) A_{1\sigma(1)} \ldots A_{N\sigma(N)}$$

with $\varepsilon = \pm 1$ being the signature of the permutations.

Generally speaking, the theory of the determinant from the real case extends well, and we have the following result, summarizing the needed properties and formulae:

Theorem 3.16. *The determinant has the following properties:*

(1) *When adding two columns, the determinants get added:*

$$\begin{aligned}\det(u+v,w_2,\ldots,w_N) &= \det(u,w_2,\ldots,w_N)\\ &+ \det(v,w_2,\ldots,w_N)\end{aligned}$$

(2) *When multiplying a column by a scalar, the determinant gets multiplied:*

$$\det(\lambda v_1,v_2\ldots,v_N)=\lambda\det(v_1,\ldots,v_N)$$

(3) *When permuting two columns, the determinant changes the sign:*

$$\det(\ldots,v,\ldots,w,\ldots)=-\det(\ldots,w,\ldots,v,\ldots)$$

(4) *The determinant* $\det(e_1,\ldots,e_N)$ *of the standard basis of* $\mathbb{C}^N$ *is* 1.

Proof. This follows indeed by doing some algebraic computations, based on the formula of the determinant from Definition 3.15 above. □

We have as well the following result, which is very useful in practice:

Theorem 3.17. *The determinant is subject to the row expansion formula*

$$\begin{aligned}\begin{vmatrix} a_{11} & \ldots & a_{1N}\\ \vdots & & \vdots\\ a_{N1} & \ldots & a_{NN}\end{vmatrix} &= a_{11}\begin{vmatrix} a_{22} & \ldots & a_{2N}\\ \vdots & & \vdots\\ a_{N2} & \ldots & a_{NN}\end{vmatrix}\\ &- a_{12}\begin{vmatrix} a_{21} & a_{23} & \ldots & a_{2N}\\ \vdots & \vdots & & \vdots\\ a_{N1} & a_{N3} & \ldots & a_{NN}\end{vmatrix}\\ &\vdots\\ &\vdots\\ &+ (-1)^{N+1}a_{1N}\begin{vmatrix} a_{21} & \ldots & a_{2,N-1}\\ \vdots & & \vdots\\ a_{N1} & \ldots & a_{N,N-1}\end{vmatrix}\end{aligned}$$

and this method fully computes it, by recurrence.

Proof. This follows indeed by doing some algebraic computations. □

We can expand as well over the columns, as follows:

Theorem 3.18. *The determinant is subject to the column expansion formula*

$$\begin{vmatrix} a_{11} & \ldots & a_{1N} \\ \vdots & & \vdots \\ a_{N1} & \ldots & a_{NN} \end{vmatrix} = a_{11} \begin{vmatrix} a_{22} & \ldots & a_{2N} \\ \vdots & & \vdots \\ a_{N2} & \ldots & a_{NN} \end{vmatrix}$$
$$- a_{21} \begin{vmatrix} a_{12} & \ldots & a_{1N} \\ a_{32} & \ldots & a_{3N} \\ \vdots & & \vdots \\ a_{N2} & \ldots & a_{NN} \end{vmatrix}$$
$$\vdots$$
$$\vdots$$
$$+ (-1)^{N+1} a_{N1} \begin{vmatrix} a_{12} & \ldots & a_{1N} \\ \vdots & & \vdots \\ a_{N-1,2} & \ldots & a_{N-1,N} \end{vmatrix}$$

and this method fully computes it, by recurrence.

Proof. Once again, this follows by doing some algebraic computations. □

Summarizing, the theory from the real case extends well.

As in the real case, as an application, we have:

Theorem 3.19. *The inverse of a square matrix, having nonzero determinant,*

$$A = \begin{pmatrix} a_{11} & \ldots & a_{1N} \\ \vdots & & \vdots \\ a_{N1} & \ldots & a_{NN} \end{pmatrix}$$

is given by the following formula,

$$A^{-1} = \frac{1}{\det A} \begin{pmatrix} \det A^{(11)} & -\det A^{(21)} & \det A^{(31)} & \ldots \\ -\det A^{(12)} & \det A^{(22)} & -\det A^{(32)} & \ldots \\ \det A^{(13)} & -\det A^{(23)} & \det A^{(33)} & \ldots \\ \vdots & \vdots & \vdots & \end{pmatrix}$$

where $A^{(ij)}$ is the matrix A, with the i-th row and j-th column removed.

Proof. This follows indeed by using the row expansion formula from Theorem 3.17, which in terms of the matrix A^{-1} in the statement reads $AA^{-1} = 1$. □

Finally, let us record the following result:

Theorem 3.20. *We have the formula*

$$\det A = \det A^t$$

valid for any square matrix A.

Proof. This follows from the general formula in Definition 3.15 above. Indeed, when transposing, we obtain:

$$\begin{aligned}
\det A^t &= \sum_{\sigma\in S_N} \varepsilon(\sigma)(A^t)_{1\sigma(1)}\ldots(A^t)_{N\sigma(N)} \\
&= \sum_{\sigma\in S_N} \varepsilon(\sigma)A_{\sigma(1)1}\ldots A_{\sigma(N)N} \\
&= \sum_{\sigma\in S_N} \varepsilon(\sigma)A_{1\sigma^{-1}(1)}\ldots A_{N\sigma^{-1}(N)} \\
&= \sum_{\sigma\in S_N} \varepsilon(\sigma^{-1})A_{1\sigma^{-1}(1)}\ldots A_{N\sigma^{-1}(N)} \\
&= \sum_{\sigma\in S_N} \varepsilon(\sigma)A_{1\sigma(1)}\ldots A_{N\sigma(N)} \\
&= \det A
\end{aligned}$$

Thus, we are led to the formula in the statement. □

Let us discuss now the diagonalization procedure, for some basic complex matrices, by using the determinant theory developed above.

We begin with a study for the 2×2 matrices. Here the theory and computations are quite elementary, and the complete result is as follows:

Theorem 3.21. *Diagonalization in 2 dimensions, for the matrices*

$$A=\begin{pmatrix} a & b\\ c & d\end{pmatrix}$$

with $a,b,c,d\in\mathbb{C}$, full discussion.

Proof. Consider indeed an arbitrary 2×2 matrix, written as follows:

$$A=\begin{pmatrix} a & b\\ c & d\end{pmatrix}$$

The trace and determinant of this matrix are as follows:

$$Tr(A)=a+d$$

$$\det A=ad-bc$$

We deduce from this, and this even without computation, that the characteristic polynomial is given by:

$$P(X) = X^2 - (a+d)X + (ac - bd)$$

We have then 2 complex roots, and so 2 complex eigenvalues. □

As a conclusion, things are simpler, and more complete, in the complex case.

We will be back to this in the next section, with full theory on the subject. We will diagonalize there all the matrices that can be diagonalized.

Let us discuss now some interesting examples of complex matrices, which definitely do not exist in the real setting, namely the Fourier ones.

Let us start with the following definition:

Definition 3.22. *The Fourier matrix is as follows,*

$$F = \frac{1}{\sqrt{N}}(w^{ij})_{ij}$$

with $w = e^{2\pi i/N}$, and with the convention that the indices are

$$i, j \in \{0, 1, \ldots, N-1\}$$

and are usually taken modulo N.

Here the conventions regarding the indices are standard, and are there for various reasons, as for instance for having the first row and column consisting of 1 entries.

In fact, in standard matrix form, and with the above conventions for the indices, the Fourier matrix is as follows:

$$F = \frac{1}{\sqrt{N}}\begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & w & w^2 & \ldots & w^{N-1} \\ 1 & w^2 & w^4 & \ldots & w^{2(N-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & w^{N-1} & w^{2(N-1)} & \ldots & w^{(N-1)^2} \end{pmatrix}$$

Observe that this is a Vandermonde matrix, in the sense of section 2 above, so we know how to compute its determinant. We will be back to this.

Let us record as well the first few values of these matrices:

Proposition 3.23. *The first Fourier matrix is $F_1 = (1)$. The second one is:*

$$F_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

The third Fourier matrix is as follows, with $w = e^{2\pi i/3}$:

$$F_3 = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & 1 & 1 \\ 1 & w & w^2 \\ 1 & w^2 & w \end{pmatrix}$$

As for the fourth Fourier matrix, this is as follows:

$$F_4 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

Proof. All these formulae are clear from definitions, with our usual convention for the indices of the Fourier matrices. □

At the general level now, we first have the following result:

Theorem 3.24. *The Fourier matrix F is unitary.*

Proof. This follows from a standard computation with roots of unity, based on the fact that the barycenter of a regular N-gon centered at 0 is 0. □

Let us discuss now some applications. Given a vector $q \in \mathbb{C}^N$, we denote by $Q \in M_N(\mathbb{C})$ the diagonal matrix having q as vector of diagonal entries. That is:

$$Q_{ii} = q_i \quad , \quad \forall i$$

$$Q_{ij} = 0 \quad , \quad \forall i \neq j$$

With these conventions, we have the following result:

Theorem 3.25. *For a complex matrix $H \in M_N(\mathbb{C})$, the following are equivalent:*

(1) *H is circulant, in the sense that*

$$H_{ij} = \xi_{j-i}$$

for a certain vector $\xi \in \mathbb{C}^N$.

(2) *H is Fourier-diagonal, in the sense that*

$$H = FQF^*$$

for a certain diafonal matrix Q.

In addition, the first row vector of FQF^* is given by:

$$\xi = \frac{Fq}{\sqrt{N}}$$

Proof. If $H_{ij} = \xi_{j-i}$ is circulant then $Q = F^*HF$ is diagonal, given by:

$$\begin{aligned} & Q_{ij} \\ = \ & \frac{1}{N}\sum_{kl} w^{jl-ik}\xi_{l-k} \\ = \ & \delta_{ij}\sum_{r} w^{jr}\xi_r \end{aligned}$$

Also, if $Q = diag(q)$ is diagonal then $H = FQF^*$ is circulant, given by:

$$\begin{aligned} & H_{ij} \\ = \ & \sum_{k} F_{ik}Q_{kk}\bar{F}_{jk} \\ = \ & \frac{1}{N}\sum_{k} w^{(i-j)k}q_k \end{aligned}$$

Observe that this latter formula proves as well the last assertion, namely:

$$\xi = \frac{Fq}{\sqrt{N}}$$

Thus, we have proved the theorem. □

The above result is very useful, and we have many applications.

In relation now with the orthogonal and unitary matrices, we have the following useful result, based on the above:

Theorem 3.26. *The various sets of circulant matrices are as follows:*

(1) *The set of all circulant matrices is:*

$$M_N(\mathbb{C})^{circ} = \left\{FQF^*\middle|q \in \mathbb{C}^N\right\}$$

(2) *The set of all circulant unitary matrices is:*

$$U_N^{circ} = \left\{FQF^*\middle|q \in \mathbb{T}^N\right\}$$

(3) *The set of all circulant orthogonal matrices is:*

$$O_N^{circ} = \left\{FQF^*\middle|q \in \mathbb{T}^N, \bar{q}_i = q_{-i}, \forall i\right\}$$

In addition, in this picture, the first row vector of FQF^* is always given by:

$$\xi = \frac{Fq}{\sqrt{N}}$$

Proof. All this follows from Theorem 3.25, as follows:

(1) This assertion, along with the last one, is Theorem 3.25 itself.

(2) This is clear from (1), because the eigenvalues must be on the unit circle $\mathbb{T}$.

(3) Observe first that for $q \in \mathbb{C}^N$ we have:

$$\overline{Fq} = F\tilde{q}$$

$$\tilde{q}_i = \bar{q}_{-i}$$

Thus $\xi = Fq$ is real if and only if, for any i:

$$\bar{q}_i = q_{-i}$$

Together with (2), this gives the result. □

Once again, the above result is very useful, and we have many applications.

Let us discuss now another application, regarding this time the bistochastic matrices. Here "bistochastic" means having sum 1, on each row and each column.

Note that, by unitarity, the row stochasticity is equivalent to the column stochasticity, and more precisely, we have:

Proposition 3.27. *For a unitary matrix*

$$U \in U_N$$

the row stochasticity is equivalent to the column stochasticity.

Proof. This follows indeed by unitarity, because if ξ denotes the all-a1 vector, we have the following equivalence:

$$H\xi = \xi \iff H^t\xi = \xi$$

Thus, we obtain the result. □

Quite remarkably, the bistochastic matrices are stable under taking products, and we have the following result:

Theorem 3.28. *We have bistochastic groups*

$$B_N \subset O_N$$

$$C_N \subset U_N$$

consisting of matrices which are bistochastic.

Proof. This is trivial, the sets in question being indeed closed under taking products of matrices, and under taking inverses. □

It is possible to show that these coincide with O_{N-1} and U_{N-1}, respectively:

Theorem 3.29. *The groups B_N and C_N, consisting of the bistochastic matrices, are isomorphic to O_{N-1} and U_{N-1}, via a discrete Fourier transform.*

Proof. Let us pick a unitary matrix $F \in U_N$ satisfying the following condition, where ξ is the all-one vector:

$$Fe_0 = \frac{1}{\sqrt{N}}\xi$$

The basic example here is the Fourier matrix, which with $w = e^{2\pi i/N}$ is:

$$F_N = \frac{1}{\sqrt{N}}(w^{ij})$$

We have then:

$$\begin{aligned} & u\xi = \xi \\ \iff \quad & uFe_0 = Fe_0 \\ \iff \quad & F^*uFe_0 = e_0 \\ \iff \quad & F^*uF = diag(1, w) \end{aligned}$$

Thus we have isomorphisms as in the statement, given by:

$$w_{ij} \to (F^*uF)_{ij}$$

But this gives both the assertions. □

Finally, we can nicely diagonalize the flat matrix, using a discrete Fourier transform. This improves our results from the real case, from section 2 above.

We will be back to this in section 6 below, with a complete discussion of the Fourier matrices, and of their generalizations, called complex Hadamard matrices.

4. Diagonalization

We have seen in the previous section that the theory of the complex matrices is more advanced and complete than the theory in the real case, and this especially when it comes to advanced linear algebra questions, such as diagonalization.

In this section we discuss the diagonalization question, in general.

First, we have the following key statement, that we already know:

Theorem 4.1. *We have the following results:*

(1) *Caracteristic polynomial.*
(2) *Eigenvalues.*

Proof. This is routine, indeed, by using the following fact:

$$Av = \lambda v \iff (A - \lambda 1_N)v = 0$$

In order for this to hold, we must have:

$$\det(A - \lambda 1_N) = 0$$

Thus, we are led to the conclusion in the statement. □

Summarizing, in order to diagonalize the matrices, real or complex, we are left with factorizing the characteristic polynomial, as a first task.

In order to deal with the general case, we will need:

Theorem 4.2. *Any polynomial $P \in \mathbb{C}[X]$ decomposes as*

$$P = c(X - a_1) \ldots (X - a_k)$$

with $c \in \mathbb{C}$ and with $a_1, \ldots, a_k \in \mathbb{C}$.

Proof. This is something quite subtle. The problem is that of proving that our polynomial has at least one root, and then we can proceed by recurrence.

In order to prove that we have at least one root, let $z_0 \in \mathbb{C}$ be a number where $|P(z)|$ attains its minimum.

By developing P around z_0, we have a formula as follows, with $k \in \mathbb{N}$ being a certain exponent, and with $c \neq 0$ being a certain coefficient:

$$P(z) \simeq P(z_0) + c(z - z_0)^k$$

The point now is that, when assuming $P(z_0) \neq 0$, we can always arrange for the number $z \simeq z_0$ to be such that:

$$|P(z)| < |P(z_0)|$$

But this is a contradiction.

Thus we have $P(z_0) = 0$, and we are done. □

Let us mention as well that in general, the roots cannot be explicitely computed.

There are, however, many algorithms and results, regarding special classes of polynomials.

We will be back to this later, at the end of the present section, notably with a generalization of the discriminant of the degree 2 polynomials, which works in degree N, and which decides whether the polynomial has a double root or not.

Let us recall as well a few concrete results. Consider a degree 2 polynomial:

$$P = aX^2 + bX + c$$

The roots are then given by the following well-known formula:

$$r, s = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

In many cases there is no need to compute. Assume indeed that our polynomial is of the following special form, which actually is the case with the characteristic polynomials:

$$P = X^2 - aX + b$$

The roots must then satisfy the following equations:

$$r + s = a$$

$$rs = b$$

When the roots are integers, they are easy to compute.

Yet another trick comes from polynomials with integer coefficients. Assume that we have a polynomial as follows, with integer coefficients, and with leading term 1:

$$P = X^k + a_{k-1}X^{k-1} + \ldots + a_1X + a_0$$

The point is that the integer roots must divide a_0. This is indeed clear.

More generally, we can apply this kind of trick for the polynomials with rational coefficients, in order to compute the rational roots. Note however that this is just a trick, because there are many polynomials with rational coefficients having no rational roots.

With the above result in hand, we can state and prove:

Theorem 4.3. *Given a matrix $A \in M_N(\mathbb{C})$, consider its characteristic polynomial*

$$P(X) = \det(A - X1_N)$$

then factorize this polynomial, by computing the complex roots, with multiplicities,

$$P(X) = \pm(X - \lambda_1)^{n_1} \ldots (X - \lambda_k)^{n_k}$$

and finally compute the corresponding eigenspaces, for each eigenvalue found:

$$V_i = \left\{ v \in \mathbb{C}^N \middle| Av = \lambda_i v \right\}$$

We have then $\dim(V_i) \leq n_i$*, and A is diagonalizable when we have equality for any i.*

Proof. This is something standard, the idea being that, in order for A to be diagonalizable, we must have a direct sum decomposition, as follows:

$$\mathbb{C}^N = V_1 \oplus \ldots \oplus V_k$$

But this leads to the conclusion in the statement. To be more precise, assume that the following holds, for any i:

$$\dim(V_i) = n_i$$

We have then a direct sum decomposition, as above, and the diagonalization formula is as follows, with P being the matrix formed by the eigenvectors, and D being the diagonal matrix formed by the eigenvalues:

$$A = PDP^{-1}$$

Thus, we are led to the conclusion in the statement. □

This was for the main result of linear algebra.

Let us record as well a useful algorithmic version of the above result:

Theorem 4.4. *The square matrices $A \in M_N(\mathbb{C})$ can be diagonalized as follows:*

(1) *Compute the characteristic polynomial.*
(2) *Factorize the characteristic polynomial.*
(3) *Compute the eigenvectors, for each eigenvalue found.*
(4) *If there are no N eigenvectors, A is not diagonalizable.*
(5) *Otherwise, A is diagonalizable, $A = PDP^{-1}$.*

Proof. This is just a reformulation of Theorem 4.3 above. □

As a remark here, in step (3) it is always better to start with the eigenvalues having big multiplicity. Indeed, a multiplicity 1 eigenvalue, for instance, can never lead to the end of the computation, via (4), simply because the eigenvectors always exist.

There are many examples for this phenomenon.

At the level of basic examples, we first have:

Theorem 4.5. *If the eigenvalues are different,*

$$\lambda_i \neq \lambda_j$$

then the matrix is diagonalizable.

Proof. This follows indeed as in the real case. □

There are many examples here, as for instance unitaries, and projections:

Theorem 4.6. *Diagonalization of:*

(1) *Unitaries.*
(2) *Projections.*

Proof. This follows indeed as in the real case:

(1) Here the diagonalization is as follows, with $|w_i| = 1$:

$$U \sim \begin{pmatrix} w_1 & & \\ & \ddots & \\ & & w_N \end{pmatrix}$$

(2) Here the diagonalization is as follows, with $e_i \in \{0, 1\}$:

$$P \sim \begin{pmatrix} e_1 & & \\ & \ddots & \\ & & e_N \end{pmatrix}$$

All this is standard, indeed. □

As an illustration, we can nicely diagonalize the flat matrix, as follows:

Proposition 4.7. *The flat matrix, namely*

$$P = \frac{1}{N}\begin{pmatrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{pmatrix}$$

can be diagonalized over the complex numbers as follows,

$$P = F\begin{pmatrix} 0 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}F^{-1}$$

where $F_{ij} = \frac{1}{\sqrt{N}}(w^{ij})$ *with* $w = e^{2\pi i/N}$ *is the Fourier matrix.*

Proof. This follows indeed by doing some computations with the roots of unity. We will be back to this, in section 8 below. □

We will be back with more examples, later on.

In order to deal now with the general case, several methods are available. First, we have the following result, which is something elementary:

Theorem 4.8. *Any matrix $A \in M_N(\mathbb{C})$ can be put in upper triangular form*

$$A \sim \begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ & & \lambda_N \end{pmatrix}$$

by performing linear manipulations on rows and columns.

Proof. This is something quite clear, and the method, due to Gauss, is well-known for instance when trying to solve systems of linear equations. □

A similar result holds of course with upper triangular replaced by lower triangular:

$$A \sim \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ * & & \lambda_N \end{pmatrix}$$

We will be back to this later, when doing linear systems.

At a more advanced level now, here is a method which works as well for any matrix, and which is much more powerful:

Theorem 4.9. *Any matrix can be put in Jordan form, as follows,*

$$A \sim \begin{pmatrix} J_1 & & \\ & \ddots & \\ & & J_k \end{pmatrix}$$

with the Jordan blocks being as follows,

$$J_i = \begin{pmatrix} \lambda_i & 1 & & & \\ & \lambda_i & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda_i & 1 \\ & & & & \lambda_i \end{pmatrix}$$

with the size being the multiplicity of λ_i.

Proof. This is quite technical, but routine. The idea here is to go back to the proof of the main result that we have so far, Theorem 4.3 above, and to make some changes. □

Summarizing, we have several methods for dealing with the matrices.

There are of course many other methods, which apply to special classes of matrices.

Let us discuss one important result of this type, namely the polar decomposition. The idea will be that of writing a formula as follows:

$$A = U|A|$$

To be more precise, U will be here a partial isometry, a generalization of the notion of isometry, and $|A|$ will be a kind of absolute value of A.

In order to discuss this, let us first discuss the absolute values. We have here:

Theorem 4.10. *Positivity, square rooots and absolute values, defined as*

$$|A| = \sqrt{AA^*}$$

which fit with the usual definition for complex numbers, at $N = 1$.

Proof. This is standard, indeed. □

There are many examples for all this.

We can now formulate our first polar decomposition result, as follows:

Theorem 4.11. *We have the polar decomposition result*

$$A = U|A|$$

for the invertible matrices.

Proof. This is something quite routine. □

There are many examples for all this.

In order to deal now with the general case, we will need:

Proposition 4.12. *Partial isometries, generalizing the usual notion of isometry: general theory, properties, and basic examples.*

There are many examples for all this.

We can now formulate our second and final polar decomposition result, as follows:

Theorem 4.13. *We have the polar decomposition result*

$$A = U|A|$$

for the arbitrary matrices.

Proof. This is something quite routine. □

There are many concrete applications here.

Let us discuss now a number of complementary methods, which are of more analytic nature, and which can be extremely useful, in practice. First, we have:

Theorem 4.14. *The set of invertible matrices, denoted*

$$GL_N(\mathbb{C}) \subset M_N(\mathbb{C})$$

is dense, in the sense that we can find invertible matrices close to any matrix.

Proof. This is clear, intuitively speaking, for instance because the invertible matrices are given by the following condition:

$$\det A \neq 0$$

Indeed, this shows that $GL_N(\mathbb{C})$ appears as a complement of the following surface:

$$S = \left\{ A \middle| \det A = 0 \right\}$$

Thus, $GL_N(\mathbb{C})$ must be dense inside $M_N(\mathbb{C})$, as claimed.

We can equally use here a direct perturbation argument, say by putting first the matrix in upper triangular form. □

There are of course other proofs for the above result.

As an application of the above result, we have:

Theorem 4.15. *We have the following formula*

$$P_{AB} = P_{BA}$$

valid for any two matrices $A, B \in M_N(\mathbb{C})$.

Proof. It follows from definitions that the characteristic polynomial of a matrix is invariant under conjugation, in the sense that we have:

$$P_C = P_{ACA^{-1}}$$

Now observe that, when assuming that A is invertible, we have:

$$AB = A(BA)A^{-1}$$

Thus, the formula in the statement holds indeed, when A is invertible:

$$\begin{aligned} P_{AB} &= P_{A(BA)A^{-1}} \\ &= P_{BA} \end{aligned}$$

By using now Theorem 4.14 above, we conclude that this formula holds for any matrix A, by continuity, and we are done. □

As an application of Theorem 4.15, we have:

Theorem 4.16. *Given two matrices $A, B \in M_N(\mathbb{C})$, the matrices*

$$AB \quad , \quad BA$$

have the same eigenvalues, with the same multiplicities.

Proof. This is just a reformulation of Theorem 4.15 above. □

We will be back to this in section 7 below, when doing spectral theory.

Let us discuss now a number of further density results, in relation with the notion of diagonalization.

This is something more technical, and we will need:

Theorem 4.17. *The resultant of two polynomials,*

$$R(P, Q)$$

definition and basic properties and formulae.

Proof. Consider indeed two polynomials, written as follows:

$$P = c(X - a_1) \ldots (X - a_k)$$

$$Q = d(X - b_1) \ldots (X - b_k)$$

We would like to compute the following quantity:

$$R(P, Q) = cd \prod_{ij} (a_i - b_j)$$

It is clear that this is a polynomial in the coefficients of P, Q.

Indeed, in order to compute this quantity, we must compute certain symmetric functions in the roots a_i, and certain symmetric functions in the roots b_j.

But, due to the general formulae relating roots and coefficients, these symmetric functions are respectively polynomials in the coefficients of P, and in the coefficients of Q.

Summarizing, the result is proved, at least at a theoretical level.

However, the formula of the resultant is quite complicated, but a determinant formula is available. □

As a basic example, we can take one of the polynomials to be of degree 1.

There is a lot of theory here, and we refer to the literature.

In connection with our questions, we will need:

Theorem 4.18. *Discriminant of a polynomial,*

$$\Delta(P) = R(P, P')$$

which vanishes when P has a double root.

Proof. This follows indeed from Theorem 4.17 above. □

As an illustration, consider a degree 2 polynomial:

$$P = aX^2 + bX + c$$

We have then, modulo some constants:

$$R(P, P') = b^2 - 4ac$$

Thus, P has a double root when $b^2 = 4ac$, as it should.

As a second application, we can do this with degree 3 polynomials.

We obtain here the well-known formula for the discriminant in degree 3.

There are many other examples and applications.

We can now formulate our density result, as follows:

Theorem 4.19. *The following hold:*

(1) *The matrices having distinct eigenvalues are dense.*
(2) *The diagonalizable matrices are dense.*

Proof. All this is quite routine, by using the fact that the complements of the hypersurfaces are dense. Of course, we can use here some ad-hoc arguments as well.

(1) Here we are led to the following question:

$$R(P, P') = 0$$

But the solutions form a hypersurface, whose complement is dense.

(2) This follows from (1). □

There are many concrete applications of the above result, the general philosophy being that "any formula which holds for the diagonal matrices should hold everywhere".

We will use this philosophy many times, in what follows.

As a basic application of all this, consider a matrix $A \in M_N(\mathbb{C})$, with eigenvalues denoted as follows:

$$\lambda_1, \ldots, \lambda_N$$

If we apply then a function $f : \mathbb{C} \to \mathbb{C}$ to our matrix A, which has suitable regularity properties, the matrix $f(A)$ has then eigenvalues as follows:

$$f(\lambda_1), \ldots, f(\lambda_N)$$

Indeed, this is clear for the diagonal matrices, then for the diagonalizable matrices, and finally for all the matrices, by density.

We will be back to all this later, on several occasions, in what follows.

Let us discuss now a number of more advanced questions, in relation with the bistochastic matrices.

We first have the following elementary result:

Proposition 4.20. *The class of bistochastic matrices is stable under:*

(1) *Permuting rows and columns.*
(2) *Taking tensor products.*

Proof. In this statement the claim regarding permutations of rows and columns is clear from definitions.

Assuming now that H, K are bistochastic, with sums λ, μ, we have:

$$\begin{aligned}
&\sum_{ia}(H \otimes K)_{ia,jb} \\
= &\sum_{ia} H_{ij}K_{ab} \\
= &\sum_{i} H_{ij} \sum_{a} K_{ab} \\
= &\lambda\mu
\end{aligned}$$

We have as well the following computation:

$$\begin{aligned}
&\sum_{jb}(H \otimes K)_{ia,jb} \\
= &\sum_{jb} H_{ij}K_{ab} \\
= &\sum_{j} H_{ij} \sum_{b} K_{ab} \\
= &\lambda\mu
\end{aligned}$$

Thus, the matrix $H \otimes K$ is bistochastic as well. □

We have the following result, which is elementary as well:

Proposition 4.21. *For a rescaled unitary matrix $H \in M_N(\mathbb{C})$, the following conditions are equivalent:*

(1) *H is bistochastic, with sums λ.*
(2) *H is row-stochastic, with sums λ, and $|\lambda|^2 = N$.*

Proof. Both the implications are elementary, as follows:

(1) $\implies$ (2) If we denote by $H_1, \ldots, H_N \in \mathbb{T}^N$ the rows of H, we have indeed:

$$\begin{aligned} N &= < H_1, H_1 > \\ &= \sum_i < H_1, H_i > \\ &= \sum_i \sum_j H_{1j} \bar{H}_{ij} \\ &= \sum_j H_{1j} \sum_i \bar{H}_{ij} \\ &= \sum_j H_{1j} \cdot \bar{\lambda} \\ &= \lambda \cdot \bar{\lambda} \\ &= |\lambda|^2 \end{aligned}$$

(2) $\implies$ (1) Consider the all-one vector $\xi = (1)_i \in \mathbb{C}^N$. The fact that H is row-stochastic with sums λ reads:

$$\begin{aligned} & \sum_j H_{ij} = \lambda, \forall i \\ \iff & \sum_j H_{ij} \xi_j = \lambda \xi_i, \forall i \\ \iff & H\xi = \lambda \xi \end{aligned}$$

Also, the fact that H is column-stochastic with sums λ reads:

$$\begin{aligned} & \sum_i H_{ij} = \lambda, \forall j \\ \iff & \sum_j H_{ij} \xi_i = \lambda \xi_j, \forall j \\ \iff & H^t \xi = \lambda \xi \end{aligned}$$

We must prove that the first condition implies the second one, provided that the row sum λ satisfies $|\lambda|^2 = N$. But this follows from the following computation:

$$\begin{aligned} & H\xi = \lambda\xi \\ \implies \quad & H^*H\xi = \lambda H^*\xi \\ \implies \quad & N^2\xi = \lambda H^*\xi \\ \implies \quad & N^2\xi = \bar{\lambda} H^t\xi \\ \implies \quad & H^t\xi = \lambda\xi \end{aligned}$$

Thus, we have proved both the implications, and we are done. □

Here is another basic result, that we will need as well in what follows:

Proposition 4.22. *For a rescaled unitary matrix $H \in M_N(\mathbb{C})$, and a number $\lambda \in \mathbb{C}$ satisfying $|\lambda|^2 = N$, the following are equivalent:*

(1) *We have $H \sim H'$, with H' being bistochastic, with sums λ.*
(2) *$K_{ij} = a_i b_j H_{ij}$ is bistochastic with sums λ, for some $a, b \in \mathbb{T}^N$.*
(3) *The equation $Hb = \lambda\bar{a}$ has solutions $a, b \in \mathbb{T}^N$.*

Proof. Once again, this is an elementary result, the proof being as follows:

(1) $\iff$ (2) Since the permutations of the rows and columns preserve the bistochasticity condition, the equivalence $H \sim H'$ that we are looking for can be assumed to come only from multiplying the rows and columns by numbers in $\mathbb{T}$.

Thus, we are looking for scalars $a_i, b_j \in \mathbb{T}$ such that $K_{ij} = a_i b_j H_{ij}$ is bistochastic with sums λ, as claimed.

(2) $\iff$ (3) The row sums of the matrix $K_{ij} = a_i b_j H_{ij}$ are given by:

$$\begin{aligned} & \sum_j K_{ij} \\ = \quad & \sum_j a_i b_j H_{ij} \\ = \quad & a_i (Hb)_i \end{aligned}$$

Thus K is row-stochastic with sums λ precisely when $Hb = \lambda\bar{a}$, and by using the equivalence in Proposition 4.21, we obtain the result. □

We will see later on some other reformulations of the bistochasticity condition, which are more advanced, and can lead to non-trivial results.

We have the following analytic result:

Theorem 4.23. *For a rescaled unitary matrix $H \in M_N(\mathbb{C})$, the excess,*

$$E(H) = \sum_{ij} H_{ij}$$

satisfies the inequality

$$|E(H)| \leq N\sqrt{N}$$

with equality if and only if H is bistochastic.

Proof. In terms of the all-one vector $\xi = (1)_i \in \mathbb{C}^N$, we have:

$$\begin{aligned} & E(H) \\ = & \sum_{ij} H_{ij} \\ = & \sum_{ij} H_{ij}\xi_j\bar{\xi}_i \\ = & \sum_i (H\xi)_i\bar{\xi}_i \\ = & < H\xi, \xi > \end{aligned}$$

Now by using the Cauchy-Schwarz inequality, along with the fact that $U = H/\sqrt{N}$ is unitary, and hence of norm 1, we obtain, as claimed:

$$\begin{aligned} & |E(H)| \\ \leq & ||H\xi|| \cdot ||\xi|| \\ \leq & ||H|| \cdot ||\xi||^2 \\ = & N\sqrt{N} \end{aligned}$$

Regarding now the equality case, this requires the vectors $H\xi, \xi$ to be proportional, and so our matrix H to be row-stochastic. Now, let us assume:

$$H\xi = \lambda\xi$$

The above computation gives:

$$|\lambda|^2 = N$$

Thus by Proposition 4.22 we obtain the result. □

The above estimate is potentially quite useful, because it allows us to analytically locate the bistochastic unitary matrices inside the unitary ones.

Let us go back now to the fundamental question, which already appeared several times in the above, of putting an arbitrary unitary matrix in bistochastic form.

What we know so far on this subject can be summarized as follows:

Proposition 4.24. *A rescaled unitary matrix $H \in M_N(\mathbb{C})$ can be put in bistochastic form when one of the following conditions is satisfied:*

(1) *The following equations, with $i = 1, \ldots, N$,*

$$|Ha|_i = \sqrt{N}$$

have solutions $a \in \mathbb{T}^N$.

(2) *The quantity, called excess,*

$$|E| = \sum_{ij} H_{ij}$$

attains its maximum $N\sqrt{N}$ over the equivalence class of H.

Proof. This follows indeed from the results that we have, namely Proposition 4.21 and Proposition 4.22 above. □

Thus, we have two approaches to the problem, one algebraic, and one analytic.

Let us first discuss the algebraic approach, coming from (1) above.

What we have there is a certain system of N equations, having as unknowns N real variables, namely the phases of $a_1, \ldots, a_N$.

This system is highly non-linear, but can be solved, however, via a certain non-explicit method, as explained by Idel and Wolf in [99].

In order to discuss this material, which is quite advanced, let us begin with some preliminaries.

We first have the following definition, which is standard:

Definition 4.25. *The complex projective space is:*

$$P_{\mathbb{C}}^{N-1} = (\mathbb{C}^N - \{0\})/ < x = \lambda y >$$

In other words, we are looking at the lines in $\mathbb{C}^N$, passing through 0.

There is a real projective space as well.

There is a lot of interesting mathematics here.

Inside this projective space, we have the Clifford torus, constructed as follows:

$$\mathbb{T}^{N-1} = \left\{(z_1, \ldots, z_N) \in P_{\mathbb{C}}^{N-1} \middle| |z_1| = \ldots = |z_N|\right\}$$

Once again, there is some interesting mathematics here.

With these conventions, we have the following result, from [99]:

Proposition 4.26. *For a unitary matrix $U \in U_N$, the following are equivalent:*

(1) *There exist $L, R \in U_N$ diagonal such that the following matrix is bistochastic:*

$$U' = LUR$$

(2) *The standard torus $\mathbb{T}^N \subset \mathbb{C}^N$ satisfies:*

$$\mathbb{T}^N \cap U\mathbb{T}^N \neq \emptyset$$

(3) *The Clifford torus $\mathbb{T}^{N-1} \subset P_{\mathbb{C}}^{N-1}$ satisfies:*

$$\mathbb{T}^{N-1} \cap U\mathbb{T}^{N-1} \neq \emptyset$$

Proof. These equivalences are all elementary, as follows:

(1) $\implies$ (2) Assuming that $U' = LUR$ is bistochastic, which in terms of the all-1 vector ξ means $U'\xi = \xi$, if we set $f = R\xi \in \mathbb{T}^N$ we have:

$$\begin{aligned} & Uf \\ = \ & \bar{L}U'\bar{R}f \\ = \ & \bar{L}U'\xi \\ = \ & \bar{L}\xi \in \mathbb{T}^N \end{aligned}$$

Thus we have $Uf \in \mathbb{T}^N \cap U\mathbb{T}^N$, which gives the conclusion.

(2) $\implies$ (1) Given $g \in \mathbb{T}^N \cap U\mathbb{T}^N$, we can define R, L as follows:

$$R = diag(g_1, \ldots, g_N)$$

$$\bar{L} = diag((Ug)_1, \ldots, (Ug)_N)$$

With these values for L, R, we have then the following formulae:

$$R\xi = g$$

$$\bar{L}\xi = Ug$$

Thus the matrix $U' = LUR$ is bistochastic, because:

$$\begin{aligned} & U'\xi \\ = \ & LUR\xi \\ = \ & LUg \\ = \ & \xi \end{aligned}$$

(2) $\implies$ (3) This is clear, because $\mathbb{T}^{N-1} \subset P_{\mathbb{C}}^{N-1}$ appears as the projective image of $\mathbb{T}^N \subset \mathbb{C}^N$, and so $\mathbb{T}^{N-1} \cap U\mathbb{T}^{N-1}$ appears as the projective image of $\mathbb{T}^N \cap U\mathbb{T}^N$.

(3) $\implies$ (2) We have indeed the following equivalence:

$$\mathbb{T}^{N-1} \cap U\mathbb{T}^{N-1} \neq \emptyset \iff \exists \lambda \neq 0, \lambda\mathbb{T}^N \cap U\mathbb{T}^N \neq \emptyset$$

But $U \in U_N$ implies $|\lambda| = 1$, and this gives the result. □

The point now is that the condition (3) above is something familiar in symplectic geometry, and known to hold for any $U \in U_N$. Thus, following [99], we have:

Theorem 4.27. *Any unitary matrix $U \in U_N$ can be put in bistochastic form,*

$$U' = LUR$$

with $L, R \in U_N$ being both diagonal, via a certain non-explicit method.

Proof. As already mentioned, the condition $\mathbb{T}^{N-1} \cap U\mathbb{T}^{N-1} \neq \emptyset$ in Proposition 4.26 (3) is something quite natural in symplectic geometry.

To be more precise, $\mathbb{T}^{N-1} \subset P_{\mathbb{C}}^{N-1}$ is a Lagrangian submanifold, $\mathbb{T}^{N-1} \to U\mathbb{T}^{N-1}$ is a Hamiltonian isotopy, and a result from [33], [44] states that $\mathbb{T}^{N-1}$ cannot be displaced from itself via a Hamiltonian isotopy.

Thus, the results in [33], [44] tells us that $\mathbb{T}^{N-1} \cap U\mathbb{T}^{N-1} \neq \emptyset$ holds indeed, for any $U \in U_N$. We therefore obtain the result, via Proposition 4.26. See [99]. □

We will be back to these questions in section 8 below.

5. Applications

We discuss in what follows some applications of the theory that we developed above, for the most to questions of analysis.

The main idea here will be that functions of several variables can be locally approximated by linear maps, in the same way as those of one variable can be locally approximated by the corresponding tangent lines, given by derivatives.

Let us begin, however, with some straightforward applications to algebra.

First, we have the following result, which is actually at the origin of the whole linear algebra theory:

Theorem 5.1. *Any linear system of equations*

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1N}x_N &= v_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2N}x_N &= v_2 \\ \vdots & \\ a_{N1}x_1 + a_{N2}x_2 + \ldots + a_{NN}x_N &= v_N \end{cases}$$

can be written in matrix form, as follows,

$$Ax = v$$

and when A is invertible, its solution is given by $x = A^{-1}v$.

Proof. Our system reads:

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1N} \\ a_{21} & a_{22} & \ldots & a_{2N} \\ \vdots & & & \vdots \\ a_{N1} & a_{N2} & \ldots & a_{NN} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_N \end{pmatrix} = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_N \end{pmatrix}$$

Consider now the matrix of coefficients, namely:

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1N} \\ a_{21} & a_{22} & \ldots & a_{2N} \\ \vdots & & & \vdots \\ a_{N1} & a_{N2} & \ldots & a_{NN} \end{pmatrix}$$

In terms of this matrix, we obtain the formula in the statement, namely:

$$Ax = v$$

When A is not invertible, the answer is more complicated. □

There are many applications of the above result. In each case, we are led to the computation of an inverse matrix A^{-1}, and this is something that we know how to solve. Thus, we have here a first true application of the theory developed so far.

We have as well the following result:

Theorem 5.2. *Any linear recurrence system*

$$\begin{cases} x_{k+1} &= a_{11}x_k + a_{12}y_k + \ldots + a_{1N}z_k \\ y_{k+1} &= a_{21}x_k + a_{22}y_k + \ldots + a_{2N}z_k \\ \vdots & \\ z_{k+1} &= a_{N1}x_k + a_{N2}y_k + \ldots + a_{NN}z_k \end{cases}$$

can be written in matrix form, as follows,

$$v_{k+1} = Av_k$$

and so the solution is given by $v_k = A^k v_0$.

Proof. Our recurrence reads:

$$\begin{pmatrix} x_{k+1} \\ y_{k+1} \\ \vdots \\ z_{k+1} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1N} \\ a_{21} & a_{22} & \ldots & a_{2N} \\ \vdots & & & \vdots \\ a_{N1} & a_{N2} & \ldots & a_{NN} \end{pmatrix} \begin{pmatrix} x_k \\ y_k \\ \vdots \\ z_k \end{pmatrix}$$

Consider now the matrix of coefficients, namely:

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1N} \\ a_{21} & a_{22} & \ldots & a_{2N} \\ \vdots & & & \vdots \\ a_{N1} & a_{N2} & \ldots & a_{NN} \end{pmatrix}$$

In terms of this matrix, we obtain the formula in the statement, namely:

$$v_{k+1} = Av_k$$

Thus, we are led to the formula in the statement. □

There are many other applications of this type, to advanced questions regarding numbers and algebra, and explicit examples for all the above.

Let us discuss now applications to analysis.

Let us explain the first, and perhaps most important application. First, we have the following result, for functions of one variable:

Theorem 5.3. *Any function of one variable can be locally approximated as*

$$f(x+t) \simeq f(x) + at$$

where $a = f'(x)$ is the derivative of f at the point x.

Proof. Let us recall indeed the definition of the derivative:

$$f'(x) = \lim_{t \to 0} \frac{f(x+t) - f(x)}{t}$$

We therefore obtain the following formula:

$$f(x+t) \simeq f(x) + f'(x)t$$

But this gives the formula in the statement. □

There are of course many applications of all this.

More generally, we have the following result:

Theorem 5.4. *Any function of one variable can be locally approximated as*

$$f(x+t) \simeq f(x) + f'(x)t + \frac{f''(x)}{2}\, t^2$$

where $f''(x)$ is the second derivative of f at the point x.

Proof. This follows indeed from Theorem 5.3 above. Observe that for a polynomial of degree 2 the series is stationary, starting from 2, and we obtain an equality.

Indeed, let us write our degree 2 polynomial as follows:

$$P = a + bX + cX^2$$

The derivatives at $x = 0$ are then given by:

$$P(0) = a$$

$$P'(0) = b$$

$$P''(0) = 2c$$

The Taylor formula in the statement at $x = 0$ reads:

$$P(t) \simeq a + bt + ct^2$$

Thus, we have indeed an equality. □

Once again, there are many applications of this.

In fact, we have the following general result:

Theorem 5.5. *Any function of one variable can be locally approximated as*

$$f(x+t)=\sum_{k=0}^{\infty}\frac{f^{(k)}(x)}{k!}\,t^k$$

where $f^{(k)}(x)$ are the higher derivatives of f at the point x.

Proof. This follows indeed from Theorem 5.3 above. Observe that for a polynomial of degree N the series is stationary, starting from N, and we obtain an equality.

Indeed, let us write our degree N polynomial as follows:

$$P=a_0+a_1X+\ldots+a_NX^N$$

The derivatives at $x=0$ are then given by:

$$\begin{aligned}P(0)&=a_0\\P'(0)&=a_1\\P''(0)&=2a_2\\&\vdots\\P^{(N)}(0)&=N!a_N\\P^{(N+1)}(0)&=0\\P^{(N+2)}(0)&=0\\&\vdots\end{aligned}$$

The Taylor formula in the statement at $x=0$ reads:

$$P(t)\simeq a_0+a_1t+\ldots+a_Nt^N$$

Thus, we are led to the above conclusion. □

As a basic appplication for all the above, we have:

Theorem 5.6. *Taylor series for:*

(1) sin.
(2) cos.
(3) exp.
(4) log.

Proof. This follows by derivating the functions in the statement:

(1) Here we must compute the derivatives of sin.

(2) Here we must compute the derivatives of cos.

(3) Here we must compute the derivatives of exp.

(4) Here we must compute the derivatives of log. □

There are of course many other examples.

In several variables now, the situation is similar at order 1, but this time involving linear algebra and matrices.

Let us discuss first, however, the 2D case. Here we can use complex numbers, and a whole theory can be developed. Let us begin with:

Theorem 5.7. *For a function $f : \mathbb{C} \to \mathbb{C}$, the following are equivalent:*

(1) *f is derivable.*
(2) *f has a Taylor series.*

If these conditions are satisfied, we say that f is holomorphic.

Proof. This is quite standard, indeed. □

We will see later several generalizations of the notion of holomorphic function, namely the meromorphic functions, and the harmonic functions.

As basic examples, we have the previous elementary functions, regarded now as functions of one complex variable, as follows:

Theorem 5.8. *Taylor series, and various details, regarding:*

(1) sin.
(2) cos.
(3) exp.
(4) log.

Proof. This follows by derivating the functions in the statement:

(1) Here we must compute the derivatives of sin.

(2) Here we must compute the derivatives of cos.

(3) Here we must compute the derivatives of exp.

(4) Here we must compute the derivatives of log. □

Observe that things got quite tricky now, in the complex setting.

There are of course many other examples.

At the level of the general theory, we have the following result:

Theorem 5.9. *Cauchy formula.*

Proof. This is quite standard, indeed. □

As a first application of the Cauchy formula, that we will need later on, in section 7 below, when doing spectral theory, we have:

Theorem 5.10. *Liouville theorem.*

Proof. This follows indeed from the Cauchy formula. □

Let us discuss now some generalizations. We will need:

Proposition 5.11. *Rational functions, basic properties.*

Proof. This is quite standard, indeed. □

We can now generalize the holomorphic functions, as follows:

Theorem 5.12. *Meromorphic functions, basic properties.*

Proof. This is quite standard, indeed. □

As a main result now, we have:

Theorem 5.13. *Residue formula.*

Proof. This is quite standard, indeed. □

There are many interesting applications here.

Let us discuss now a second generalization of the holomorphic functions, which is interesting as well:

Definition 5.14. *Harmonic functions.*

We have basic examples here coming from polynomials. We can compute as well the radial harmonic functions.

At the level of the general theory now, we have:

Theorem 5.15. *Mean formula for harmonic functions.*

Proof. This is quite standard, indeed. □

We will be back to this later on.

In several real variables now, the situation is similar at order 1, but this time involving linear algebra and matrices, as follows:

Theorem 5.16. *Any function of several variables can be locally approximated as*

$$f(x+t)\simeq f(x)+At$$

with A being the matrix of partial derivatives at x,

$$A=\left(\frac{\partial f_i}{\partial x_j}(x)\right)_{ij}$$

acting on the vectors $r\in\mathbb{C}^N$ by usual multiplication.

Proof. This is indeed standard, by using a kind of recurrence.

To be more precise, consider the matrix in the statement:

$$A=\begin{pmatrix}\frac{\partial f_1}{\partial x_1}(x) & \ldots & \frac{\partial f_1}{\partial x_N}(x)\\ \vdots & & \vdots\\ \frac{\partial f_N}{\partial x_1}(x) & \ldots & \frac{\partial f_N}{\partial x_N}(x)\end{pmatrix}$$

The idea is then that around x, our function behaves exactly as $v\to Av$:

$$\begin{aligned}f\begin{pmatrix}x_1+t_1\\ \vdots\\ x_N+t_N\end{pmatrix}&\simeq f\begin{pmatrix}x_1\\ \vdots\\ x_N\end{pmatrix}\\ &+\begin{pmatrix}\frac{\partial f_1}{\partial x_1}(x) & \ldots & \frac{\partial f_1}{\partial x_N}(x)\\ \vdots & & \vdots\\ \frac{\partial f_N}{\partial x_1}(x) & \ldots & \frac{\partial f_N}{\partial x_N}(x)\end{pmatrix}\begin{pmatrix}t_1\\ \vdots\\ t_N\end{pmatrix}\end{aligned}$$

Thus, we are led to the conclusion in the statement. □

Once again, there are many applications of all this.

Regarding the higher derivatives, the situation here is more complicated.

The derivative is very useful when integrating, and we will discuss this now.

Let us first recall the basic theory here:

Theorem 5.17. *We have the Riemann integration formula,*

$$\int_a^b f(x)dx=(b-a)\times\lim_{N\to\infty}\frac{1}{N}\sum_{k=1}^{N}f\left(a+\frac{b-a}{N}\cdot k\right)$$

which can serve as a formal definition for the integral.

Proof. This is indeed standard, by drawing rectangles. We have indeed:

$$\int_a^b f(x)dx=(b-a)\times\lim_{N\to\infty}\frac{1}{N}\sum_{k=1}^{N}f(x_i)$$

When the points $x_1,\ldots,x_N\in[a,b]$ are uniformly distributed, we obtain the formula in the statement. □

There are many applications here, for instance to the summation of series.

As a basic application, we can sum powers, with fixed results at small exponents, and estimates in general. We have indeed the following result:

Theorem 5.18. *The basic Riemann sums, namely*

$$1^k + 2^k + \ldots + N^k$$

depending on an exponent $k \in \mathbb{N}$, are as follows:

(1) *At $k = 1$ we have the following exact formula:*

$$1 + 2 + \ldots + N = \frac{N(N+1)}{2}$$

(2) *At $k = 2$ we have the following exact formula:*

$$1^2 + 2^2 + \ldots + N^2 = \frac{N(N+1)(2N+1)}{6}$$

(3) *At $k = 3$ we have the following exact formula:*

$$1^3 + 2^3 + \ldots + N^3 = \left[\frac{N(N+1)}{2}\right]^2$$

(4) *At $k \in \mathbb{N}$ we have the following estimate:*

$$1^k + 2^k + \ldots + N^k \simeq \frac{N^{k+1}}{k+1}$$

Proof. This is something well-known, the idea being as follows:

(1) The average of the numbers $1, 2, \ldots, N$ is given by:

$$\frac{1}{N}(1 + 2 + \ldots + N) = \frac{N+1}{2}$$

Thus, we obtain the formula in the statement, without any computation.

(2) There are several proofs here, a well-known one being by drawing certain squares in the plane.

(3) There are several proofs here, a well-known one being by drawing certain cubes in the space.

(4) Here there is no trick, and we must use the Riemann integration formula. We have the following computation:

$$\begin{aligned}\int_0^1 x^k dx &= \left[\frac{x^{k+1}}{k+1}\right]_0^1 \\ &= \frac{1}{k+1} - 0 \\ &= \frac{1}{k+1}\end{aligned}$$

But this gives the estimate in the statement, by using a Riemann sum. □

Getting back now to the basics, and to the definition of the integral, we have as well the following alternative approach:

Theorem 5.19. *We have the Monte Carlo integration formula,*

$$\int_a^b f(x)dx = (b-a) \times \lim_{N\to\infty} \frac{1}{N} \sum_{k=1}^{N} f(x_i)$$

with $x_1, \ldots, x_N \in [a, b]$ *being random.*

Proof. We recall from the construction of the integral that the idea is to use a formula as follows, with $x_1, \ldots, x_N \in [a, b]$ being uniformly distributed:

$$\int_a^b f(x)dx = (b-a) \times \lim_{N\to\infty} \frac{1}{N} \sum_{k=1}^{N} f(x_i)$$

But this works as well when $x_1, \ldots, x_N \in [a, b]$ are randomly distributed, for somewhat obvious reasons, and this gives the result. □

Observe that the Monte Carlo integration works better than Riemann integration, for instance when trying to improve the estimate, via $N \to N + 1$.

Also, the Monte Carlo integration works better for functions having various symmetries. Indeed, the Riemann integration can get "fooled" by these symmetries.

Getting back now to linear algebra, we have the following key result:

Theorem 5.20. *We have the change of variable formula*

$$\int_a^b f(x)dx = \int_c^d f(\varphi(t))\varphi'(t)dt$$

where $c = \varphi^{-1}(a)$ *and* $d = \varphi^{-1}(b)$.

Proof. This follows with from the following differentiation rule:

$$(F\varphi)'(t) = F'(\varphi(t))\varphi'(t)$$

Indeed, in connection with our problem, we can set:

$$f = F'$$

Now by integrating between c and d, we obtain the result. □

In several variables now, the result, which is something non-trivial and extremely useful, is as follows:

Theorem 5.21. *Given a transformation in several variables,*

$$\varphi = (\varphi_1, \ldots, \varphi_N)$$

we have the following change of variable formula,

$$\int_E f(x)dx = \int_{\varphi^{-1}(E)} f(\varphi(t))J_\varphi(t)dt$$

with the J_φ quantity, called Jacobian, being given by:

$$J_\varphi(t) = \det\left[\left(\frac{\partial\varphi_i}{\partial x_j}(x)\right)_{ij}\right]$$

Proof. Observe first that this generalizes the change of variable formula in 1 dimension, from Theorem 5.20 above.

In general, the proof is quite tricky, the idea being that of assuming that the change of variables is linear, and by using the definition of the determinant as a volume.

The details and computations here are non-trivial. This is in fact our first "true" theorem here. □

In what regards the applications, these often come via:

Theorem 5.22. *We have polar coordinates in 2 dimensions,*

$$\begin{cases} x &= r\cos t \\ y &= r\sin t \end{cases}$$

the corresponding Jacobian being $J = r$.

Proof. This is elementary, the Jacobian being:

$$\begin{aligned} J &= \begin{vmatrix} \frac{\partial r\cos t}{\partial r} & \frac{\partial r\cos t}{\partial t} \\ \frac{\partial r\sin t}{\partial r} & \frac{\partial r\sin t}{\partial t} \end{vmatrix} \\ &= \begin{vmatrix} \cos t & -r\sin t \\ \sin t & r\cos t \end{vmatrix} \\ &= r\cos^2 t + r\sin^2 t \\ &= r \end{aligned}$$

Thus, we have indeed the formula in the statement. □

As a main application, we can compute the Gauss integral:

Theorem 5.23. *We have the following formula,*

$$\int_{\mathbb{R}} e^{-x^2} dx = \sqrt{\pi}$$

called Gauss integral formula.

Proof. Consider indeed the Gauss integral:

$$I = \int_{\mathbb{R}} e^{-x^2} dx$$

By using polar coordinates, we obtain:

$$\begin{aligned} I^2 &= \int_{\mathbb{R}} e^{-x^2} dx \int_{\mathbb{R}} e^{-y^2} dy \\ &= \int_{\mathbb{R}} \int_{\mathbb{R}} e^{-x^2-y^2} dxdy \\ &= \int_0^{2\pi} \int_0^{\infty} e^{-r^2\cos^2 t - r^2 \sin^2 t} r dr dt \\ &= \int_0^{2\pi} \int_0^{\infty} e^{-r^2} r dr dt \\ &= 2\pi \int_0^{\infty} \left(-\frac{e^{-r^2}}{2} \right)' dr \\ &= 2\pi \left[0 - \left(-\frac{1}{2} \right) \right] \\ &= \pi \end{aligned}$$

Thus, we are led to the formula in the statement. □

As a main application of the Gauss formula, we have the following result:

Theorem 5.24. *The following function integrates up to* 1*:*

$$g_1(x) = \frac{1}{\sqrt{2\pi}} e^{-x^2/2}$$

More generally, the following function integrates up to 1*,*

$$g_t(x) = \frac{1}{\sqrt{2\pi t}} e^{-x^2/2t}$$

for any value of the parameter $t > 0$*.*

Proof. It is enough to establish the second formula, because the first one is the $t = 1$ particular case of it. We have, with the change of variables $x = \sqrt{2t}\, y$:

$$\begin{aligned}
&\int_{\mathbb{R}} e^{-x^2/2t} dx \\
= &\int_{\mathbb{R}} e^{-y^2} \sqrt{2t}\, dy \\
= &\sqrt{2t} \int_{\mathbb{R}} e^{-y^2} dy \\
= &\sqrt{2t} \times \sqrt{\pi} \\
= &\sqrt{2\pi t}
\end{aligned}$$

Thus, we are led to the conclusions in the statement. □

The above functions are very important in probability, so let us briefly discuss now this material. We will present here an introduction to the subject, and leave examples, more theory, and more advanced aspects for later, in sections 6 and 11 below.

With the idea in mind of doing things a bit abstractly, our starting point will be:

Definition 5.25. *Let X be a probability space, that is to say, a space with a probability measure, and with the corresponding integration denoted $\mathbb{E}$, and called expectation.*

(1) *The random variables are the real functions as follows:*

$$f \in L^\infty(X)$$

(2) *The moments of such a variable are the numbers:*

$$M_k(f) = \mathbb{E}(f^k)$$

(3) *The law of such a variable is the measure given by:*

$$M_k(f) = \int_{\mathbb{R}} x^k d\mu_f(x)$$

Here the fact that μ_f exists indeed is not trivial. By linearity, we would like to have a real probability measure making hold the following formula, for any $P \in \mathbb{R}[X]$:

$$\mathbb{E}(P(f)) = \int_{\mathbb{R}} P(x) d\mu_f(x)$$

By using a continuity argument, it is enough to have this formula for the characteristic functions χ_I of the arbitrary measurable sets of real numbers $I \subset \mathbb{R}$:

$$\mathbb{E}(\chi_I(f)) = \int_{\mathbb{R}} \chi_I(x) d\mu_f(x)$$

Thus, we would like to have a measure μ_f such that:

$$\mathbb{P}(f \in I) = \mu_f(I)$$

But this latter formula can serve as a definition for μ_f, with the axioms of real probability measures being trivially satisifed, and so we are done.

Alternatively, assuming some familiarity with measure theory, μ_f is simply the push-forward of the probability measure on X, via the random variable $f : X \to \mathbb{R}$.

We can now introduce the normal distributions, as follows:

Definition 5.26. *The normal law of parameter* 1 *is the following measure:*

$$g_1 = \frac{1}{\sqrt{2\pi}} e^{-x^2/2} dx$$

More generally, the normal law of parameter $t > 0$ *is the following measure:*

$$g_t = \frac{1}{\sqrt{2\pi t}} e^{-x^2/2t} dx$$

These are also called Gaussian distributions, with "g" standing for Gauss.

As a first comment, these laws are traditionally denoted $\mathcal{N}(0, 1)$ and $\mathcal{N}(0, t)$, but since we will be doing in this book all kinds of probability, namely classical and free, real and complex, discrete and continuous, and so on, we will have to deal with lots of interesting probability measures, and we will be using simplified notations for them.

Let us mention as well that the normal laws traditionally have 2 parameters, the mean and the variance. Here we do not need the mean, all our theory using centered laws.

Generally speaking, the normal laws appear as bit everywhere, in real life. The reasons behind this phenomenon come from the Central Limit Theorem (CLT), that we will explain in a moment, after developing the needed general theory.

As a first result regarding the normal laws, we have:

Proposition 5.27. *We have the variance formula*

$$V(g_t) = t$$

valid for any $t > 0$.

Proof. The first moment is 0, because our normal law g_t is centered:

$$M_1 = 0$$

As for the second moment, this can be computed as follows:

$$\begin{aligned}
& M_2\\
= \ & \frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} x^2e^{-x^2/2t}dx\\
= \ & \frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} (tx)\left(-e^{-x^2/2t}\right)'dx\\
= \ & \frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} te^{-x^2/2t}dx\\
= \ & \sqrt{\frac{t}{2\pi}}\int_{\mathbb{R}} e^{-x^2/2t}dx\\
= \ & \sqrt{\frac{t}{2\pi}}\times\sqrt{2\pi t}\\
= \ & t
\end{aligned}$$

We conclude from this that the variance is $V=t$. □

Let us discuss now some further properties of the normal law, which are very useful, but of more specialized nature.

We first have the following result:

Theorem 5.28. *The moments of the normal law are the numbers*

$$M_k(g_t)=t^{k/2}\times k!!$$

where the double factorials are by definition given by

$$k!!=1\cdot 3\cdot 5\ldots(k-1)$$

with the convention $k!!=0$ when k is odd.

Proof. We have the following computation:

$$\begin{aligned}
& M_k\\
= \ & \frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} x^ke^{-x^2/2t}dx\\
= \ & \frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} (tx^{k-1})\left(-e^{-x^2/2t}\right)'dx\\
= \ & \frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} t(k-1)x^{k-2}e^{-x^2/2t}dx\\
= \ & t(k-1)\times\frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} x^{k-2}e^{-x^2/2t}dx\\
= \ & t(k-1)M_{k-2}
\end{aligned}$$

Now recall from the proof of Proposition 5.27 above that we have:

$$M_0 = 1$$

$$M_1 = 0$$

Thus by recurrence, the even moments all vanish, and the odd moments are given by the formula in the statement. □

We can improve the above result, as follows:

Theorem 5.29. *The moments of the normal law are the numbers*

$$M_k(g_t) = t^{k/2}|P_2(k)|$$

where $P_2(k)$ is the set of pairings of $\{1, \ldots, k\}$.

Proof. Let us count the pairings of $\{1, \ldots, k\}$. In order to have such a pairing, we must pair 1 with one of $2, \ldots, k$, and then use a pairing of the remaining $k-2$ points.

Thus, we have the following recurrence formula:

$$|P_2(k)| = (k-1)|P_2(k-2)|$$

As for the initial data, this is:

$$P_1 = 0$$

$$P_2 = 1$$

We therefore obtain, by recurrence:

$$|P_2(k)| = k!!$$

Thus, we are led to the conclusion in the statement. □

We are done done yet, and here is one more improvement:

Theorem 5.30. *The moments of the normal law are the numbers*

$$M_k(g_t) = \sum_{\pi \in P_2(k)} t^{|\pi|}$$

where $P_2(k)$ is the set of pairings of $\{1, \ldots, k\}$, and $|.|$ is the number of blocks.

Proof. This follows indeed from Theorem 5.29 above, because the number of blocks of a pairing of $\{1, \ldots, k\}$ is trivially $k/2$, independently of the pairing. □

We will see later on that many other interesting probability distributions are subject to similar formulae regarding their moments, involving partitions, and a lot of interesting combinatorics.

Discussing this will be in fact a main theme of the present book.

Now back to generalities, it is well-known that the normal laws appear a bit everywhere, in real life. For instance when you grade an exam, the grades arrange on a Gaussian bell. It goes the same with many other experiments, in physics or engineering.

The reasons behind this phenomenon come from a main theorem in probability, called Central Limit Theorem (CLT), that we will explain in section 11 below.

In a purely mathematical context, in relation with algebra and geometry, the simplest way of recovering the normal laws is by looking at the coordinates over the real spheres $S_{\mathbb{R}}^{N-1}$, in the $N\to\infty$ limit. We will discuss this in the next section.

6. Advanced calculus

We discuss here more advanced questions, related to the computation of the volumes of the spheres, and more generally to the integration over the spheres.

Before anything, we first have:

Theorem 6.1. *Assuming that the length of the unit circle is*

$$L = 2\pi$$

it follows that the area of the unit disk is:

$$A = \pi$$

Proof. This follows by drawing polygons, and taking the $N \to \infty$ limit. To be more precise, let us cut the disk as a pizza, in N slices, and leave aside the rounded parts.

The area to be eaten can be then computed as follows, where H is the height of the slices, S is the length of their sides, and $P = NS$ is the total length of the sides:

$$\begin{aligned} A &= N \times \frac{1}{2} \times H \times S \\ &= \frac{1}{2} \times H \times P \\ &\simeq \frac{1}{2} \times 1 \times L \\ &= \frac{2\pi}{2} \\ &= \pi \end{aligned}$$

Thus, we are led to the conclusion in the statement. □

In general, we need polar coordinates, in order to deal with such questions. In 2 dimensions, the polar coordinate formula, that we already know, is as follows:

Theorem 6.2. *We have polar coordinates in 2 dimensions,*

$$\begin{cases} x &= r\cos t \\ y &= r\sin t \end{cases}$$

the corresponding Jacobian being $J = r$.

Proof. This is elementary, the Jacobian being:

$$\begin{aligned}
J &= \begin{vmatrix} \frac{\partial r\cos t}{\partial r} & \frac{\partial r\cos t}{\partial t} \\ \frac{\partial r\sin t}{\partial r} & \frac{\partial r\sin t}{\partial t} \end{vmatrix} \\
&= \begin{vmatrix} \cos t & -r\sin t \\ \sin t & r\cos t \end{vmatrix} \\
&= r\cos^2 t + r\sin^2 t \\
&= r
\end{aligned}$$

Thus, we have indeed the formula in the statement. □

In 3 dimensions now, the polar coordinate formula is quite similar, with some care needed in order to determine the precise range of the angles, as follows:

Theorem 6.3. *We have spherical coordinates in* 3 *dimensions,*

$$\begin{cases} x &= r\cos s \\ y &= r\sin s\cos t \\ z &= r\sin s\sin t \end{cases}$$

the corresponding Jacobian being $J(r,s,t) = r^2\sin s$.

Proof. The fact that we have indeed spherical coordinates is clear. To be more precise, we are led to variables as in the statement, namely:

$$\begin{cases} x &= r\cos s \\ y &= r\sin s\cos t \\ z &= r\sin s\sin t \end{cases}$$

The Jacobian is given by the following formula:

$$\begin{aligned}
& J(r,s,t) \\
= & \begin{vmatrix} \cos s & -r\sin s & 0 \\ \sin s\cos t & r\cos s\cos t & -r\sin s\sin t \\ \sin s\sin t & r\cos s\sin t & r\sin s\cos t \end{vmatrix} \\
= & r^2\sin s\sin t\begin{vmatrix} \cos s & -r\sin s \\ \sin s\sin t & r\cos s\sin t \end{vmatrix} + r\sin s\cos t\begin{vmatrix} \cos s & -r\sin s \\ \sin s\cos t & r\cos s\cos t \end{vmatrix} \\
= & r\sin s\sin^2 t\begin{vmatrix} \cos s & -r\sin s \\ \sin s & r\cos s \end{vmatrix} + r\sin s\cos^2 t\begin{vmatrix} \cos s & -r\sin s \\ \sin s & r\cos s \end{vmatrix} \\
= & r\sin s(\sin^2 t+\cos^2 t)\begin{vmatrix} \cos s & -r\sin s \\ \sin s & r\cos s \end{vmatrix} \\
= & r\sin s\times 1\times r \\
= & r^2\sin s
\end{aligned}$$

Thus, we have indeed the formula in the statement. □

The above formula is extremely useful, and we have many applications of it.

Let us work out now the spherical coordinate formula in N dimensions. The formula here, which generalizes those at $N=2,3$, is as follows:

Theorem 6.4. *We have spherical coordinates in N dimensions,*

$$\begin{cases} x_1 &= r\cos t_1 \\ x_2 &= r\sin t_1\cos t_2 \\ \vdots & \\ x_{N-1} &= r\sin t_1\sin t_2\ldots\sin t_{N-2}\cos t_{N-1} \\ x_N &= r\sin t_1\sin t_2\ldots\sin t_{N-2}\sin t_{N-1} \end{cases}$$

the corresponding Jacobian being given by the following formula:

$$J(r,t)=r^{N-1}\sin^{N-2}t_1\sin^{N-3}t_2\ \ldots\ \sin^2 t_{N-3}\sin t_{N-2}$$

Proof. Observe first that these generalizes the above results, in 2 and 3 dimensions.

The fact that we have indeed spherical coordinates is clear. We are led indeed to the formulae in the statement, namely:

$$\begin{cases} x_1 &= r\cos t_1\\ x_2 &= r\sin t_1\cos t_2\\ \vdots\\ x_{N-1} &= r\sin t_1\sin t_2\ldots\sin t_{N-2}\cos t_{N-1}\\ x_N &= r\sin t_1\sin t_2\ldots\sin t_{N-2}\sin t_{N-1}\end{cases}$$

Regarding the Jacobian, the proof is similar to the one from 2 or 3 dimensions, by developing the determinant over the last column, and then by proceeding by recurrence. Indeed, by developing, we have:

$$\begin{aligned} & J_N\\ = \ & r\sin t_1\ldots\sin t_{N-2}\sin t_{N-1}\times\sin t_{N-1}J_{N-1}\\ + \ & r\sin t_1\ldots\sin t_{N-2}\cos t_{N-1}\times\cos t_{N-1}J_{N-1}\\ = \ & r\sin t_1\ldots\sin t_{N-2}(\sin^2 t_{N-1}+\cos^2 t_{N-1})J_{N-1}\\ = \ & r\sin t_1\ldots\sin t_{N-2}J_{N-1}\end{aligned}$$

Thus, we obtain the formula in the statement, by recurrence. □

Let us present now some classical applications of all this, concerning the computation of the volumes of spheres.

For this purpose, we must understand how the products of arbitrary coordinates integrate, over the spheres.

Let us start with the case $N=2$. Here the sphere is the unit circle $\mathbb{T}$, and with $z=e^{it}$ the coordinates are $\cos t,\sin t$.

Let us first integrate arbitrary powers of these coordinates. We have here:

Proposition 6.5. *We have the following formulae,*

$$\int_0^{\pi/2}\cos^p t\,dt=\int_0^{\pi/2}\sin^p t\,dt=\left(\frac{\pi}{2}\right)^{\varepsilon(p)}\frac{p!!}{(p+1)!!}$$

where $\varepsilon(p)=1$ if p is even, and $\varepsilon(p)=0$ if p is odd, and where

$$m!!=(m-1)(m-3)(m-5)\ldots$$

with the product ending at 2 if m is odd, and ending at 1 if m is even.

Proof. Let us first compute the integral on the left in the statement:

$$I_p = \int_0^{\pi/2} \cos^p t\, dt$$

We do this by partial integration. We have the following formula:

$$\begin{aligned} & (\cos^p t \sin t)' \\ = \ & p\cos^{p-1} t(-\sin t)\sin t + \cos^p t \cos t \\ = \ & p\cos^{p+1} t - p\cos^{p-1} t + \cos^{p+1} t \\ = \ & (p+1)\cos^{p+1} t - p\cos^{p-1} t \end{aligned}$$

By integrating between 0 and $\pi/2$, we obtain the following formula:

$$(p+1)I_{p+1} = pI_{p-1}$$

Thus we can compute I_p by recurrence, and we obtain:

$$\begin{aligned} I_p &= \frac{p-1}{p} I_{p-2} \\ &= \frac{p-1}{p} \cdot \frac{p-3}{p-2} I_{p-4} \\ &= \frac{p-1}{p} \cdot \frac{p-3}{p-2} \cdot \frac{p-5}{p-4} I_{p-6} \\ &\vdots \\ &= \frac{p!!}{(p+1)!!} I_{1-\varepsilon(p)} \end{aligned}$$

On the other hand, at $p = 0$ we have the following formula:

$$\begin{aligned} I_0 &= \int_0^{\pi/2} 1\, dt \\ &= \frac{\pi}{2} \end{aligned}$$

Also, at $p = 1$ we have the following formula:

$$\begin{aligned} I_1 &= \int_0^{\pi/2} \cos t\, dt \\ &= 1 \end{aligned}$$

Thus, we obtain the result, by recurrence.

As for the second formula, regarding the integrals of powers of $\sin t$, this follows from the first formula, with the following change of variables:

$$t = \frac{\pi}{2} - s$$

Thus, we have proved both formulae in the statement. □

As a first application, we can compute the volume of the sphere:

Theorem 6.6. *The volume of the sphere in $\mathbb{R}^N$ is given by*

$$\frac{V}{2^N}=\left(\frac{\pi}{2}\right)^{[N/2]}\frac{1}{(N+1)!!}$$

with the convention

$$N!!=(N-1)(N-3)(N-5)\ldots$$

with the product ending at 2 if N is odd, and ending at 1 if N is even.

Proof. This is standard, indeed, by using spherical coordinates, then Fubini, and then the formula in Proposition 6.5 in order to conclude.

To be more precise, let us denote by Q the positive part of the sphere, obtained by cutting the sphere in 2^N parts. We have then:

$$vol(S)=2^N vol(Q)$$

We have the following computation:

$$\begin{aligned}
&\frac{V}{2^N}\\
=\ &\int_Q 1\\
=\ &\int_0^1\int_0^{\pi/2}\ldots\int_0^{\pi/2} r^{N-1}\sin^{N-2}t_1\ldots\sin t_{N-2}\,drdt_1\ldots dt_{N-1}\\
=\ &\int_0^1 r^{N-1}dr\int_0^{\pi/2}\sin^{N-2}t_1\,dt_1\ldots\int_0^{\pi/2}\sin t_{N-2}dt_{N-2}\int_0^{\pi/2}1dt_{N-1}\\
=\ &\frac{1}{N}\times\left(\frac{\pi}{2}\right)^{[N/2]}\times\frac{(N-2)!!}{(N-1)!!}\cdot\frac{(N-3)!!}{(N-2)!!}\ldots\frac{2!!}{3!!}\cdot\frac{1!!}{2!!}\cdot 1\\
=\ &\frac{1}{N}\times\left(\frac{\pi}{2}\right)^{[N/2]}\times\frac{1}{(N-1)!!}\\
=\ &\left(\frac{\pi}{2}\right)^{[N/2]}\frac{1}{(N+1)!!}
\end{aligned}$$

Here we have used the following formula, for computing the exponent of $\pi/2$:

$$\begin{aligned} & \varepsilon(0)+\varepsilon(1)+\varepsilon(2)+\ldots+\varepsilon(N-2) \\ = \ & 1+0+1+\ldots+\varepsilon(N-2) \\ = \ & \left[\frac{N-2}{2}\right]+1 \\ = \ & \left[\frac{N}{2}\right] \end{aligned}$$

Thus, we obtain the formula in the statement. □

There are as well some other formulations, some of them involving the Gamma function. However, the formula in Theorem 6.6, which is uniform in N, is quite convenient.

As main particular cases of the above formula, we have:

Theorem 6.7. *The volumes of the low-dimensional spheres are as follows:*

(1) *At $N=1$, the length of the unit interval is:*

$$V=2$$

(2) *At $N=2$, the area of the unit disk is:*

$$V=\pi$$

(3) *At $N=3$, the volume of the unit sphere is:*

$$V=\frac{4\pi}{3}$$

(4) *At $N=4$, the volume of the corresponding unit sphere is:*

$$V=\frac{\pi^2}{2}$$

Proof. Some of these results are well-known, but we can obtain all of them as particular cases of the general formula in Theorem 6.6, as follows:

(1) At $N=1$ we obtain $V/2=1$, so $V=2$.

(2) At $N=2$ we obtain $V/4=\pi/2\cdot 1/2$, so $V=\pi$.

(3) At $N=3$ we obtain $V/8=\pi/2\cdot 1/3$, so $V=4\pi/3$.

(4) At $N=4$ we obtain $V/16=\pi^2/4\cdot 1/8$, so $V=\pi^2/2$. □

There are of course higher formulae as well.

In order to obtain estimates, we can use:

Theorem 6.8. *We have the Stirling formula*

$$N!\simeq\left(\frac{N}{e}\right)^N\sqrt{2\pi N}$$

and the higher order terms can be worked out too.

Proof. This is something quite tricky, the idea being to use the logarithm. Indeed, by using a Riemann sum, we can easily obtain the following formula:

$$\frac{1}{N}(\log 1+\log 2+\ldots+\log N)\simeq\log N-1$$

Thus, we are led to the following estimate:

$$N!\simeq\left(\frac{N}{e}\right)^N$$

With a bit more care, we obtain the formula in the statement, namely:

$$N!\simeq\left(\frac{N}{e}\right)^N\sqrt{2\pi N}$$

The higher terms are more delicate to obtain. □

With the above formula in hand, we have many applications, as follows:

Theorem 6.9. *Stirling approximations for:*

(1) *Binomial coefficients.*
(2) *Central binomial coefficients.*
(3) *Double factorials.*
(4) *Volumes of spheres.*

Proof. All this is quite standard, the idea being as follows:

(1) This follows from the definition of the binomial coefficients, namely:

$$\binom{N}{k}=\frac{N!}{k!(N-k)!}$$

(2) This follows from the definition of the central binomial coefficients:

$$\binom{2N}{N}=\frac{(2N)!}{N!N!}$$

(3) This follows from the definition of the double factorials:

$$N!!=(N-1)(N-3)(N-5)\ldots$$

(4) This follows from the formula in Theorem 6.6, namely:

$$\frac{V}{2^N}=\left(\frac{\pi}{2}\right)^{[N/2]}\frac{1}{(N+1)!!}$$

Thus, we are led to the conclusions in the statement. □

Let us discuss now the computation of the arbitrary integrals over the sphere.

We will need a technical result extending Proposition 6.5 above, as follows:

Theorem 6.10. *We have the following formula,*

$$\int_0^{\pi/2} \cos^p t \sin^q t \, dt = \left(\frac{\pi}{2}\right)^{\varepsilon(p)\varepsilon(q)} \frac{p!!q!!}{(p+q+1)!!}$$

where $\varepsilon(p) = 1$ if p is even, and $\varepsilon(p) = 0$ if p is odd, and where

$$m!! = (m-1)(m-3)(m-5)\ldots$$

with the product ending at 2 if m is odd, and ending at 1 if m is even.

Proof. This is standard, indeed, by doing a partial integration, and then proving the result by a double recurrence, on both p and q. Let us set indeed:

$$I_{pq} = \int_0^{\pi/2} \cos^p t \sin^q t \, dt$$

In order to do the partial integration, observe that we have:

$$\begin{aligned} & (\cos^p t \sin^q t)' \\ = \;& p \cos^{p-1} t(-\sin t) \sin^q t \\ + \;& \cos^p t \cdot q \sin^{q-1} t \cos t \\ = \;& -p \cos^{p-1} t \sin^{q+1} t + q \cos^{p+1} t \sin^{q-1} t \end{aligned}$$

By integrating between 0 and $\pi/2$, we obtain, for $p, q > 0$:

$$pI_{p-1,q+1} = qI_{p+1,q-1}$$

Thus, we can compute I_{pq} by recurrence. When q is even we have:

$$\begin{aligned} I_{pq} &= \frac{q-1}{p+1} I_{p+2,q-2} \\ &= \frac{q-1}{p+1} \cdot \frac{q-3}{p+3} I_{p+4,q-4} \\ &= \frac{q-1}{p+1} \cdot \frac{q-3}{p+3} \cdot \frac{q-5}{p+5} I_{p+6,q-6} \\ &= \vdots \\ &= \frac{p!!q!!}{(p+q)!!} I_{p+q} \end{aligned}$$

But the last term comes from Proposition 6.5, and we obtain the result:

$$\begin{aligned}
I_{pq} &= \frac{p!!q!!}{(p+q)!!}\,I_{p+q}\\
&= \frac{p!!q!!}{(p+q)!!}\left(\frac{\pi}{2}\right)^{\varepsilon(p+q)}\frac{(p+q)!!}{(p+q+1)!!}\\
&= \left(\frac{\pi}{2}\right)^{\varepsilon(p)\varepsilon(q)}\frac{p!!q!!}{(p+q+1)!!}
\end{aligned}$$

Observe that this gives the result for p even as well, by symmetry. Indeed, we have $I_{pq}=I_{qp}$, by using the following change of variables:

$$t=\frac{\pi}{2}-s$$

In the remaining case now, where both p,q are odd, we can use once again the formula $pI_{p-1,q+1}=qI_{p+1,q-1}$ established above, and the recurrence goes as follows:

$$\begin{aligned}
I_{pq} &= \frac{q-1}{p+1}\,I_{p+2,q-2}\\
&= \frac{q-1}{p+1}\cdot\frac{q-3}{p+3}\,I_{p+4,q-4}\\
&= \frac{q-1}{p+1}\cdot\frac{q-3}{p+3}\cdot\frac{q-5}{p+5}\,I_{p+6,q-6}\\
&= \vdots\\
&= \frac{p!!q!!}{(p+q-1)!!}\,I_{p+q-1,1}
\end{aligned}$$

In order to compute the last term, observe that we have:

$$\begin{aligned}
I_{p1} &= \int_0^{\pi/2}\cos^p t\sin t\,dt\\
&= -\frac{1}{p+1}\int_0^{\pi/2}(\cos^{p+1}t)'\,dt\\
&= \frac{1}{p+1}
\end{aligned}$$

Thus, we can finish our computation in the case p, q odd, as follows:

$$\begin{aligned} I_{pq} &= \frac{p!!q!!}{(p+q-1)!!}\, I_{p+q-1,1} \\ &= \frac{p!!q!!}{(p+q-1)!!} \cdot \frac{1}{p+q} \\ &= \frac{p!!q!!}{(p+q+1)!!} \end{aligned}$$

Thus, we obtain the formula in the statement, the exponent of $\pi/2$ appearing there being $\varepsilon(p)\varepsilon(q) = 0 \cdot 0 = 0$ in the present case, and this finishes the proof. □

We can now integrate over the spheres, as follows:

Theorem 6.11. *The spherical integral of $x_{i_1} \ldots x_{i_k}$ vanishes, unless each $a \in \{1, \ldots, N\}$ appears an even number of times in the sequence $i_1, \ldots, i_k$. We have*

$$\int_{S^{N-1}} x_{i_1} \ldots x_{i_k}\, dx = \frac{(N-1)!!l_1!! \ldots l_N!!}{(N + \Sigma l_i - 1)!!}$$

with l_a being this number of occurrences.

Proof. First, the result holds indeed at $N = 2$, due to the following formula proved above, where $\varepsilon(p) = 1$ when $p \in \mathbb{N}$ is even, and $\varepsilon(p) = 0$ when p is odd:

$$\int_0^{\pi/2} \cos^p t \sin^q t\, dt = \left(\frac{\pi}{2}\right)^{\varepsilon(p)\varepsilon(q)} \frac{p!!q!!}{(p+q+1)!!}$$

In general, we can restrict attention to the case $l_a \in 2\mathbb{N}$, since the other integrals vanish. The integral in the statement can be written in spherical coordinates, as follows:

$$I = \frac{2^N}{V} \int_0^{\pi/2} \ldots \int_0^{\pi/2} x_1^{l_1} \ldots x_N^{l_N} J\, dt_1 \ldots dt_{N-1}$$

In this formula, indeed:

– V is the volume of the sphere.

– J is the Jacobian.

– The 2^N factor comes from the restriction to the $1/2^N$ part of the sphere where all the coordinates are positive.

The normalization constant in front of the integral is:

$$\begin{aligned} \frac{2^N}{V} &= \frac{2^N}{N\pi^{N/2}} \cdot \Gamma\left(\frac{N}{2} + 1\right) \\ &= \left(\frac{2}{\pi}\right)^{[N/2]} (N-1)!! \end{aligned}$$

As for the unnormalized integral, this is given by:

$$I'=\int_0^{\pi/2}\ldots\int_0^{\pi/2}\quad(\cos t_1)^{l_1}(\sin t_1\cos t_2)^{l_2}$$
$$\vdots$$
$$(\sin t_1\sin t_2\ldots\sin t_{N-2}\cos t_{N-1})^{l_{N-1}}$$
$$(\sin t_1\sin t_2\ldots\sin t_{N-2}\sin t_{N-1})^{l_N}$$
$$\sin^{N-2}t_1\sin^{N-3}t_2\ldots\sin^2t_{N-3}\sin t_{N-2}$$
$$dt_1\ldots dt_{N-1}$$

By rearranging the terms, we obtain:

$$\begin{aligned}I'&=\int_0^{\pi/2}\cos^{l_1}t_1\sin^{l_2+\ldots+l_N+N-2}t_1\,dt_1\\&\int_0^{\pi/2}\cos^{l_2}t_2\sin^{l_3+\ldots+l_N+N-3}t_2\,dt_2\\&\vdots\\&\int_0^{\pi/2}\cos^{l_{N-2}}t_{N-2}\sin^{l_{N-1}+l_N+1}t_{N-2}\,dt_{N-2}\\&\int_0^{\pi/2}\cos^{l_{N-1}}t_{N-1}\sin^{l_N}t_{N-1}\,dt_{N-1}\end{aligned}$$

Now by using the above-mentioned formula at $N=2$, this gives:

$$\begin{aligned}I'&=\frac{l_1!!(l_2+\ldots+l_N+N-2)!!}{(l_1+\ldots+l_N+N-1)!!}\left(\frac{\pi}{2}\right)^{\varepsilon(N-2)}\\&\frac{l_2!!(l_3+\ldots+l_N+N-3)!!}{(l_2+\ldots+l_N+N-2)!!}\left(\frac{\pi}{2}\right)^{\varepsilon(N-3)}\\&\vdots\\&\frac{l_{N-2}!!(l_{N-1}+l_N+1)!!}{(l_{N-2}+l_{N-1}+l_N+2)!!}\left(\frac{\pi}{2}\right)^{\varepsilon(1)}\\&\frac{l_{N-1}!!l_N!!}{(l_{N-1}+l_N+1)!!}\left(\frac{\pi}{2}\right)^{\varepsilon(0)}\end{aligned}$$

Now observe that the various double factorials multiply up to quantity in the statement, modulo a $(N-1)!!$ factor, and that the $\frac{\pi}{2}$ factors multiply up to:

$$F=\left(\frac{\pi}{2}\right)^{[N/2]}$$

Thus by multiplying with the normalization constant, we obtain the result. □

More generally, we have the following useful formula:

Theorem 6.12. *For any $k_1, \ldots, k_p \in \mathbb{N}$ we have*

$$\int_{S^{N-1}} \left| x_1^{k_1} \ldots x_p^{k_p} \right| \, dx = \left(\frac{2}{\pi} \right)^{\Sigma(k_1,\ldots,k_p)} \frac{(N-1)!!k_1!! \ldots k_p!!}{(N+\Sigma k_i - 1)!!}$$

with $\Sigma = [odds/2]$ if N is odd and $\Sigma = [(odds+1)/2]$ if N is even, where "odds" denotes the number of odd numbers in the sequence $k_1, \ldots, k_p$.

Proof. The result holds indeed at $N = 2$, due to Proposition 6.5:

$$\frac{2}{\pi} \int_0^{\pi/2} \cos^p t \sin^q t \, dt = \left(\frac{2}{\pi} \right)^{\delta(p,q)} \frac{p!!q!!}{(p+q+1)!!}$$

Let us discuss now that general case. According to the general theory, the integral in the statement can be written in spherical coordinates, as follows:

$$I = \frac{2^N}{V} \int_0^{\pi/2} \ldots \int_0^{\pi/2} x_1^{k_1} \ldots x_N^{k_N} J \, dt_1 \ldots dt_{N-1}$$

Here V is the volume of the sphere, J is the Jacobian, and the 2^N factor comes from the restriction to the $1/2^N$ part of the sphere where all the coordinates are positive.

The normalization constant in front of the integral is:

$$\begin{aligned} \frac{2^N}{V} &= \frac{2^N}{N\pi^{N/2}} \cdot \Gamma\left(\frac{N}{2} + 1 \right) \\ &= \left(\frac{2}{\pi} \right)^{[N/2]} (N-1)!! \end{aligned}$$

As for the unnormalized integral, this is given by:

$$\begin{aligned} I' = \int_0^{\pi/2} \ldots \int_0^{\pi/2} \quad & (\cos t_1)^{k_1} \\ & (\sin t_1 \cos t_2)^{k_2} \\ & \vdots \\ & \vdots \\ & (\sin t_1 \sin t_2 \ldots \sin t_{N-2} \cos t_{N-1})^{k_{N-1}} \\ & (\sin t_1 \sin t_2 \ldots \sin t_{N-2} \sin t_{N-1})^{k_N} \\ & \sin^{N-2} t_1 \sin^{N-3} t_2 \ldots \sin^2 t_{N-3} \sin t_{N-2} \\ & dt_1 \ldots dt_{N-1} \end{aligned}$$

By rearranging the terms, we get:

$$\begin{aligned} & I' \\ = & \int_0^{\pi/2}\cos^{k_1}t_1\sin^{k_2+\ldots+k_N+N-2}t_1\,dt_1 \\ & \int_0^{\pi/2}\cos^{k_2}t_2\sin^{k_3+\ldots+k_N+N-3}t_2\,dt_2 \\ & \vdots \\ & \vdots \\ & \int_0^{\pi/2}\cos^{k_{N-2}}t_{N-2}\sin^{k_{N-1}+k_N+1}t_{N-2}\,dt_{N-2} \\ & \int_0^{\pi/2}\cos^{k_{N-1}}t_{N-1}\sin^{k_N}t_{N-1}\,dt_{N-1} \end{aligned}$$

Now by using the formula at $N=2$, we get:

$$\begin{aligned} & I' \\ = & \frac{\pi}{2}\cdot\frac{k_1!!(k_2+\ldots+k_N+N-2)!!}{(k_1+\ldots+k_N+N-1)!!}\left(\frac{2}{\pi}\right)^{\delta(k_1,k_2+\ldots+k_N+N-2)} \\ & \frac{\pi}{2}\cdot\frac{k_2!!(k_3+\ldots+k_N+N-3)!!}{(k_2+\ldots+k_N+N-2)!!}\left(\frac{2}{\pi}\right)^{\delta(k_2,k_3+\ldots+k_N+N-3)} \\ & \vdots \\ & \vdots \\ & \frac{\pi}{2}\cdot\frac{k_{N-2}!!(k_{N-1}+k_N+1)!!}{(k_{N-2}+k_{N-1}+k_N+2)!!}\left(\frac{2}{\pi}\right)^{\delta(k_{N-2},k_{N-1}+k_N+1)} \\ & \frac{\pi}{2}\cdot\frac{k_{N-1}!!k_N!!}{(k_{N-1}+k_N+1)!!}\left(\frac{2}{\pi}\right)^{\delta(k_{N-1},k_N)} \end{aligned}$$

In this expression most of the factorials cancel, and the δ exponents on the right sum up to the following number:

$$\Delta(k_1,\ldots,k_N)=\sum_{i=1}^{N-1}\delta(k_i,k_{i+1}+\ldots+k_N+N-i-1)$$

In other words, with this notation, the above formula reads:

$$\begin{aligned} & I' \\ = & \left(\frac{\pi}{2}\right)^{N-1} \frac{k_1!!k_2!!\ldots k_N!!}{(k_1+\ldots+k_N+N-1)!!} \left(\frac{2}{\pi}\right)^{\Delta(k_1,\ldots,k_N)} \\ = & \left(\frac{2}{\pi}\right)^{\Delta(k_1,\ldots,k_N)-N+1} \frac{k_1!!k_2!!\ldots k_N!!}{(k_1+\ldots+k_N+N-1)!!} \\ = & \left(\frac{2}{\pi}\right)^{\Sigma(k_1,\ldots,k_N)-[N/2]} \frac{k_1!!k_2!!\ldots k_N!!}{(k_1+\ldots+k_N+N-1)!!} \end{aligned}$$

Here the formula relating Δ to Σ follows from a number of simple observations, the first of which is the following one: due to obvious parity reasons, the sequence of δ numbers appearing in the definition of Δ cannot contain two consecutive zeroes.

Together with $I = (2^N/V)I'$, this gives the formula in the statement. □

As a first observation, the exponent Σ appearing in the above statement can be written as well in the following compact form:

$$\Sigma(k_1,\ldots,k_p) = \left[\frac{N+odds+1}{2}\right] - \left[\frac{N+1}{2}\right]$$

However, for concrete applications, the writing above is more convenient.

As a first application, we have the following result:

Theorem 6.13. *The moments of the hyperspherical variables are*

$$\int_{S^{N-1}} x_i^k dx = \frac{(N-1)!!k!!}{(N+k-1)!!}$$

and the normalized variables

$$y_i = \frac{x_i}{\sqrt{N}}$$

become normal with $N \to \infty$.

Proof. The formula in the statement follows from the general integration formula over the sphere, established above, which is as follows:

$$\int_{S^{N-1}} x_{i_1}\ldots x_{i_k}\, dx = \frac{(N-1)!!l_1!!\ldots l_N!!}{(N+\sum l_i-1)!!}$$

Indeed, with $i_1 = \ldots = i_k = i$, we obtain from this:

$$\int_{S^{N-1}} x_i^k dx = \frac{(N-1)!!k!!}{(N+k-1)!!}$$

Now observe that with $N\to\infty$ we have the following estimate:

$$\begin{aligned}\int_{S^{N-1}}x_i^kdx&=\frac{(N-1)!!}{(N+k-1)!!}\times k!!\\&\simeq N^{k/2}k!!\\&=N^{k/2}M_k(g_1)\end{aligned}$$

Thus, we are led to the conclusions in the statement. □

As a comment here, the rescaled variables $y_i=x_i/\sqrt{N}$ can be shown as well to become independent with $N\to\infty$. We will be back to this.

7. Spectral theory

We have seen so far the basics of linear algebra, concerning the determinant, and the diagonalization procedure, along with some applications. In this section we discuss a number of more advanced topics, commonly known as "spectral theory".

This theory can be developed either in finite or infinite dimensions, and the differences are not notable. We will jump on this occasion, and do things in infinite dimensions.

Among our motivations is the fact that the spaces of infinite dimensions are of great importance in various branches of theoretical physics, such as quantum mechanics.

Let us begin with some abstract theory. We have:

Definition 7.1. *A subset $V \subset \mathbb{C}^N$ is called a vector space when:*

(1) $u, v \in V \implies u, v \in V$.
(2) $\lambda \in \mathbb{C}, u \in V \implies \lambda u \in V$.

We have many interesting examples of such spaces.

More generally, we have the following definition:

Definition 7.2. *A vector space is a set V with an addition operation*

$$(u, v) \to u + v$$

and a multiplication by scalars operation

$$(\lambda, u) \to \lambda u$$

having the following properties:

(1) $u + v = v + u$.
(2) $(u + v) + w = u + (v + w)$.
(3) $(\lambda + \mu)u = \lambda u + \mu u$.
(4) $(\lambda\mu)u = \lambda(\mu u)$.
(5) $\lambda(u + v) = \lambda u + \lambda v$.

There are many examples of such spaces.

It is possible to talk about lines and so on, in the arbitrary vector spaces, but let us get straight to the point.

We can talk about linear maps, as follows:

Definition 7.3. *A map $f : V \to W$ is called linear when:*

(1) $f(u + v) = f(u) + f(v)$.
(2) $f(\lambda u) = \lambda f(u)$.

Observe that we must have $f(0) = 0$.

This fits with the previous definition of linearity. Also, we have ditched the notion of affine map, because we can easily recover these from the linear maps.

Let us develop some general theory. We first have:

Definition 7.4. *Let V be a vector space. A family $v_1, \ldots, v_n \in V$ is called:*

(1) *Linearly independent, when:*

$$\sum_i \lambda_i v_i = 0 \implies \lambda_i = 0$$

(2) *Generating, when any $v \in V$ can be written as:*

$$v = \sum_i \lambda_i v_i$$

(3) *A basis, when we can write*

$$v = \sum_i \lambda_i v_i$$

as above, in a unique way.

Observe that basis = linearly independent + generating.

We say that V is finite dimensional when it has a finite generating set. Observe that a subspace of a finite dimensional space is finite dimensional.

Here is now a key theorem:

Theorem 7.5. *Any finite dimensional vector space has a basis.*

Proof. This follows indeed by starting with a vector, and adding more vectors. □

In relation now with the linear maps, we have:

Theorem 7.6. *Any linear map $f : V \to W$ between finite dimensional linear spaces corresponds to a rectangular matrix.*

Proof. This follows exactly as in the $f : \mathbb{R}^N \to \mathbb{R}^M$ case. In fact, by using the basis theorem, we can assume that our map is of the form $f : \mathbb{R}^N \to \mathbb{R}^M$. □

We have the following result:

Proposition 7.7. *Let $f : V \to W$ be a linear map.*

(1) $\ker f$ *is a linear space.*
(2) Imf *is a linear space.*
(3) $\dim \ker f + \dim Imf = N$.

Proof. This is indeed standard. □

Let us discuss now the scalar products. We will only consider complex spaces. In infinite dimensions, the definition is the same as in finite dimensions, namely:

Definition 7.8. *A scalar product on a complex vector space H is an operation $H\times H\to\mathbb{C}$, denoted $(x,y)\to<x,y>$, satisfying the following conditions:*

(1) $<x,y>$ *is linear in* x*, and antilinear in* y*.*
(2) $\overline{<x,y>}=<y,x>$*, for any* x,y*.*
(3) $<x,x>>0$*, for any* $x\neq 0$*.*

As a basic example, we have $H=\mathbb{C}^N$, which scalar product as follows:

$$<x,y>=\sum_i x_i\bar{y}_i$$

Let us formulate now the following key definition:

Definition 7.9. *The norm of a vector $x\in H$ is the following quantity:*

$$||x||=\sqrt{<x,x>}$$

We also call this number length of x, or distance from x to the origin.

The terminology comes from what happens in $\mathbb{C}^N$.

We have two important results regarding the norms.

First is the Cauchy-Schwarz inequality:

Theorem 7.10. *We have the Cauchy-Schwarz inequality*

$$|<x,y>|\leq||x||\cdot||y||$$

and the equality case holds precisely when x,y are proportional.

Proof. Consider indeed the following quantity, depending on a real variable $t\in\mathbb{R}$, and on a variable on the unit circle, $w\in\mathbb{T}$:

$$f(t)=||wtx+y||^2$$

By developing f, we see that this is a degree 2 polynomial in t:

$$\begin{aligned}
& f(t)\\
= \;& <wtx+y,wtx+y>\\
= \;& t^2<x,x>+tw<x,y>+t\bar{w}<y,x>+<y,y>\\
= \;& t^2||x||^2+2tRe(w<x,y>)+||y||^2
\end{aligned}$$

Since f is obviously positive, its discriminant must be negative:

$$4Re(w<x,y>)^2-4||x||^2\cdot||y||^2\leq 0$$

But this is equivalent to the following condition:

$$|Re(w < x, y >)| \leq ||x|| \cdot ||y||$$

Now the point is that we can arrange for the number $w \in \mathbb{T}$ to be such that the quantity $w < x, y >$ is real. Thus, we obtain the following inequality:

$$| < x, y > | \leq ||x|| \cdot ||y||$$

Finally, the study of the equality case is straightforward. □

We have as well the Minkowski inequality:

Theorem 7.11. *We have the Minkowski inequality*

$$||x + y|| \leq ||x|| + ||y||$$

and the equality case holds precisely when x, y are proportional.

Proof. This follows indeed from the Cauchy-Schwarz inequality, as follows:

$$\begin{aligned}
& ||x + y|| \leq ||x|| + ||y|| \\
\iff \quad & ||x + y||^2 \leq (||x|| + ||y||)^2 \\
\iff \quad & ||x||^2 + ||y||^2 + 2Re < x, y > \leq ||x||^2 + ||y||^2 + 2||x|| \cdot ||y|| \\
\iff \quad & Re < x, y > \leq ||x|| \cdot ||y||
\end{aligned}$$

As for the equality case, this is clear from Cauchy-Schwarz as well. □

As a consequence of this, we have the following result:

Theorem 7.12. *The following function is a distance*

$$d(x, y) = ||x - y||$$

in the usual sense.

Proof. This follows indeed from the Minkowski inequality. □

Let us discuss now spectral theory. Our starting point will be:

Definition 7.13. *A Hilbert space is a complex vector space H given with a scalar product $< x, y >$, satisfying the following conditions:*

(1) $< x, y >$ *is linear in x, and antilinear in y.*
(2) $\overline{< x, y >} =< y, x >$, *for any x, y.*
(3) $< x, x >> 0$, *for any $x \neq 0$.*
(4) H *is complete with respect to the norm* $||x|| = \sqrt{< x, x >}$.

Here the fact that $||.||$ is indeed a norm comes from the Minkowski inequality.

As a basic example, we have $H = \mathbb{C}^N$, which usual scalar product:

$$< x, y >= \sum_i x_i \bar{y}_i$$

More generally, we have the following construction:

Proposition 7.14. *The sequences of numbers $x = (x_i)$ which are square-summable,*

$$\sum_i |x_i|^2 < \infty$$

form a Hilbert space, denoted $l^2(\mathbb{N})$, with the following scalar product:

$$< x, y >= \sum_i x_i \bar{y}_i$$

In fact, given any index set I, we can construct a Hilbert space $l^2(I)$, in this way.

Proof. This is clear, indeed. □

On the other hand, we can talk as well about spaces of functions, as follows:

Proposition 7.15. *Given an interval $X \subset \mathbb{R}$, the quantity*

$$< f, g >= \int_X f(x)\overline{g(x)}dx$$

is a scalar product, making $H = L^2(X)$ a Hilbert space.

Proof. This is routine, indeed. □

We can unify the above constructions, as follows:

Theorem 7.16. *Given a measured space X, the quantity*

$$< f, g >= \int_X f(x)\overline{g(x)}dx$$

is a scalar product, making $H = L^2(X)$ a Hilbert space.

Proof. Here the first assertion is clear, and the fact that the Cauchy sequences converge is clear as well, by taking the pointwise limit, and using a standard argument. □

Observe that with $X = \{1, \ldots, N\}$ we obtain the space $H = \mathbb{C}^N$. Also, with $X = \mathbb{N}$, with the counting measure, we obtain the space $H = l^2(\mathbb{N})$. In fact, with an arbitrary set I, once again with the counting mesure, we obtain the space $H = l^2(I)$.

Finally, we have the following important theoretical result:

Theorem 7.17. *Given a Hilbert space H, any algebraic basis*

$$\{f_i\}_{i\in I}$$

can be turned into an orthonormal basis

$$\{e_i\}_{i\in I}$$

by using the Gram-Schmidt procedure. Thus, we have

$$H \simeq l^2(I)$$

for a certain set I.

Proof. All this is standard, by recurrence in finite dimensions, and by recurrence as well in infinite, countable dimensions.

As for the case of infinite, uncountable dimensions, here the result holds as well, with the proof using recurrence arguments borrowed from logic. □

When the set I is countable, H is called separable. As a basic example, we have:

Proposition 7.18. *The following Hilbert space is separable,*

$$H = L^2[0,1]$$

because we can use the basis

$$f_n = x^n$$

with $n \in \mathbb{N}$, coming from the Weierstrass theorem.

Proof. Working out all this is actually an excellent exercise. □

Let us get now into the study of operators. We first have:

Theorem 7.19. *Let H be a Hilbert space, with orthonormal basis $\{e_i\}_{i\in I}$. The algebra $\mathcal{L}(H)$ of linear operators*

$$T : H \to H$$

embeds into the matrix algebra $M_I(\mathbb{C})$, with T corresponding to the matrix:

$$M_{ij} =< Te_j, e_i >$$

In particular:

(1) *In the finite dimensional case, where $\dim(H) = N < \infty$, we obtain in this way a usual matrix algebra:*

$$\mathcal{L}(H) \simeq M_N(\mathbb{C})$$

(2) *In the separable infinite dimensional case, where $I \simeq \mathbb{N}$, we obtain in this way an algebra of infinite matrices:*

$$\mathcal{L}(H) \subset M_\infty(\mathbb{C})$$

Proof. The correspondence $T \to M$ is indeed linear, its kernel is $\{0\}$, and its image is contained in $M_I(\mathbb{C})$. As for the last two assertions, these are clear as well. □

In infinite dimensions, the embedding $\mathcal{L}(H) \subset M_I(\mathbb{C})$ that we obtain is not an isomorphism. For instance on $H = l^2(\mathbb{N})$ the following matrix does not define an operator:

$$M = \begin{pmatrix} 1 & 1 & \ldots \\ 1 & 1 & \ldots \\ \vdots & \vdots & \end{pmatrix}$$

The above result is something quite theoretical, because for basic spaces like $L^2[0,1]$, which do not have a simple orthonormal basis, the embedding $\mathcal{L}(H) \subset M_\infty(\mathbb{C})$ that we obtain is not very useful.

Thus, while the operators $T : H \to H$ are basically some infinite matrices, it is better to think of these operators as being objects on their own.

In what follows we will be interested in the operators $T : H \to H$ which are bounded. Regarding such operators, we have the following result:

Theorem 7.20. *Given a Hilbert space H, the linear operators $T : H \to H$ which are bounded, in the sense that we have*

$$||T|| = \sup_{||x|| \leq 1} ||Tx|| < \infty$$

form a complex algebra with unit $B(H)$, having the property

$$||ST|| \leq ||S|| \cdot ||T||$$

and which is complete with respect to the norm (the Cauchy sequences converge).

Proof. The fact that we have indeed an algebra follows from the following estimates, which are all elementary:

$$||S + T|| \leq ||S|| + ||T||$$
$$||\lambda T|| = |\lambda| \cdot ||T||$$
$$||ST|| \leq ||S|| \cdot ||T||$$

Regarding now the last assertion, if $\{T_n\} \subset B(H)$ is Cauchy then $\{T_n x\}$ is Cauchy for any $x \in H$, so we can define the limit $T = \lim_{n\to\infty} T_n$ by setting:

$$Tx = \lim_{n\to\infty} T_n x$$

Let us first check that the application $x \to Tx$ is linear. We have:

$$\begin{aligned} T(x + y) &= \lim_{n\to\infty} T_n(x + y) \\ &= \lim_{n\to\infty} T_n(x) + T_n(y) \\ &= \lim_{n\to\infty} T_n(x) + \lim_{n\to\infty} T_n(y) \\ &= T(x) + T(y) \end{aligned}$$

Similarly, we have as well the following computation:

$$\begin{aligned} T(\lambda x) &= \lim_{n\to\infty} T_n(\lambda x) \\ &= \lambda \lim_{n\to\infty} T_n(x) \\ &= \lambda T(x) \end{aligned}$$

Thus we have $T \in \mathcal{L}(H)$. It remains now to prove that we have $T \in B(H)$, and that $T_n \to T$ in norm. For this purpose, observe that we have:

$$\begin{aligned} & ||T_n - T_m|| \leq \varepsilon \ , \ \forall n, m \geq N \\ \implies & ||T_n x - T_m x|| \leq \varepsilon \ , \ \forall ||x|| = 1 \ , \ \forall n, m \geq N \\ \implies & ||T_n x - Tx|| \leq \varepsilon \ , \ \forall ||x|| = 1 \ , \ \forall n \geq N \\ \implies & ||T_N x - Tx|| \leq \varepsilon \ , \ \forall ||x|| = 1 \\ \implies & ||T_N - T|| \leq \varepsilon \end{aligned}$$

As a first consequence, we obtain $T \in B(H)$, because we have:

$$\begin{aligned} ||T|| &= ||T_N + (T - T_N)|| \\ &\leq ||T_N|| + ||T - T_N|| \\ &\leq ||T_N|| + \varepsilon \\ &< \infty \end{aligned}$$

As a second consequence, we obtain $T_N \to T$ in norm, and we are done. □

As a first observation, in view of the construction from Theorem 7.19 above we have embeddings as follows:

$$B(H) \subset \mathcal{L}(H) \subset M_I(\mathbb{C})$$

To be more precise, the algebra $B(H)$ consists of the $I \times I$ complex matrices which define linear maps $T : H \to H$, and which satisfy as well a second boundedness condition, coming from:

$$||T|| < \infty$$

In finite dimensions we have equalities everywhere, but in general this is not true, the standard example of a non-bounded operator being:

$$T = \begin{pmatrix} 1 & & \\ & 2 & \\ & & \ddots \end{pmatrix}$$

However, as already mentioned after Theorem 7.19, this is something quite theoretical, because for basic function spaces like $L^2[0,1]$, the embedding $B(H) \subset M_\infty(\mathbb{C})$ that we obtain is not very useful. Thus, while the operators $T : H \to H$ are basically some infinite matrices, it is better to think of these operators as being objects on their own.

We will be interested in what follows in $B(H)$ and its closed subalgebras $A \subset B(H)$. It is convenient to formulate the following definition:

Definition 7.21. *A Banach algebra is a complex algebra with unit A, having a vector space norm $||.||$ satisfying*

$$||ab|| \leq ||a|| \cdot ||b||$$

and which makes it a Banach space (the Cauchy sequences converge).

As already mentioned, the basic examples of Banach algebras, or at least the basic examples that we will be interested in here, are the operator algebra $B(H)$, and its norm closed subalgebras $A \subset B(H)$, such as the algebras $A =< T >$ generated by a single operator $T \in B(H)$. There are many other examples, but more on this later.

Generally speaking, the elements $a \in A$ of a Banach algebra can be thought of as being operators on some Hilbert space, which is not present.

With this idea in mind, we can emulate spectral theory in our setting, the starting point being:

Definition 7.22. *The spectrum of an element $a \in A$ is the set*

$$\sigma(a) = \left\{\lambda \in \mathbb{C} \middle| a - \lambda \notin A^{-1}\right\}$$

where $A^{-1} \subset A$ is the set of invertible elements.

As a basic example, the spectrum of a usual matrix $M \in M_N(\mathbb{C})$ is the collection of its eigenvalues, taken of course without multiplicities. In the case of the trivial algebra $A = \mathbb{C}$, appearing at $N = 1$, the spectrum of an element is the element itself.

As a first, basic result regarding spectra, we have:

Proposition 7.23. *We have the following formula, valid for any $a, b \in A$:*

$$\sigma(ab) \cup \{0\} = \sigma(ba) \cup \{0\}$$

Moreover, there are examples where $\sigma(ab) \neq \sigma(ba)$.

Proof. We first prove that we have:

$$1 \notin \sigma(ab) \implies 1 \notin \sigma(ba)$$

Assume indeed that $1 - ab$ is invertible, with inverse:

$$c = (1 - ab)^{-1}$$

We have then the following formulae:

$$abc = cab = c - 1$$

By using these formulae, we obtain:

$$\begin{aligned}
&(1+bca)(1-ba)\\
=\ &1+bca-ba-bcaba\\
=\ &1+bca-ba-bca+ba\\
=\ &1
\end{aligned}$$

A similar computation shows that we have:

$$(1-ba)(1+bca)=1$$

We conclude that $1-ba$ is invertible, with inverse $1+bca$, which proves our claim.

By multiplying by scalars, we deduce from this that for any $\lambda\in\mathbb{C}-\{0\}$ we have:

$$\lambda\notin\sigma(ab)\implies\lambda\notin\sigma(ba)$$

But this leads to the conclusion in the statement, namely:

$$\sigma(ab)\cup\{0\}=\sigma(ba)\cup\{0\}$$

Regarding now the last claim, let us first recall that for usual matrices $a,b\in M_N(\mathbb{C})$ we have $0\in\sigma(ab)\iff 0\in\sigma(ba)$, because ab is invertible if any only if ba is.

However, this latter fact fails for general operators on Hilbert spaces. As a basic example here, we can take our operator a to be the shift on the space $l^2(\mathbb{N})$:

$$S(e_i)=e_{i+1}$$

As for b, we can take the adjoint of S, which is the following operator:

$$S^*(e_i)=\begin{cases}e_{i-1} & \text{if } i>0\\ 0 & \text{if } i=0\end{cases}$$

Indeed, we have $S^*S=1$, and so:

$$0\notin\sigma(SS^*)$$

On the other, hand, SS^* being the projection onto $e_0^\perp$, this operator is not invertible, and so:

$$0\in\sigma(SS^*)$$

Thus, the spectra do not match on 0. □

Let us discuss now a second basic about spectra, which is very useful.

Given an element $a\in A$, and a rational function $f=P/Q$ having poles outside $\sigma(a)$, we can construct the element:

$$f(a)=P(a)Q(a)^{-1}$$

For simplicity, we write:

$$f(a)=\frac{P(a)}{Q(a)}$$

With this convention, we have the following result:

Theorem 7.24. *We have the "rational functional calculus" formula*

$$\sigma(f(a)) = f(\sigma(a))$$

valid for any rational function $f \in \mathbb{C}(X)$ having poles outside $\sigma(a)$.

Proof. In order to prove this result, we can proceed in two steps, as follows:

(1) Assume first that we are in the polynomial function case, $f \in \mathbb{C}[X]$. We pick a scalar $\lambda \in \mathbb{C}$, and we write:

$$f(X) - \lambda = c(X - r_1) \dots (X - r_n)$$

We have then, as desired:

$$\begin{aligned}
& \lambda \notin \sigma(f(a)) \\
\iff \quad & f(a) - \lambda \in A^{-1} \\
\iff \quad & c(a - r_1) \dots (a - r_n) \in A^{-1} \\
\iff \quad & a - r_1, \dots, a - r_n \in A^{-1} \\
\iff \quad & r_1, \dots, r_n \notin \sigma(a) \\
\iff \quad & \lambda \notin f(\sigma(a))
\end{aligned}$$

(2) Assume now that we are in the general case, $f \in \mathbb{C}(X)$. We pick a scalar $\lambda \in \mathbb{C}$, we write $f = P/Q$, and we set:

$$F = P - \lambda Q$$

By using now (1), for this polynomial, we obtain:

$$\begin{aligned}
& \lambda \in \sigma(f(a)) \\
\iff \quad & F(a) \notin A^{-1} \\
\iff \quad & 0 \in \sigma(F(a)) \\
\iff \quad & 0 \in F(\sigma(a)) \\
\iff \quad & \exists \mu \in \sigma(a), F(\mu) = 0 \\
\iff \quad & \lambda \in f(\sigma(a))
\end{aligned}$$

Thus, we have obtained the formula in the statement. □

Let us prove now that the spectra are non-empty, $\sigma(a) \neq \emptyset$. This is of course something that we know well for the usual matrices. However, a bit of thinking tells us that, even for the usual matrices, this is something quite advanced.

In general, this is definitely something non-trivial.

In order to establish this result, we will need a number of preliminaries, as follows:

Proposition 7.25. *Let A be a Banach algebra.*

(1) $||a|| < 1 \implies (1-a)^{-1} = 1 + a + a^2 + \ldots$
(2) *The set A^{-1} is open.*
(3) *The map $a \to a^{-1}$ is differentiable.*

Proof. All these assertions are elementary, as follows:

(1) This follows exactly as in the scalar case, by using the norm.

(2) Assuming $a \in A^{-1}$ and $||a - b|| < \frac{1}{||a^{-1}||}$, we have:

$$\begin{aligned} & ||1 - a^{-1}b|| \\ = \ & ||a^{-1}(a-b)|| \\ \leq \ & ||a^{-1}|| \cdot ||a-b|| \\ < \ & 1 \end{aligned}$$

Thus by (1) we have:

$$a^{-1}b \in A^{-1}$$

We deduce that we have $b \in A^{-1}$, as desired.

(3) This follows as in the scalar case, the formula of the derivative being:

$$f'(a)x = -a^{-1}xa^{-1}$$

To be more precise, this is the term which appears at order 1, when developing. □

We can now formulate a key theorem about Banach algebras, as follows:

Theorem 7.26. *The spectrum of a Banach algebra element $\sigma(a) \subset \mathbb{C}$ is:*

(1) *Compact.*
(2) *Contained in the disc $D_0(||a||)$.*
(3) *Non-empty.*

Proof. This can be proved by using the above results, as follows:

(1) In view of (2) below, it is enough to prove that $\sigma(a)$ is closed. But this follows from the following computation, with $|\varepsilon|$ being small:

$$\begin{aligned} \lambda \notin \sigma(a) \quad & \implies \quad a - \lambda \in A^{-1} \\ & \implies \quad a - \lambda - \varepsilon \in A^{-1} \\ & \implies \quad \lambda + \varepsilon \notin \sigma(a) \end{aligned}$$

(2) This follows from the following computation:

$$\begin{aligned}\lambda > ||a|| &\implies \left|\left|\frac{a}{\lambda}\right|\right| < 1\\ &\implies 1-\frac{a}{\lambda} \in A^{-1}\\ &\implies \lambda - a \in A^{-1}\\ &\implies \lambda \notin \sigma(a)\end{aligned}$$

(3) Assume by contradiction $\sigma(a) = \emptyset$. Given a linear form $f \in A^*$, consider the following map, which is well-defined, due to our assumption $\sigma(a) = \emptyset$:

$$\varphi : \mathbb{C} \to \mathbb{C}$$

$$\lambda \to f((a-\lambda)^{-1})$$

This map is differentiable, and so holomorphic. Also, we have:

$$\begin{aligned}&\lambda \to \infty\\ \implies\ &a - \lambda \to \infty\\ \implies\ &(a-\lambda)^{-1} \to 0\\ \implies\ &f((a-\lambda))^{-1} \to 0\end{aligned}$$

Thus by the Liouville theorem we obtain:

$$\varphi = 0$$

With this in hand, by Hahn-Banach we obtain then:

$$(a-\lambda)^{-1} = 0$$

But this is a contradition, as desired. □

This was for the basic spectral theory in Banach algebras. It is possible to go beyond this, notably with a holomorphic function extension of the rational functional calculus formula $\sigma(f(a)) = f(\sigma(a))$ from Theorem 7.24, but we will not need this here.

Instead, let us get back now to the operator algebra $B(H)$, from Theorem 7.20. The point is that this Banach algebra is of a very special type, due to the following fact:

Theorem 7.27. *The Banach algebra $B(H)$ has an involution $T \to T^*$, given by*

$$< Tx, y > = < x, T^*y >$$

and the norm the involution are related by the formula $||TT^*|| = ||T||^2$.

Proof. The existence of the adjoint operator T^*, given by the formula in the statement, comes from the fact that $\varphi(x) =< Tx, y >$ being a linear map $H \to \mathbb{C}$, we must have a formula as follows, for a certain vector $T^*y \in H$:

$$\varphi(x) =< x, T^*y >$$

Moreover, since this vector is unique, T^* is unique too, and we have as well:

$$(S+T)^* = S^* + T^*$$

$$(\lambda T)^* = \bar{\lambda} T^*$$

$$(ST)^* = T^* S^*$$

$$(T^*)^* = T$$

Observe also that we have indeed $T^* \in B(H)$, because:

$$\begin{aligned} ||T|| &= \sup_{||x||=1} \sup_{||y||=1} < Tx, y > \\ &= \sup_{||y||=1} \sup_{||x||=1} < x, T^*y > \\ &= ||T^*|| \end{aligned}$$

Regarding now the last assertion, observe that we have:

$$\begin{aligned} ||TT^*|| &\leq ||T|| \cdot ||T^*|| \\ &= ||T||^2 \end{aligned}$$

On the other hand, we have as well the following estimate:

$$\begin{aligned} ||T||^2 &= \sup_{||x||=1} | < Tx, Tx > | \\ &= \sup_{||x||=1} | < x, T^*Tx > | \\ &\leq ||T^*T|| \end{aligned}$$

By replacing $T \to T^*$ we obtain from this:

$$||T||^2 \leq ||TT^*||$$

Thus, we have obtained the needed inequality, and we are done. □

As a first observation, in the context of the construction $T \to M$ from Theorem 7.19 above, the adjoint operation $T \to T^*$ takes a very simple form, namely:

$$(M^*)_{ij} = \overline{M}_{ji}$$

However, as already explained before, while the operators $T : H \to H$ are basically some infinite matrices, it is better to think of them as being objects on their own.

The above result suggests the following definition:

Definition 7.28. *A unital C^*-algebra is a complex algebra with unit A, having:*

(1) *A norm $a \to ||a||$, making it a Banach algebra (the Cauchy sequences converge).*
(2) *An involution $a \to a^*$, which satisfies $||aa^*|| = ||a||^2$, for any $a \in A$.*

As a basic example here, we know from Theorem 7.27 above that the full operator algebra $B(H)$ is a C^*-algebra, for any Hilbert space H.

More generally, any closed $*$-subalgebra $A \subset B(H)$ is a C^*-algebra. The celebrated Gelfand-Naimark-Segal (GNS) theorem states that any C^*-algebra appears in fact in this way. This is something non-trivial, and we will be back to it later on.

For the moment, we are interested in developing the theory of C^*-algebras, without reference to operators, or Hilbert spaces.

Our first task will be that of understanding the structure of the commutative C^*-algebras. As a first observation, we have:

Proposition 7.29. *If X is an abstract compact space, the algebra $C(X)$ of continuous functions $f : X \to \mathbb{C}$ is a C^*-algebra, with structure as follows:*

(1) *The norm is the usual sup norm:*

$$||f|| = \sup_{x \in X} |f(x)|$$

(2) *The involution is the usual involution:*

$$f^*(x) = \overline{f(x)}$$

This algebra is commutative, in the sense that $fg = gf$, for any $f, g \in C(X)$.

Proof. Almost everything here is trivial. Observe also that we have indeed:

$$\begin{aligned} ||ff^*|| &= \sup_{x \in X} |f(x)\overline{f(x)}| \\ &= \sup_{x \in X} |f(x)|^2 \\ &= ||f||^2 \end{aligned}$$

Finally, we have $fg = gf$, since for any $x \in X$ we have:

$$f(x)g(x) = g(x)f(x)$$

Thus, we are led to the conclusions in the statement. □

Our claim now is that any commutative C^*-algebra appears in this way. This is a non-trivial result, which requires a number of preliminaries. We will need:

Definition 7.30. *Given an element $a \in A$, its spectral radius*

$$\rho(a) \in (0, ||a||)$$

is the radius of the smallest disk centered at 0 containing $\sigma(a)$.

Here we have used a number of results that we already know.

We have the following key result, extending our spectral theory knowledge:

Theorem 7.31. *Let A be a C^*-algebra.*

(1) *The spectrum of a norm one element is in the unit disk.*
(2) *The spectrum of a unitary element ($a^* = a^{-1}$) is on the unit circle.*
(3) *The spectrum of a self-adjoint element ($a = a^*$) consists of real numbers.*
(4) *The spectral radius of a normal element ($aa^* = a^*a$) is equal to its norm.*

Proof. We use the various results established above.

(1) This comes from the following formula, valid when $||a|| < 1$:

$$\frac{1}{1-a} = 1 + a + a^2 + \ldots$$

(2) This follows by using Theorem 7.24, with the following function:

$$f(z) = z^{-1}$$

Indeed, we have the following computation:

$$\begin{aligned} \sigma(a)^{-1} &= \sigma(a^{-1}) \\ &= \sigma(a^*) \\ &= \overline{\sigma(a)} \end{aligned}$$

Now since $\lambda^{-1} = \bar{\lambda}$ characterizes the elements $\lambda \in \mathbb{T}$, this gives the result.

(3) This follows by using the result (2), just established above, and Theorem 7.24, with the following rational function, depending on $t \in \mathbb{R}$:

$$f(z) = \frac{z + it}{z - it}$$

Indeed, for $t >> 0$ the element $f(a)$ is well-defined, and we have:

$$\begin{aligned} \left(\frac{a+it}{a-it}\right)^* &= \frac{a-it}{a+it} \\ &= \left(\frac{a+it}{a-it}\right)^{-1} \end{aligned}$$

Thus the element $f(a)$ is a unitary, and by using (2) its spectrum is contained in $\mathbb{T}$. We conclude that we have:

$$f(\sigma(a)) = \sigma(f(a)) \subset \mathbb{T}$$

Thus we obtain:

$$\sigma(a) \subset f^{-1}(\mathbb{T}) = \mathbb{R}$$

In other words, we have proved the result.

(4) We already know from (1) that we have the following inequality:

$$\rho(a) \leq ||a||$$

For the converse, we fix a number as follows:

$$\rho > \rho(a)$$

We have the following computation:

$$\begin{aligned} \int_{|z|=\rho} \frac{z^n}{z-a}\, dz &= \sum_{k=0}^{\infty} \left(\int_{|z|=\rho} z^{n-k-1} dz \right) a^k \\ &= a^{n-1} \end{aligned}$$

By applying the norm and taking n-th roots we obtain from this:

$$\rho \geq \lim_{n\to\infty} ||a^n||^{1/n}$$

In the case $a = a^*$ we have $||a^n|| = ||a||^n$ for any exponent of the form $n = 2^k$, and by taking n-th roots we get:

$$\rho \geq ||a||$$

But this gives the missing inequality:

$$\rho(a) \geq ||a||$$

In the general case $aa^* = a^*a$ we have:

$$a^n(a^n)^* = (aa^*)^n$$

We therefore obtain from this, by using our above observation:

$$\rho(a)^2 = \rho(aa^*)$$

Now since aa^* is self-adjoint, we get:

$$\rho(aa^*) = ||a||^2$$

Thus, we are done. □

Summarizing, we have so far a collection of technical results regarding the spectra of the elements in C^*-algebras, which are similar to the results regarding the eigenvalues of the usual matrices. This list can be enlarged, but for the moment, this is all we need.

We are now in position of proving a key result, namely:

Theorem 7.32 (Gelfand). *Any commutative C^*-algebra is the form $C(X)$, with its "spectrum"*

$$X = Spec(A)$$

appearing as the space of characters:

$$\chi : A \to \mathbb{C}$$

Proof. Given a commutative C^*-algebra A, we can define indeed X to be the set of characters $\chi : A \to \mathbb{C}$, with the topology making continuous all the evaluation maps:

$$ev_a : \chi \to \chi(a)$$

Then X is a compact space, and $a \to ev_a$ is a morphism of algebras:

$$ev : A \to C(X)$$

We first prove that ev is involutive. We use the following formula:

$$a = \frac{a + a^*}{2} - i \cdot \frac{i(a - a^*)}{2}$$

Thus it is enough to prove the following equality, for self-adjoint elements a:

$$ev_{a^*} = ev_a^*$$

But this is the same as proving that $a = a^*$ implies that ev_a is a real function, which is in turn true, because $ev_a(\chi) = \chi(a)$ is an element of $\sigma(a)$, contained in $\mathbb{R}$.

Since A is commutative, each element is normal, so ev is isometric:

$$\begin{aligned} ||ev_a|| &= \rho(a) \\ &= ||a|| \end{aligned}$$

It remains to prove that ev is surjective. But this follows from the Stone-Weierstrass theorem, because $ev(A)$ is a closed subalgebra of $C(X)$, which separates the points. □

As a first consequence of the Gelfand theorem, we can extend Theorem 7.24 above to the case of the normal elements ($aa^* = a^*a$), in the following way:

Theorem 7.33. *Assume that $a \in A$ is normal, and let $f \in C(\sigma(a))$.*

(1) *We can define an element*

$$f(a) \in A$$

with $f \to f(a)$ being a morphism of C^*-algebras.

(2) *We have the "continuous functional calculus" formula:*

$$\sigma(f(a)) = f(\sigma(a))$$

Proof. Since our element a is normal, the C^*-algebra $B =< a >$ that is generates is commutative, and the Gelfand theorem gives an identification as follows:

$$B = C(X)$$

$$X = Spec(B)$$

The map $X \to \sigma(a)$ given by evaluation at a being bijective, we have an identification of compact spaces, as follows:

$$X = \sigma(a)$$

Thus we have $B = C(\sigma(a))$, and this gives all the assertions. □

As an important remark here, the above result, when applied to the normal operators $T \in B(H)$, is more of less the spectral theorem for such operators.

We can develop as well the theory of positive elements, as follows:

Theorem 7.34. *For an element $a \in A$, the following are equivalent:*

(1) *a is positive, in the sense that $\sigma(a) \subset [0, \infty)$.*
(2) *$a = b^2$, for some $b \in A$ satisfying $b = b^*$.*
(3) *$a = cc^*$, for some $c \in A$.*

Proof. This is something quite standard, as follows:

(1) $\implies$ (2) Observe that $\sigma(a) \subset \mathbb{R}$ implies $a = a^*$. Thus the algebra $< a >$ is commutative, and by using the Gelfand theorem, we can set $b = \sqrt{a}$.

(2) $\implies$ (3) This is trivial, because we can set $c = b$.

(2) $\implies$ (1) This is clear too, because we have:

$$\begin{aligned} \sigma(a) &= \sigma(b^2) \\ &= \sigma(b)^2 \subset \mathbb{R}^2 \\ &= [0, \infty) \end{aligned}$$

(3) $\implies$ (1) We proceed by contradiction. By multiplying c by a suitable element of $< cc^* >$, we are led to the existence of an element $d \neq 0$ satisfying:

$$-dd^* \geq 0$$

By writing now $d = x + iy$ with $x = x^*, y = y^*$ we have:

$$dd^* + d^*d = 2(x^2 + y^2) \geq 0$$

Thus $d^*d \geq 0$. But this contradicts the elementary fact that $\sigma(dd^*), \sigma(d^*d)$ must coincide outside $\{0\}$, coming from Proposition 7.23 above. □

The Gelfand theorem has as well some important philosophical consequences. Indeed, in view of this theorem, we can formulate the following definition:

Definition 7.35. *Given an arbitrary C^*-algebra A, we write*

$$A = C(X)$$

and call X a noncommutative compact space. Equivalently, the category of the noncommutative compact spaces is the category of the C^*-algebras, with the arrows reversed.

When A is commutative, the space X considered above exists indeed, as a Gelfand spectrum, $X = Spec(A)$. In general, X is something rather abstract, and our philosophy here will be that of studying of course A, but formulating our results in terms of X. For instance whenever we have a morphism $\Phi : A \to B$, we will write $A = C(X), B = C(Y)$, and rather speak of the corresponding morphism $\phi : Y \to X$. And so on.

As a second main result about the C^*-algebras, we have:

Theorem 7.36. *Let $A \subset M_n(\mathbb{C})$ be a C^*-algebra.*

(1) *We can write $1 = q_1 + \ldots + q_k$, with $q_i \in A$ central minimal projections.*
(2) *Each of the linear spaces $A_i = q_i A q_i$ is a non-unital $*$-subalgebra of A.*
(3) *We have a non-unital $*$-algebra sum decomposition $A = A_1 \oplus \ldots \oplus A_k$.*
(4) *We have unital $*$-algebra isomorphisms $A_i \simeq M_{r_i}(\mathbb{C})$, where $r_i = rank(q_i)$.*
(5) *Thus, we have a C^*-algebra isomorphism $A \simeq M_{r_1}(\mathbb{C}) \oplus \ldots \oplus M_{r_k}(\mathbb{C})$.*

Proof. This is something well-known, with the proof of the assertions (1,2,3,4,5) in the statement being something elementary, and routine:

(1) This is rather a definition.

(2) This is something clear.

(3) The direct sum conditions are indeed easy to check.

(4) This comes from the fact that each q_i was chosen central minimal.

(5) This follows from (3,4). □

Let us review now the third fundamental result regarding the C^*-algebras, namely the representation theorem of Gelfand, Naimark and Segal, which states that any C^*-algebra appears as an algebra of operators, $A \subset B(H)$, over some Hilbert space H.

In the commutative case, the precise statement is as follows:

Proposition 7.37. *Let A be a commutative C^*-algebra, write $A = C(X)$, with X being a compact space, and let μ be a positive measure on X. We have then an embedding*

$$A \subset B(H)$$

where $H = L^2(X)$, with $f \in A$ corresponding to the operator $g \to fg$.

Proof. Given $f \in C(X)$, consider the following operator, on the space $H = L^2(X)$:

$$T_f(g) = fg$$

Observe that T_f is indeed well-defined, and bounded as well, because:

$$\begin{aligned} ||fg||_2 &= \sqrt{\int_X |f(x)|^2 |g(x)|^2 d\mu(x)} \\ &\leq ||f||_\infty ||g||_2 \end{aligned}$$

The application $f \to T_f$ being linear, involutive, continuous, and injective as well, we obtain in this way a C^*-algebra embedding $A \subset B(H)$, as claimed. □

In general, the idea will be that of extending the above construction. In order to do so, we must first discuss the analogues of the positive measures.

In order to do so, we will use a functional analysis trick, coming from the Riesz theorem, which amounts in replacing the positive measures μ with the corresponding integration functionals. To be more precise, let us start with the following definition:

Definition 7.38. *Consider a linear map $\varphi : A \to \mathbb{C}$.*

(1) *φ is called positive when:*

$$a \geq 0 \implies \varphi(a) \geq 0$$

(2) *φ is called faithful and positive when:*

$$a \geq 0, a \neq 0 \implies \varphi(a) > 0$$

In the commutative case, $A = C(X)$, the positive linear forms appear as follows, with μ being positive, and strictly positive if we want φ to be faithful and positive:

$$\varphi(f) = \int_X f(x) d\mu(x)$$

In general, the positive linear forms can be thought of as being integration functionals with respect to some underlying "positive measures".

We can use these positive linear forms as follows:

Proposition 7.39. *Let $\varphi : A \to \mathbb{C}$ be a positive linear form.*

(1) *$< a, b >= \varphi(ab^*)$ defines a generalized scalar product on A.*
(2) *By separating and completing we obtain a Hilbert space H.*
(3) *$\pi(a) : b \to ab$ defines a representation $\pi : A \to B(H)$.*
(4) *If φ is faithful in the above sense, then π is faithful.*

Proof. Almost everything here is straightforward, as follows:

(1) This is clear from definitions, and from Theorem 7.34.

(2) This is a standard procedure, which works for any scalar product.

(3) All the verifications here are standard algebraic computations.

(4) This follows indeed from:

$$a \neq 0 \implies \pi(aa^*) \neq 0 \implies \pi(a) \neq 0$$

Thus, we obtain the result. □

In order to establish the GNS theorem, it remains to prove that any C^*-algebra has a faithful and positive linear form $\varphi : A \to \mathbb{C}$. This is something more technical:

Theorem 7.40. *Let A be a C^*-algebra.*

(1) *Any positive linear form $\varphi : A \to \mathbb{C}$ is continuous.*
(2) *A linear form φ is positive iff there is a norm one $h \in A_+$ such that $||\varphi|| = \varphi(h)$.*
(3) *For any $a \in A$ there exists a positive norm one form φ such that $\varphi(aa^*) = ||a||^2$.*
(4) *If A is separable there is a faithful positive form $\varphi : A \to \mathbb{C}$.*

Proof. The proof here, which is quite technical, inspired from the existence proof of the probability measures on abstract compact spaces, goes as follows:

(1) This follows from Proposition 7.39, via the following inequality:

$$\begin{aligned} |\varphi(a)| &\leq ||\pi(a)||\varphi(1) \\ &\leq ||a||\varphi(1) \end{aligned}$$

(2) In one sense we can take $h = 1$. Conversely, let $a \in A_+$, $||a|| \leq 1$. We have:

$$\begin{aligned} |\varphi(h) - \varphi(a)| &\leq ||\varphi|| \cdot ||h - a|| \\ &\leq \varphi(h)1 \\ &= \varphi(h) \end{aligned}$$

Thus we have:

$$Re(\varphi(a)) \geq 0$$

It remains to prove that the following holds:

$$a = a^* \implies \varphi(a) \in \mathbb{R}$$

By using $1 - h \geq 0$ we can apply the above to $a = 1 - h$ and we obtain:

$$Re(\varphi(1 - h)) \geq 0$$

We conclude that:

$$\begin{aligned} Re(\varphi(1)) &\geq Re(\varphi(h)) \\ &= ||\varphi|| \end{aligned}$$

Thus we have:

$$\varphi(1) = ||\varphi||$$

Summing up, we can assume $h = 1$. Now observe that for any self-adjoint element a, and any $t \in \mathbb{R}$ we have the following inequality:

$$\begin{aligned} |\varphi(1 + ita)|^2 &\leq ||\varphi||^2 \cdot ||1 + ita||^2 \\ &= \varphi(1)^2 ||1 + t^2 a^2|| \\ &\leq \varphi(1)^2 (1 + t^2 ||a||^2) \end{aligned}$$

On the other hand with $\varphi(a) = x + iy$ we have:

$$\begin{aligned} |\varphi(1 + ita)| &= |\varphi(1) - ty + itx| \\ &\geq (\varphi(1) - ty)^2 \end{aligned}$$

We therefore obtain that for any $t \in \mathbb{R}$ we have:

$$\varphi(1)^2 (1 + t^2 ||a||^2) \geq (\varphi(1) - ty)^2$$

Thus we have $y = 0$, and this finishes the proof of our remaining claim.

(3) Consider the linear subspace of A spanned by the element aa^*. We can define here a linear form by the following formula:

$$\varphi(\lambda aa^*) = \lambda ||a||^2$$

This linear form has norm one, and by Hahn-Banach we get a norm one extension to the whole A. The positivity of φ follows from (2).

(4) Let (a_n) be a dense sequence inside A. For any n we can construct as in (3) a positive form satisfying:

$$\varphi_n(a_n a_n^*) = ||a_n||^2$$

We can define then φ in the following way:

$$\varphi = \sum_{n=1}^{\infty} \frac{\varphi_n}{2^n}$$

Let $a \in A$ be a nonzero element. Pick a_n close to a and consider the pair (H, π) associated to the pair (A, φ_n), as in Proposition 7.39. We have then:

$$\begin{aligned} \varphi_n(aa^*) &= ||\pi(a)1|| \\ &\geq ||\pi(a_n)1|| - ||a - a_n|| \\ &= ||a_n|| - ||a - a_n|| \\ &> 0 \end{aligned}$$

Thus we have:

$$\varphi_n(aa^*) > 0$$

It follows that we have $\varphi(aa^*) > 0$, and we are done. □

With these ingredients in hand, we can now state and prove:

Theorem 7.41 (GNS theorem)**.** *Let A be a C^*-algebra.*

(1) *A appears as a closed $*$-subalgebra $A \subset B(H)$, for some Hilbert space H.*
(2) *When A is separable (usually the case), H can be chosen to be separable.*
(3) *When A is finite dimensional, H can be chosen to be finite dimensional.*

Proof. This result, from [87], follows indeed by combining the construction from Proposition 7.39 with the existence result from Theorem 7.40 above. □

The GNS theorem is something powerful and concrete, which perfectly complements the Gelfand theorem, and the resulting noncommutative compact space formalism.

8. Special matrices

We have already seen quite a number of special matrices, such as projections, symmetries, rotations, and other orthogonal and unitary matrices. We have seen as well more complicated examples, such as positive matrices, or matrices with positive entries.

Our purpose here is to discuss a further number of examples of special matrices, such as the circulant ones, the bistochastic ones, and the Hadamard ones. Besides being very useful and present in mathematics, these are quite of interest in quantum physics.

Let us fix $N \in \mathbb{N}$, and consider the Fourier matrix, with $w = e^{2\pi i/N}$:

$$F = (w^{ij})/\sqrt{N}$$

Given a vector $q \in \mathbb{C}^N$, we denote by $Q \in M_N(\mathbb{C})$ the diagonal matrix having q as vector of diagonal entries. That is:

$$Q_{ii} = q_i \quad , \quad \forall i$$

$$Q_{ij} = 0 \quad , \quad \forall i \neq j$$

With these conventions, we have the following result:

Theorem 8.1. *For a complex matrix $H \in M_N(\mathbb{C})$, the following are equivalent:*

(1) *H is circulant, in the sense that*

$$H_{ij} = \xi_{j-i}$$

for a certain vector $\xi \in \mathbb{C}^N$.

(2) *H is Fourier-diagonal, in the sense that*

$$H = FQF^*$$

for a certain diafonal matrix Q.

In addition, the first row vector of FQF^* is given by:

$$\xi = \frac{Fq}{\sqrt{N}}$$

Proof. If $H_{ij} = \xi_{j-i}$ is circulant then $Q = F^*HF$ is diagonal, given by:

$$\begin{aligned} Q_{ij} &= \frac{1}{N}\sum_{kl} w^{jl-ik}\xi_{l-k} \\ &= \delta_{ij}\sum_{r} w^{jr}\xi_r \end{aligned}$$

Also, if $Q = diag(q)$ is diagonal then $H = FQF^*$ is circulant, given by:

$$\begin{aligned} H_{ij} &= \sum_k F_{ik}Q_{kk}\bar{F}_{jk} \\ &= \frac{1}{N}\sum_k w^{(i-j)k}q_k \end{aligned}$$

Observe that this latter formula proves as well the last assertion, namely:

$$\xi = \frac{Fq}{\sqrt{N}}$$

Thus, we have proved the theorem. □

The above result is very useful, and we have many applications.

In relation now with the orthogonal and unitary matrices, we have:

Proposition 8.2. *The various sets of circulant matrices are as follows:*

(1) $M_N(\mathbb{C})^{circ} = \{FQF^*|q \in \mathbb{C}^N\}$.
(2) $U_N^{circ} = \{FQF^*|q \in \mathbb{T}^N\}$.
(3) $O_N^{circ} = \{FQF^*|q \in \mathbb{T}^N, \bar{q}_i = q_{-i}, \forall i\}$.

In addition, the first row vector of FQF^* is given by:

$$\xi = \frac{Fq}{\sqrt{N}}$$

Proof. All this follows from Theorem 8.1, as follows:

(1) This assertion, along with the last one, is Theorem 8.1 itself.

(2) This is clear from (1), because the eigenvalues must be on the unit circle $\mathbb{T}$.

(3) Observe first that for $q \in \mathbb{C}^N$ we have:

$$\overline{Fq} = F\tilde{q}$$

$$\tilde{q}_i = \bar{q}_{-i}$$

Thus $\xi = Fq$ is real if and only if, for any i:

$$\bar{q}_i = q_{-i}$$

Together with (2), this gives the result. □

Once again, the above result is very useful, and we have many applications.

Let us discuss now the bistochastic matrices. Here "bistochastic" means having sum 1, on each row and each column.

Note that, by unitarity, the row stochasticity is equivalent to the column stochasticity, and more precisely, we have:

Proposition 8.3. *For a unitary matrix*

$$U \in U_N$$

the row stochasticity is equivalent to the column stochasticity.

Proof. This follows indeed by unitarity, because if ξ denotes the all-a1 vector, we have the following equivalence:

$$H\xi = \xi \iff H^t\xi = \xi$$

Thus, we obtain the result. □

Quite remarkably, the bistochastic matrices are stable under taking products, and we have the following result:

Theorem 8.4. *We have bistochastic groups*

$$B_N \subset O_N$$

$$C_N \subset U_N$$

consisting of matrices which are bistochastic.

Proof. This is trivial. □

It is possible to show that these coincide with O_{N-1} and U_{N-1}, respectively:

Theorem 8.5. *The groups B_N and C_N, consisting of the bistochastic matrices, are isomorphic to O_{N-1} and U_{N-1}, via a discrete Fourier transform.*

Proof. Let us pick a unitary matrix $F \in U_N$ satisfying the following condition, where ξ is the all-one vector:

$$Fe_0 = \frac{1}{\sqrt{N}}\xi$$

The basic example here is the Fourier matrix, which with $w = e^{2\pi i/N}$ is:

$$F_N = \frac{1}{\sqrt{N}}(w^{ij})$$

We have then:

$$\begin{aligned} & u\xi = \xi \\ \iff \quad & uFe_0 = Fe_0 \\ \iff \quad & F^*uFe_0 = e_0 \\ \iff \quad & F^*uF = diag(1, w) \end{aligned}$$

Thus we have isomorphisms as in the statement, given by:

$$w_{ij} \to (F^*uF)_{ij}$$

But this gives both the assertions. □

Let us discuss now the Hadamard matrices, which are something really beautiful.

The definition here, going back to 19th century work of Sylvester, is as follows:

Definition 8.6. *An Hadamard matrix is a square binary matrix,*

$$H \in M_N(\pm 1)$$

whose rows are pairwise orthogonal, with respect to the scalar product on $\mathbb{R}^N$.

As a first observation, we do not really need real numbers in order to talk about the Hadamard matrices, because the orthogonality condition tells us that, when comparing two rows, the number of matchings should equal the number of mismatchings.

Thus, we can replace if we want the $1, -1$ entries of our matrix by any two symbols, of our choice. Here is an example of an Hadamard matrix, with this convention:

$$\begin{matrix} \heartsuit & \heartsuit & \heartsuit & \heartsuit \\ \heartsuit & \clubsuit & \heartsuit & \clubsuit \\ \heartsuit & \heartsuit & \clubsuit & \clubsuit \\ \heartsuit & \clubsuit & \clubsuit & \heartsuit \end{matrix}$$

However, it is probably better to run away from this, and use real numbers instead, as in Definition 8.6, with the idea in mind of connecting the Hadamard matrices to the foundations of modern mathematics, namely Calculus 1 and Calculus 2.

So, getting back now to the real numbers, here is a first result:

Proposition 8.7. *The set of the* $N \times N$ *Hadamard matrices is*

$$Y_N = M_N(\pm 1) \cap \sqrt{N} O_N$$

where O_N *is the orthogonal group, the intersection being taken inside* $M_N(\mathbb{R})$.

Proof. Let $H \in M_N(\pm 1)$, and consider the rescaled matrix:

$$U = \frac{H}{\sqrt{N}}$$

Since the rows of this rescaled matrix have norm 1, with respect to the usual scalar product on $\mathbb{R}^N$, we conclude that H is Hadamard precisely when U belongs to the orthogonal group O_N:

$$U \in O_N$$

But this is equivalent to:

$$H \in Y_N$$

Thus, we obtain the result. □

As an interesting consequence of the above result, which is not exactly obvious when using the design theory approach, we have the following result:

Proposition 8.8. *Let $H \in M_N(\pm 1)$ be an Hadamard matrix.*

(1) *The columns of H must be pairwise orthogonal.*
(2) *The transpose matrix $H^t \in M_N(\pm 1)$ is Hadamard as well.*

Proof. Since the orthogonal group O_N is stable under transposition, so is the set Y_N constructed in Proposition 8.7, and this gives both the assertions. □

Let us study now the examples.

There are many such matrices, and in order to cut a bit from the complexity, we can use the following notions:

Definition 8.9. *Two Hadamard matrices are called equivalent, and we write $H \sim K$, when it is possible to pass from H to K via the following operations:*

(1) *Permuting the rows, or the columns.*
(2) *Multiplying the rows or columns by -1.*

Also, we say that H is dephased when its first row and column consist of 1 entries.

Observe that we do not include the transposition operation $H \to H^t$ in our list of allowed operations. This is because Proposition 8.8 above, while looking quite elementary, rests however on a deep linear algebra fact, namely that the transpose of an orthogonal matrix is orthogonal as well, and this can produce complications later on.

Observe that, up to the equivalence relation, any Hadamard matrix $H \in M_N(\pm 1)$ can be put in dephased form. Moreover, the dephasing operation is unique, if we use only the operations (2) in Definition 8.9, namely row and column multiplications by -1.

With these notions in hand, we can formulate our first classification result:

Proposition 8.10. *There is only one Hadamard matrix at $N = 2$, namely*

$$W_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

up to the above equivalence relation for such matrices.

Proof. The matrix in the statement W_2, called Walsh matrix, is clearly Hadamard. Conversely, given $H \in M_N(\pm 1)$ Hadamard, we can dephase it, as follows:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \begin{pmatrix} 1 & 1 \\ ac & bd \end{pmatrix} \to \begin{pmatrix} 1 & 1 \\ 1 & abcd \end{pmatrix}$$

Now since the dephasing operation preserves the class of the Hadamard matrices, we must have $abcd = -1$, and so we obtain by dephasing the matrix W_2. □

At $N = 3$ we cannot have examples, due to the orthogonality condition, which forces N to be even. At $N = 4$ now, we have several examples, as for instance:

$$W_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

This matrix is a particular case of the following construction:

Proposition 8.11. *If $H \in M_M(\pm 1)$ and $K \in M_N(\pm 1)$ are Hadamard matrices, then so is their tensor product, constructed in double index notation as follows:*

$$H \otimes K \in M_{MN}(\pm 1)$$

$$(H \otimes K)_{ia,jb} = H_{ij}K_{ab}$$

In particular the Walsh matrices,

$$W_N = W_2^{\otimes n}$$

with $N = 2^n$, are all Hadamard.

Proof. The matrix in the statement $H \otimes K$ has indeed ± 1 entries, and its rows R_{ia} are pairwise orthogonal, as shown by the following computation:

$$\begin{aligned} & < R_{ia}, R_{kc} > \\ = & \sum_{jb} H_{ij}K_{ab} \cdot H_{kj}K_{cb} \\ = & \sum_{j} H_{ij}H_{kj} \sum_{b} K_{ab}K_{cb} \\ = & MN\delta_{ik}\delta_{ac} \end{aligned}$$

As for the second assertion, this follows from this, W_2 being Hadamard. □

Before going further, we should perhaps clarify a bit our tensor product notations.

In order to write $H \in M_N(\pm 1)$ the indices of H must belong to $\{1, \ldots, N\}$, or at least to an ordered set $\{I_1, \ldots, I_N\}$. But with double indices we are indeed in this latter situation, because we can use the lexicographic order on these indices.

To be more precise, by using the lexicographic order on the double indices, we have the following formula:

$$H \otimes K = \begin{pmatrix} H_{11}K & \ldots & H_{1M}K \\ \vdots & & \vdots \\ H_{M1}K & \ldots & H_{MM}K \end{pmatrix}$$

As an example, by tensoring W_2 with itself, we obtain the above matrix W_4.

Getting back now to our classification work, here is the result at $N = 4$:

Proposition 8.12. *There is only one Hadamard matrix at $N = 4$, namely*

$$W_4 = W_2 \otimes W_2$$

up to the standard equivalence relation for such matrices.

Proof. Consider an Hadamard matrix $H \in M_4(\pm 1)$, assumed to be dephased:

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & a & b & c \\ 1 & d & e & f \\ 1 & g & h & i \end{pmatrix}$$

By orthogonality of the first 2 rows we must have $\{a, b, c\} = \{-1, -1, 1\}$, and so by permuting the last 3 columns, we can further assume that our matrix is as follows:

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & m & n & o \\ 1 & p & q & r \end{pmatrix}$$

By orthogonality of the first 2 columns we must have $\{m, p\} = \{-1, 1\}$, and so by permuting the last 2 rows, we can further assume that our matrix is as follows:

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & x & y \\ 1 & -1 & z & t \end{pmatrix}$$

But this gives the result, because from the orthogonality of the rows we obtain:

$$x = y = -1$$

Indeed, with these values of x, y plugged in, from the orthogonality of the columns we obtain:

$$z = -1, t = 1$$

Thus, up to equivalence we have $H = W_4$, as claimed. □

The case $N = 5$ is excluded, because the orthogonality condition forces $N \in 2\mathbb{N}$.

The point now is that the case $N = 6$ is excluded as well, because we have:

Proposition 8.13. *The size of an Hadamard matrix must be*

$$N \in \{2\} \cup 4\mathbb{N}$$

and we have examples at any values $N = 2^n$.

Proof. By permuting the rows and columns or by multiplying them by -1, as to rearrange the first 3 rows, we can always assume that our matrix looks as follows:

$$H=\begin{pmatrix}1\ldots\ldots1 & 1\ldots\ldots1 & 1\ldots\ldots1 & 1\ldots\ldots1\\ 1\ldots\ldots1 & 1\ldots\ldots1 & -1\ldots-1 & -1\ldots-1\\ 1\ldots\ldots1 & -1\ldots-1 & 1\ldots\ldots1 & -1\ldots-1\\ \underbrace{\cdots\cdots\cdots}_{x} & \underbrace{\cdots\cdots\cdots}_{y} & \underbrace{\cdots\cdots\cdots}_{z} & \underbrace{\cdots\cdots\cdots}_{t}\end{pmatrix}$$

Now if we denote by x,y,z,t the sizes of the 4 block columns, as indicated, the orthogonality conditions between the first 3 rows give the following system of equations:

$$\begin{aligned}(1\perp 2)\quad &:\quad x+y=z+t\\ (1\perp 3)\quad &:\quad x+z=y+t\\ (2\perp 3)\quad &:\quad x+t=y+z\end{aligned}$$

The solution of this system is:

$$x=y=z=t$$

We conclude that the size of our matrix, which is $N=x+y+z+t$, must be a multiple of 4, as claimed. □

As a consequence, we are led to the study of the Hamadard matrices at:

$$N=8,12,16,20,24,\ldots$$

This study can be done either abstractly, via various algebraic methods, or with a computer, and this leads to the conclusion that the number of Hadamard matrices of size $N\in 4\mathbb{N}$ grows with N, and this in a rather exponential fashion.

In particular, we are led in this way into the following statement:

Conjecture 8.14 (Hadamard Conjecture (HC))**.** *There is at least one Hadamard matrix*

$$H\in M_N(\pm 1)$$

for any integer $N\in 4\mathbb{N}$.

This conjecture, going back to the 19th century, is probably one of the most beautiful statements in combinatorics, linear algebra, and mathematics in general. Quite remarkably, the numeric verification so far goes up to the number of the beast:

$$\mathfrak{N}=666$$

Our purpose now will be that of gathering some evidence for this conjecture.

At $N=8$ we have the Walsh matrix W_8.

Thus, the next existence problem comes at $N=12$. And here, we can use the following key construction, due to Paley:

Theorem 8.15. *Let $q = p^r$ be an odd prime power, define*

$$\chi : \mathbb{F}_q \to \{-1, 0, 1\}$$

by $\chi(0) = 0$, $\chi(a) = 1$ if $a = b^2$ for some $b \neq 0$, and $\chi(a) = -1$ otherwise, and finally set

$$Q_{ab} = \chi(a - b)$$

We have then constructions of Hadamard matrices, as follows:

(1) *Paley 1: if $q = 3(4)$ we have a matrix of size $N = q + 1$, as follows:*

$$P_N^1 = 1 + \begin{pmatrix} 0 & 1 & \ldots & 1 \\ -1 & & & \\ \vdots & & Q & \\ -1 & & & \end{pmatrix}$$

(2) *Paley 2: if $q = 1(4)$ we have a matrix of size $N = 2q + 2$, as follows:*

$$P_N^2 = \begin{pmatrix} 0 & 1 & \ldots & 1 \\ 1 & & & \\ \vdots & & Q & \\ 1 & & & \end{pmatrix} \quad : \quad 0 \to \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \quad , \quad \pm 1 \to \pm \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

These matrices are skew-symmetric ($H + H^t = 2$), respectively symmetric ($H = H^t$).

Proof. In order to simplify the presentation, we will denote by 1 all the identity matrices, of any size, and by $\mathbb{I}$ all the rectangular all-one matrices, of any size as well.

It is elementary to check that the matrix $Q_{ab} = \chi(a - b)$ has the following properties:

$$QQ^t = q1 - \mathbb{I}$$

$$Q\mathbb{I} = \mathbb{I}Q = 0$$

In addition, we have the following formulae, which are elementary as well, coming from the fact that -1 is a square in $\mathbb{F}_q$ precisely when $q = 1(4)$:

$$q = 1(4) \implies Q = Q^t$$

$$q = 3(4) \implies Q = -Q^t$$

With these observations in hand, the proof goes as follows:

(1) With our conventions for the symbols 1 and $\mathbb{I}$, explained above, the matrix in the statement is as follows:

$$P_N^1 = \begin{pmatrix} 1 & \mathbb{I} \\ -\mathbb{I} & 1 + Q \end{pmatrix}$$

With this formula in hand, the Hadamard matrix condition follows from:

$$\begin{aligned}
& P_N^1(P_N^1)^t \\
= \ & \begin{pmatrix} 1 & \mathbb{I} \\ -\mathbb{I} & 1+Q \end{pmatrix} \begin{pmatrix} 1 & -\mathbb{I} \\ \mathbb{I} & 1-Q \end{pmatrix} \\
= \ & \begin{pmatrix} N & 0 \\ 0 & \mathbb{I}+1-Q^2 \end{pmatrix} \\
= \ & \begin{pmatrix} N & 0 \\ 0 & N \end{pmatrix}
\end{aligned}$$

(2) If we denote by G, F the matrices in the statement, which replace respectively the $0, 1$ entries, then we have the following formula for our matrix:

$$P_N^2 = \begin{pmatrix} 0 & \mathbb{I} \\ \mathbb{I} & Q \end{pmatrix} \otimes F + 1 \otimes G$$

With this formula in hand, the Hadamard matrix condition follows from:

$$\begin{aligned}
& (P_N^2)^2 \\
= \ & \begin{pmatrix} 0 & \mathbb{I} \\ \mathbb{I} & Q \end{pmatrix}^2 \otimes F^2 + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes G^2 + \begin{pmatrix} 0 & \mathbb{I} \\ \mathbb{I} & Q \end{pmatrix} \otimes (FG + GF) \\
= \ & \begin{pmatrix} q & 0 \\ 0 & q \end{pmatrix} \otimes 2 + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes 2 + \begin{pmatrix} 0 & \mathbb{I} \\ \mathbb{I} & Q \end{pmatrix} \otimes 0 \\
= \ & \begin{pmatrix} N & 0 \\ 0 & N \end{pmatrix}
\end{aligned}$$

Finally, the last assertion is clear, from the above formulae relating Q, Q^t. □

These constructions allow us to get well beyond the Walsh matrix level, and we have the following result:

Theorem 8.16. *The HC is verified at least up to $N = 88$, as follows:*

(1) *At $N = 4, 8, 16, 32, 64$ we have Walsh matrices.*
(2) *At $N = 12, 20, 24, 28, 44, 48, 60, 68, 72, 80, 84, 88$ we have Paley 1 matrices.*
(3) *At $N = 36, 52, 76$ we have Paley 2 matrices.*
(4) *At $N = 40, 56$ we have Paley 1 matrices tensored with W_2.*

However, at $N = 92$ these constructions (Walsh, Paley, tensoring) don't work.

Proof. First of all, the numbers in (1-4) are indeed all the multiples of 4, up to 88. As for the various assertions, the proof here goes as follows:

(1) This is clear.

(2) Since $N - 1$ takes the values $q = 11, 19, 23, 27, 43, 47, 59, 67, 71, 79, 83, 87$, all prime powers, we can indeed apply the Paley 1 construction, in all these cases.

(3) Since $N = 4(8)$ here, and $N/2 - 1$ takes the values $q = 17, 25, 37$, all prime powers, we can indeed apply the Paley 2 construction, in these cases.

(4) At $N = 40$ we have indeed $P_{20}^1 \otimes W_2$, and at $N = 56$ we have $P_{28}^1 \otimes W_2$.

Finally, we have $92 - 1 = 7 \times 13$, so the Paley 1 construction does not work, and $92/2 = 46$, so the Paley 2 construction, or tensoring with W_2, does not work either. □

At $N = 92$ the situation is considerably more complicated, and we have:

Theorem 8.17. *Assuming that $A, B, C, D \in M_K(\pm 1)$ are circulant, symmetric, pairwise commute and satisfy*

$$A^2 + B^2 + C^2 + D^2 = 4K$$

the following $4K \times 4K$ matrix

$$H = \begin{pmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{pmatrix}$$

is Hadamard, called of Williamson type. Moreover, such a matrix exists at $K = 23$.

Proof. We use the same method as for the Paley theorem, namely tensor calculus. Consider the following matrices $1, i, j, k \in M_4(0, 1)$, called the quaternion units:

$$1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad , \quad i = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$j = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \quad , \quad k = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

These matrices describe the positions of the A, B, C, D entries in the matrix H from teh statement, and so this matrix can be written as follows:

$$H = A \otimes 1 + B \otimes i + C \otimes j + D \otimes k$$

Assuming now that A, B, C, D are symmetric, we have:

$$\begin{aligned} & HH^t \\ = \ & (A \otimes 1 + B \otimes i + C \otimes j + D \otimes k)(A \otimes 1 - B \otimes i - C \otimes j - D \otimes k) \\ = \ & (A^2 + B^2 + C^2 + D^2) \otimes 1 - ([A, B] - [C, D]) \otimes i \\ & -([A, C] - [B, D]) \otimes j - ([A, D] - [B, C]) \otimes k \end{aligned}$$

Thus, if we further assume that A, B, C, D pairwise commute, and satisfy the condition $A^2 + B^2 + C^2 + D^2 = 4K$, we obtain indeed an Hadamard matrix.

In general, finding such matrices is a difficult task, and this is where Williamson's extra assumption that A, B, C, D should be taken circulant comes from.

Regarding now the $K = 23$ construction, which produces an Hadamard matrix of order $N = 92$, this comes via a computer search. □

Things get even worse at higher values of N, where more and more complicated constructions are needed. The whole subject is quite technical, and, as already mentioned, human knowledge here stops so far at $\mathfrak{N} = 666$.

One potential way of getting away from these questions is that of looking at various special classes of Hadamard matrices.

However, this is not really the case, because passed a few trivialities, the existence of special Hadamard matrices is generally subject to an improvement of the HC, as in the cocyclic case, or to difficult non-existence questions.

Illustrating and quite famous here is the situation in the circulant case. Given a vector $\gamma \in (\pm 1)^N$, one can ask whether the matrix $H \in M_N(\pm 1)$ defined by $H_{ij} = \gamma_{j-i}$ is Hadamard or not. Here is a solution to the problem:

$$K_4 = \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}$$

More generally, any vector $\gamma \in (\pm 1)^4$ satisfying $\sum \gamma_i = \pm 1$ is a solution to the problem.

The following conjecture, going back to the 50s, states that there are no other solutions:

Conjecture 8.18 (Circulant Hadamard Conjecture (CHC))**.** *There is no circulant Hadamard matrix of size $N \times N$, for any $N \neq 4$.*

The fact that such a simple-looking problem is still open might seem quite surprising.

Indeed, if we denote by $S \subset \{1, \ldots, N\}$ the set of positions of the -1 entries of γ, the Hadamard matrix condition is simply, for any $k \neq 0$, taken modulo N:

$$|S \cap (S + k)| = |S| - N/4$$

Thus, the above conjecture simply states that at $N \neq 4$, such a set S cannot exist. Let us record here this latter statement, originally due to Ryser:

Conjecture 8.19 (Ryser Conjecture)**.** *Given an integer $N > 4$, there is no set $S \subset \{1, \ldots, N\}$ satisfying the condition*

$$|S \cap (S + k)| = |S| - N/4$$

for any $k \neq 0$, taken modulo N.

There has been a lot of work on this conjecture. However, as it was the case with the HC, all this leads to complicated combinatorics, design theory, algebra and number theory, and so on, and there is no serious idea here, at least so far.

Let us step now into analytic questions.

The first result here, found in 1893 by Hadamard, about 25 years after Sylvester's 1867 founding paper, and which actually led to such matrices being called Hadamard, is as follows:

Theorem 8.20. *Given a matrix $H \in M_N(\pm 1)$, we have*

$$|\det(H)| \leq N^{N/2}$$

with equality precisely when H is Hadamard.

Proof. We use here the fact that the determinant of a system of N vectors in $\mathbb{R}^N$ is the signed volume of the associated parallelepiped:

$$\det(H_1, \ldots, H_N) = \pm vol < H_1, \ldots, H_N >$$

This is actually the definition of the determinant, in case you have forgotten the basics (!), with the need for the sign coming for having good additivity properties.

In the case where our vectors take their entries in ± 1, we therefore have the following inequality, with equality precisely when our vectors are pairwise orthogonal:

$$\begin{aligned} |\det(H_1, \ldots, H_N)| &\leq ||H_1|| \times \ldots \times ||H_N|| \\ &= (\sqrt{N})^N \end{aligned}$$

Thus, we have obtained the result, straight from the definition of det. □

The above result is quite interesting, philosophically speaking. Let us recall indeed from that the set formed by the $N \times N$ Hadamard matrices is:

$$Y_N = M_N(\pm 1) \cap \sqrt{N} O_N$$

Thus, what we have in Theorem 8.20 is an analytic method for locating Y_N inside $M_N(\pm 1)$.

This suggests doing many geometric and analytic things, as for instance looking at the maximizers of $|\det(H)|$ at values $N \in \mathbb{N}$ which are not multiples of 4. These latter matrices are called "quasi-Hadamard".

From a "dual" point of view, the question of locating Y_N inside $\sqrt{N}O_N$, once again via analytic methods, makes sense as well. The result here is as follows:

Theorem 8.21. *Given a matrix $U \in O_N$ we have*

$$||U||_1 \leq N\sqrt{N}$$

with equality precisely when $H = U/\sqrt{N}$ is Hadamard.

Proof. We have indeed the following estimate, valid for any $U \in O_N$:

$$\begin{aligned} ||U||_1 &= \sum_{ij} |U_{ij}| \\ &\leq N\left(\sum_{ij} |U_{ij}|^2\right)^{1/2} \\ &= N\sqrt{N} \end{aligned}$$

The equality case holds when for any i, j we have:

$$|U_{ij}| = \sqrt{N}$$

But this amounts in saying that $H = U/\sqrt{N}$ must satisfy $H \in M_N(\pm 1)$, and so that H must be Hadamard. □

As a first comment here, the above Cauchy-Schwarz estimate can be improved with a Hölder estimate, the conclusion being that the rescaled Hadamard matrices maximize the p-norm on O_N at any $p \in [1, 2)$, and minimize it at any $p \in (2, \infty]$.

As it was the case with the Hadamard determinant bound, all this suggests doing some further geometry and analysis, this time on the Lie group O_N, notably with a notion of "almost Hadamard matrix" at stake.

We have seen that the Hadamard matrices $H \in M_N(\pm 1)$ are very interesting combinatorial objects. In what follows, we will be interested in their complex versions:

Definition 8.22. *A complex Hadamard matrix is a square complex matrix*

$$H \in M_N(\mathbb{C})$$

whose entries are on the unit circle, $H_{ij} \in \mathbb{T}$, and whose rows are pairwise orthogonal.

Here, and in what follows, the scalar product is the usual one on $\mathbb{C}^N$, taken to be linear in the first variable and antilinear in the second one:

$$< x, y >= \sum_i x_i \bar{y}_i$$

As basic examples of complex Hamadard matrices, we have of course the real Hadamard matrices, $H \in M_N(\pm 1)$. We will see that there are many other examples.

Let us start by extending some basic results from the real case. First, we have:

Proposition 8.23. *The set of the $N\times N$ complex Hadamard matrices is the real algebraic manifold*

$$X_N=M_N(\mathbb{T})\cap\sqrt{N}U_N$$

where U_N is the unitary group, the intersection being taken inside $M_N(\mathbb{C})$.

Proof. Let $H\in M_N(\mathbb{T})$. Then H is Hadamard if and only if its rescaling $U=H/\sqrt{N}$ belongs to the unitary group U_N, and so when $H\in Y_N$, as claimed. □

The above manifold X_N, while appearing by definition as an intersection of smooth manifolds, is very far from being smooth. We will be back to this, later on.

As a basic consequence of the above result, we have:

Proposition 8.24. *Let $H\in M_N(\mathbb{C})$ be an Hadamard matrix.*

(1) *The columns of H must be pairwise orthogonal.*
(2) *The matrices $H^t,\bar{H},H^*\in M_N(\mathbb{C})$ are Hadamard as well.*

Proof. We use the well-known fact that if a matrix is unitary, $U\in U_N$, then so is its complex conjugate $\bar{U}=(\bar{U}_{ij})$, the inversion formulae being as follows:

$$U^*=U^{-1}$$

$$U^t=\bar{U}^{-1}$$

Thus the unitary group U_N is stable under the operations:

$$U\to U^t$$

$$U\to\bar{U}$$

$$U\to U^*$$

It follows that the algebraic manifold X_N constructed in Proposition 8.23 is stable as well under these operations. But this gives all the assertions. □

Let us introduce now the following equivalence notion for the complex Hadamard matrices, taking into account some basic operations which can be performed:

Definition 8.25. *Two complex Hadamard matrices are called equivalent, and we write $H\sim K$, when it is possible to pass from H to K via the following operations:*

(1) *Permuting the rows, or permuting the columns.*
(2) *Multiplying the rows or columns by numbers in $\mathbb{T}$.*

Also, we say that H is dephased when its first row and column consist of 1 entries.

The same remarks as in the real case apply. For instance, we have not taken into account the results in Proposition 8.24 when formulating the above definition, because the operations $H \to H^t, \bar{H}, H^*$ are far more subtle than those in (1,2) above.

At the level of the examples now, we have the following basic construction, which works at any $N \in \mathbb{N}$, in stark contrast with what happens in the real case:

Theorem 8.26. *The Fourier matrix, namely*

$$F_N = (w^{ij})_{ij}$$

with $w = e^{2\pi i/N}$, which in standard matrix form, with indices $i, j = 0, 1, \ldots, N-1$, is as follows,

$$F_N = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & w & w^2 & \ldots & w^{N-1} \\ 1 & w^2 & w^4 & \ldots & w^{2(N-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & w^{N-1} & w^{(2N-1)} & \ldots & w^{(N-1)^2} \end{pmatrix}$$

is a complex Hadamard matrix, in dephased form.

Proof. By using the standard fact that the averages of complex numbers correspond to barycenters, we conclude that the scalar products between the rows of F_N are:

$$\begin{aligned} & < R_a, R_b > \\ = & \sum_j w^{aj} w^{-bj} \\ = & \sum_j w^{(a-b)j} \\ = & N\delta_{ab} \end{aligned}$$

Thus F_N is indeed a complex Hadamard matrix. As for the fact that F_N is dephased, this follows from our convention $i, j = 0, 1, \ldots, N-1$, which is there for this. □

Thus, there is no analogue of the HC in the complex case. We will see later on that the Fourier matrix F_N can be put in circulant form, so there is no analogue of the CHC either, in this setting. This is of course very good news.

As a first classification result now, in the complex case, we have:

Proposition 8.27. *The Fourier matrices F_2, F_3, which are given by*

$$F_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad , \quad F_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & w & w^2 \\ 1 & w^2 & w \end{pmatrix}$$

with $w = e^{2\pi i/3}$ are the only Hadamard matrices at $N = 2, 3$, up to equivalence.

Proof. The proof at $N = 2$ is similar to the proof of Proposition 8.10, from the real case. Indeed, given $H \in M_N(\mathbb{T})$ Hadamard, we can dephase it, as follows:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \begin{pmatrix} 1 & 1 \\ \bar{a}c & \bar{b}d \end{pmatrix} \to \begin{pmatrix} 1 & 1 \\ 1 & a\bar{b}\bar{c}d \end{pmatrix}$$

Now since the dephasing operation preserves the class of the Hadamard matrices, we must have $a\bar{b}\bar{c}d = -1$, and so we obtain by dephasing the matrix F_2.

Regarding now the case $N = 3$, consider an Hadamard matrix $H \in M_3(\mathbb{T})$, assumed to be in dephased form, as follows:

$$H = \begin{pmatrix} 1 & 1 & 1 \\ 1 & x & y \\ 1 & z & t \end{pmatrix}$$

The orthogonality conditions between the rows of this matrix read:

$$(1 \perp 2) \quad : \quad x + y = -1$$

$$(1 \perp 3) \quad : \quad z + t = -1$$

$$(2 \perp 3) \quad : \quad x\bar{z} + y\bar{t} = -1$$

In order to process these conditions, which are all of the same nature, consider an arbitrary equation of the following type:

$$p + q = -1 \quad , \quad p, q \in \mathbb{T}$$

This equation tells us that the triangle having vertices at $1, p, q$ must be equilateral, and so that we must have, with $w = e^{2\pi i/3}$:

$$\{p, q\} = \{w, w^2\}$$

By using this fact, for the first two equations, we conclude that we must have:

$$\{x, y\} = \{w, w^2\}$$

$$\{z, t\} = \{w, w^2\}$$

As for the third equation, this tells us that we must have $x \neq z$.

Thus, our Hadamard matrix H is either the Fourier matrix F_3, or is the matrix obtained from F_3 by permuting the last two columns, and we are done. □

Let us discuss now the classification at $N = 4$.

We have the following version of the tensor product construction, coming from Diţă's paper [76], involving parameters:

Proposition 8.28. *If $H \in M_M(\mathbb{T})$ and $K \in M_N(\mathbb{T})$ are Hadamard, then so are the following two matrices, for any choice of a parameter matrix $Q \in M_{M\times N}(\mathbb{T})$:*

(1) $H \otimes_Q K \in M_{MN}(\mathbb{T})$, *given by* $(H \otimes_Q K)_{ia,jb} = Q_{ib}H_{ij}K_{ab}$.

(2) $H_Q \otimes K \in M_{MN}(\mathbb{T})$, *given by* $(H_Q \otimes K)_{ia,jb} = Q_{ja}H_{ij}K_{ab}$.

These are called right and left Diţă deformations of $H \otimes K$, with parameter Q.

Proof. These results follow from the same computations as in the usual tensor product case, the idea being that the Q parameters will cancel:

(1) The rows R_{ia} of the matrix $H \otimes_Q K$ are indeed pairwise orthogonal, because:

$$\begin{aligned} < R_{ia}, R_{kc} > &= \sum_{jb} Q_{ib}H_{ij}K_{ab} \cdot \bar{Q}_{kb}\bar{H}_{kj}\bar{K}_{cb} \\ &= M\delta_{ik}\sum_{b} K_{ab}\bar{K}_{cb} \\ &= M\delta_{ik} \cdot N\delta_{ac} \\ &= MN\delta_{ik,ac} \end{aligned}$$

(2) The rows L_{ia} of the matrix $H_Q \otimes K$ are orthogonal as well, because:

$$\begin{aligned} < L_{ia}, L_{kc} > &= \sum_{jb} Q_{ja}H_{ij}K_{ab} \cdot \bar{Q}_{jc}\bar{H}_{kj}\bar{K}_{cb} \\ &= N\delta_{ac}\sum_{j} H_{ij}\bar{H}_{kj} \\ &= N\delta_{ac} \cdot M\delta_{ik} \\ &= MN\delta_{ik,ac} \end{aligned}$$

Thus, both the matrices in the statement are Hadamard, as claimed. □

With the above construction in hand, we have the following result:

Theorem 8.29. *The only complex Hadamard matrices at $N = 4$ are, up to the standard equivalence relation, the matrices*

$$F_4^s = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & s & -1 & -s \\ 1 & -s & -1 & s \end{pmatrix}$$

with $s \in \mathbb{T}$, which appear as right Diţă deformations of $W_4 = F_2 \otimes F_2$.

Proof. The matrix F_4^s is indeed Hadamard, appearing from the construction in Proposition 8.28, assuming that the parameter matrix there $Q \in M_2(\mathbb{T})$ is dephased:

$$Q = \begin{pmatrix} 1 & 1 \\ 1 & s \end{pmatrix}$$

Observe also that, conversely, any right Diţă deformation of $W_4 = F_2 \otimes F_2$ is of this form. Indeed, if we consider such a deformation, with general parameter matrix $Q = \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right)$ as above, by dephasing we obtain an equivalence with $F_4^{s'}$, where $s' = ps/qr$:

$$\begin{pmatrix} p & q & p & q \\ p & -q & p & -q \\ r & s & -r & -s \\ r & -s & -r & s \end{pmatrix} \to \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ r/p & s/q & -r/p & -s/q \\ r/p & -s/q & -r/p & s/q \end{pmatrix}$$

$$\to \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & ps/qr & -1 & -ps/qr \\ 1 & -ps/qr & -1 & ps/qr \end{pmatrix}$$

It remains to prove that the matrices F_4^s are non-equivalent, and that any complex Hadamard matrix $H \in M_4(\mathbb{T})$ is equivalent to one of these matrices F_4^s.

But this follows by using the same kind of arguments as in the proof of Proposition 8.12, and from the proof of Proposition 8.27. Indeed, let us first dephase our matrix:

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & a & b & c \\ 1 & d & e & f \\ 1 & g & h & i \end{pmatrix}$$

We use now the fact, coming from plane geometry, that the solutions $x, y, z, t \in \mathbb{T}$ of the equation $x + y + z + t = 0$ are given by $\{x, y, z, t\} = \{p, q, -p, -q\}$, with $p, q \in \mathbb{T}$.

In our case, we have $1 + a + d + g = 0$, and so up to a permutation of the last 3 rows, our matrix must look at follows, for a certain $s \in \mathbb{T}$:

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & b & c \\ 1 & s & e & f \\ 1 & -s & h & i \end{pmatrix}$$

In the case $s = \pm 1$ we can permute the middle two columns, then repeat the same reasoning, and we end up with the matrix in the statement.

In the case $s \neq \pm 1$ we have $1 + s + e + f = 0$, and so $-1 \in \{e, f\}$. Up to a permutation of the last columns, we can assume $e = -1$, and our matrix becomes:

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & b & c \\ 1 & s & -1 & -s \\ 1 & -s & h & i \end{pmatrix}$$

Similarly, from $1-s+h+i=0$ we deduce that $-1\in\{h,i\}$. In the case $h=-1$ our matrix must look as follows, and we are led to the matrix in the statement:

$$H=\begin{pmatrix}1&1&1&1\\1&-1&b&c\\1&s&-1&-s\\1&-s&-1&i\end{pmatrix}$$

As for the remaining case $i=-1$, here our matrix must look as follows:

$$H=\begin{pmatrix}1&1&1&1\\1&-1&b&c\\1&s&-1&-s\\1&-s&h&-1\end{pmatrix}$$

We obtain from the last column $c=s$, then from the second row $b=-s$, then from the third column $h=s$, and so our matrix must be as follows:

$$H=\begin{pmatrix}1&1&1&1\\1&-1&-s&s\\1&s&-1&-s\\1&-s&s&-1\end{pmatrix}$$

But, in order for the second and third row to be orthogonal, we must have $s\in\mathbb{R}$, and so $s=\pm1$, which contradicts our above assumption $s\neq\pm1$.

Thus, we are done with the proof of the main assertion. As for the fact that the matrices in the statement are indeed not equivalent, this is standard as well. See [169]. □

At $N=5$ now, the situation is considerably more complicated, with F_5 being the only known example, but with the proof of its uniqueness being highly nontrivial.

We discuss now yet another type of special complex Hadamard matrices, namely the circulant ones. There has been a lot of work here, starting with the Circulant Hadamard Conjecture (CHC) in the real case, and with many results in the complex case as well. We will present here the main techniques in dealing with such matrices.

It is convenient to introduce the circulant matrices as follows:

Definition 8.30. *A complex matrix $H\in M_N(\mathbb{C})$ is called circulant when we have*

$$H_{ij}=\gamma_{j-i}$$

for some $\gamma\in\mathbb{C}^N$, with the matrix indices $i,j\in\{0,1,\ldots,N-1\}$ taken modulo N.

Here the index convention is quite standard, as for the Fourier matrices F_N, and with this coming from Fourier analysis considerations, that we will get into later on.

Here is a basic, and very fundamental example of a circulant Hadamard matrix, which in addition has real entries, and is symmetric:

$$K_4 = \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}$$

According to the CHC, explained before, this matrix is, up to equivalence, the only circulant Hadamard matrix $H \in M_N(\pm 1)$, regardless of the value of $N \in \mathbb{N}$.

Our first purpose will be that of showing that the CHC dissapears in the complex case, where we have examples at any $N \in \mathbb{N}$.

As a first result here, we have:

Proposition 8.31. *The following are circulant and symmetric Hadamard matrices,*

$$F_2' = \begin{pmatrix} i & 1 \\ 1 & i \end{pmatrix}$$

$$F_3' = \begin{pmatrix} w & 1 & 1 \\ 1 & w & 1 \\ 1 & 1 & w \end{pmatrix}$$

$$F_4'' = \begin{pmatrix} -1 & \nu & 1 & \nu \\ \nu & -1 & \nu & 1 \\ 1 & \nu & -1 & \nu \\ \nu & 1 & \nu & -1 \end{pmatrix}$$

where $w = e^{2\pi i/3}, \nu = e^{\pi i/4}$, equivalent to the Fourier matrices F_2, F_3, F_4.

Proof. The orthogonality between rows being clear, we have here complex Hadamard matrices. The fact that we have an equivalence $F_2 \sim F_2'$ follows from:

$$\begin{aligned} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} &\sim \begin{pmatrix} i & i \\ 1 & -1 \end{pmatrix} \\ &\sim \begin{pmatrix} i & 1 \\ 1 & i \end{pmatrix} \end{aligned}$$

At $N=3$ now, the equivalence $F_3\sim F_3'$ can be constructed as follows:

$$\begin{pmatrix}1&1&1\\1&w&w^2\\1&w^2&w\end{pmatrix}\sim\begin{pmatrix}1&1&w\\1&w&1\\w&1&1\end{pmatrix}\sim\begin{pmatrix}w&1&1\\1&w&1\\1&1&w\end{pmatrix}$$

As for the case $N=4$, here the equivalence $F_4\sim F_4''$ can be constructed as follows, where we use the logarithmic notation $[k]_s=e^{2\pi ki/s}$, with respect to $s=8$:

$$\begin{bmatrix}0&0&0&0\\0&2&4&6\\0&4&0&4\\0&6&4&2\end{bmatrix}_8\sim\begin{bmatrix}0&1&4&1\\1&4&1&0\\4&1&0&1\\1&0&1&4\end{bmatrix}_8\sim\begin{bmatrix}4&1&0&1\\1&4&1&0\\0&1&4&1\\1&0&1&4\end{bmatrix}_8$$

We will explain later the reasons for denoting this matrix F_4'', instead of F_4'. □

Getting back now to the real circulant matrix K_4, this is equivalent to the Fourier matrix $F_G=F_2\otimes F_2$ of the Klein group $G=\mathbb{Z}_2\times\mathbb{Z}_2$, as shown by:

$$\begin{pmatrix}-1&1&1&1\\1&-1&1&1\\1&1&-1&1\\1&1&1&-1\end{pmatrix}\sim\begin{pmatrix}1&1&1&-1\\1&-1&1&1\\1&1&-1&1\\-1&1&1&1\end{pmatrix}\sim\begin{pmatrix}1&1&1&1\\1&-1&1&-1\\1&1&-1&-1\\1&-1&-1&1\end{pmatrix}$$

Thus, many interesting examples of complex Hadamard matrices can be put in circulant form.

In fact, we have the following construction of circulant and symmetric Hadamard matrices at $N=4$, which involves an extra parameter $q\in\mathbb{T}$:

Proposition 8.32. *The following circulant and symmetric matrix is Hadamard,*

$$K_4^q = \begin{pmatrix} -1 & q & 1 & q \\ q & -1 & q & 1 \\ 1 & q & -1 & q \\ q & 1 & q & -1 \end{pmatrix}$$

for any $q \in \mathbb{T}$. At $q = 1, e^{\pi i/4}$ recover respectively the matrices K_4, F_4''.

Proof. The rows of the above matrix are pairwise orthogonal for any $q \in \mathbb{C}$, and so at $q \in \mathbb{T}$ we obtain a complex Hadamard matrix. The last assertion is clear. □

Let us prove now that any Fourier matrix F_N can be put in circulant and symmetric form. We use Björck's cyclic root formalism, which is as follows:

Theorem 8.33. *Assume that $H \in M_N(\mathbb{T})$ is circulant, $H_{ij} = \gamma_{j-i}$. Then H is Hadamard if and only if the vector $(z_0, z_1, \ldots, z_{N-1})$ given by $z_i = \gamma_i/\gamma_{i-1}$ satisfies:*

$$\begin{aligned} z_0 + z_1 + \ldots + z_{N-1} &= 0 \\ z_0 z_1 + z_1 z_2 + \ldots + z_{N-1} z_0 &= 0 \\ &\ldots \\ z_0 z_1 \ldots z_{N-2} + \ldots + z_{N-1} z_0 \ldots z_{N-3} &= 0 \\ z_0 z_1 \ldots z_{N-1} &= 1 \end{aligned}$$

If so is the case, we say that $z = (z_0, \ldots, z_{N-1})$ is a cyclic N-root.

Proof. This follows from a direct computation, the idea being that, with $H_{ij} = \gamma_{j-i}$ as above, the orthogonality conditions between the rows are best written in terms of the variables $z_i = \gamma_i/\gamma_{i-1}$, and correspond to the equations in the statement. □

Observe that, up to a global multiplication by a scalar $w \in \mathbb{T}$, the first row vector $\gamma = (\gamma_0, \ldots, \gamma_{N-1})$ of the matrix $H \in M_N(\mathbb{T})$ constructed above is as follows:

$$\gamma = (z_0, z_0 z_1, z_0 z_1 z_2, \ldots\ldots, z_0 z_1 \ldots z_{N-1})$$

Now back to the Fourier matrices, we have the following result:

Theorem 8.34. *Given $N \in \mathbb{N}$, set $\nu = e^{\pi i/N}$ and $q = \nu^{N-1}, w = \nu^2$. Then*

$$(q, qw, qw^2, \ldots, qw^{N-1})$$

is a cyclic N-root, and the corresponding complex Hadamard matrix F_N' is circulant and symmetric, and equivalent to the Fourier matrix F_N.

Proof. Given $q, w \in \mathbb{T}$, let us find out when $(q, qw, qw^2, \ldots, qw^{N-1})$ is a cyclic root:

(1) In order for the $= 0$ equations in Theorem 8.33 to be satisfied, the value of q is irrelevant, and w must be a primitive N-root of unity.

(2) As for the $= 1$ equation in Theorem 8.33, this states in our case that we must have $q^N w^{\frac{N(N-1)}{2}} = 1$, and so that we must have $q^N = (-1)^{N-1}$.

We conclude that with the values of $q, w \in \mathbb{T}$ in the statement, we have indeed a cyclic N-root. Now construct $H_{ij} = \gamma_{j-i}$ as in Theorem 8.33. We have:

$$\begin{aligned}
& \gamma_k = \gamma_{-k}, \forall k \\
\iff \quad & q^{k+1} w^{\frac{k(k+1)}{2}} = q^{-k+1} w^{\frac{k(k-1)}{2}}, \forall k \\
\iff \quad & q^{2k} w^k = 1, \forall k \\
\iff \quad & q^2 = w^{-1}
\end{aligned}$$

But this latter condition holds indeed, because we have:

$$\begin{aligned}
q^2 &= \nu^{2N-2} \\
&= \nu^{-2} \\
&= w^{-1}
\end{aligned}$$

We conclude that our circulant matrix H is symmetric as well, as claimed.

It remains to construct an equivalence $H \sim F_N$. In order to do this, observe that, due to our conventions $q = \nu^{N-1}, w = \nu^2$, the first row vector of H is given by:

$$\begin{aligned}
\gamma_k &= q^{k+1} w^{\frac{k(k+1)}{2}} \\
&= \nu^{(N-1)(k+1)} \nu^{k(k+1)} \\
&= \nu^{(N+k-1)(k+1)}
\end{aligned}$$

Thus, the entries of H are given by the following formula:

$$\begin{aligned}
H_{-i,j} &= H_{0,i+j} \\
&= \nu^{(N+i+j-1)(i+j+1)} \\
&= \nu^{i^2+j^2+2ij+Ni+Nj+N-1} \\
&= \nu^{N-1} \cdot \nu^{i^2+Ni} \cdot \nu^{j^2+Nj} \cdot \nu^{2ij}
\end{aligned}$$

With this formula in hand, we can now finish. Indeed, the matrix $H = (H_{ij})$ is equivalent to the matrix $H' = (H_{-i,j})$. Now regarding H', observe that in the above formula, the factors ν^{N-1}, ν^{i^2+Ni}, ν^{j^2+Nj} correspond respectively to a global multiplication by a scalar, and to row and column multiplications by scalars. Thus H' is equivalent to the matrix H'' obtained by deleting these factors.

But this latter matrix, given by $H''_{ij} = \nu^{2ij}$ with $\nu = e^{\pi i/N}$, is precisely the Fourier matrix F_N, and we are done. □

Thus we have no analogues of HC and CHC. We have however some interesting questions, of geometric nature, for instance concerning the notion of defect.

9. Group theory

We have seen so far the basics of linear algebra, with the conclusion that the theory is very useful, and quickly becomes non-trivial.

We have seen as well some abstract applications, to questions in analysis, and combinatorics, and with some results on the infinite dimensional case as well. All this is of course very useful in physics.

In the remainder of this book, or rather second half of it, to be more precise, we discuss a related topic, the matrix groups.

The theory here is once again very useful in connection with various questions in physics, the general idea here being that any physical system S has a group of symmetries $G(S)$, whose study can lead to interesting conclusions about S.

Let us begin with some abstract aspects. An abstract group G is something very simple, namely a set, with a composition operation:

$$(g, h) \to gh$$

This composition operation must of course satisfy what we should expect from a "multiplication", and the precise definition of the groups is as follows:

Definition 9.1. *A group is a set G endowed with a multiplication operation $(g, h) \to gh$ having the following properties:*

(1) *Associativity:* $(gh)k = g(hk)$, $\forall g, h, k \in G$.
(2) *Unit:* $\exists 1 \in G$ *such that* $g1 = 1g = g$, $\forall g \in G$.
(3) *Inverses:* $\forall g \in G$, $\exists g^{-1} \in G$ *such that* $gg^{-1} = g^{-1}g = 1$.

When the multiplication is commutative, $gh = hg$, $\forall g, h \in G$, we call G abelian, and usually denote its multiplication, unit and inverse operation as follows:

$$(g, h) \to g + h$$

$$0 \in G$$

$$g \to -g$$

However, this is not a general rule, and rather the converse is true, in the sense that if a group is denoted as above, this means that the group must be abelian.

There are many examples of abelian and non-abelian groups, with typically the various sets of numbers being abelian groups, and the sets of matrices being non-abelian groups. Once again, this is of course not a general rule.

Here are some basic examples and counterexamples:

Proposition 9.2. *We have the following groups, and non-groups:*

(1) $(\mathbb{Z}, +)$ *is a group.*
(2) $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ *are groups as well.*
(3) $(\mathbb{N}, +)$ *is not a group.*
(4) $(\mathbb{Q}^*, \cdot)$ *is a group.*
(5) $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ *are groups as well.*
(6) $(\mathbb{N}^*, \cdot)$, $(\mathbb{Z}^*, \cdot)$ *are not groups.*

Proof. All this is clear from definitions:

(1) The axioms are indeed satisfied.

(2) Once again, the axioms are satisfied.

(3) Here we do not have inverses, so we do not have a group.

(4) The axioms are satisfied.

(5) Once again, the axioms are satisfied.

(6) Here we do not have inverses, so we do not have a groups. □

We have as well other types of "numbers", such as those taken modulo p, with p being arbitrary, or prime. We will discuss this later on.

We have as well many interesting groups coming from linear algebra:

Theorem 9.3. *We have the following groups:*

(1) $(\mathbb{R}^N, +)$ *and* $(\mathbb{C}^N, +)$.
(2) $(M_N(\mathbb{R}), +)$ *and* $(M_N(\mathbb{C}), +)$.
(3) $(GL_N(\mathbb{R}), \cdot)$ *and* $(GL_N(\mathbb{C}), \cdot)$, *the invertible matrices.*
(4) $(SL_N(\mathbb{R}), \cdot)$ *and* $(SL_N(\mathbb{C}), \cdot)$, *with* S *standing for "special", meaning* $\det = 1$.
(5) $(O_N, \cdot)$ *and* $(U_N, \cdot)$, *the orthogonal and unitary matrices.*
(6) $(SO_N, \cdot)$ *and* $(SU_N, \cdot)$, *with* S *standing as above for* $\det = 1$.

Proof. All this is clear from definitions, and from our linear algebra knowledge:

(1) The axioms are indeed clearly satisfied.

(2) Once again, the axioms are clearly satisfied.

(3) This is once again clear from definitions, and is best seen by using the associated linear maps. Indeed, the composition of two invertible maps is invertible.

(4) Here we have subgroups of the groups in (3), because $\det(AB) = \det A \det B$, and so the matrices satisfying $\det A = 1$ are stable under multiplication.

(5) This is clear too from definitions, and is best best seen by using the associated linear maps. Indeed, the composition of two isometries is an isometry.

(6) The sets of matrices in the statement are obtained by intersecting the groups in (4) and (5), and so they are groups indeed. □

Summarizing, the notion of group is something extremely wide.

In order to have some theory going, we obviously have to impose to some conditions on the groups that we consider, and this because in general, the theory is too wide.

With this idea in mind, let us work out some examples, in the finite case.

The simplest possible finite group is the cyclic group $\mathbb{Z}_N$. There are many ways of picturing $\mathbb{Z}_N$, both additive and multiplicative:

Definition 9.4. *The cyclic group $\mathbb{Z}_N$ can be defined as follows:*

(1) *As the additive group of remainders modulo N.*
(2) *As the multiplicative group of the N-th roots of the unity.*

Note that the definitions are equivalent, because with $w = e^{2\pi i/N}$ we have:

$$w^a w^b = w^{a+b}$$

In other words, we have here a group isomorphism.

Yet another interesting example, more advanced this time, is the dihedral group D_N. This is the symmetry group of the regular N-gon. Here are some basic examples:

$N = 2$. Here the N-gon is just a segment, and its symmetries are the identity id and the obvious symmetry τ. Thus $D_2 = \{id, \tau\}$, and in group theory terms, $D_2 = \mathbb{Z}_2$.

$N = 3$. Here the N-gon is an equilateral triangle, and the symmetries are the $3! = 6$ possible permutations of the vertices. Thus we have $D_3 = S_3$.

$N = 4$. Here the N-gon is a square, and as symmetries we have 4 rotations, of angles $0°, 90°, 180°, 270°$, as well as 4 symmetries, with respect to the 4 symmetry axes.

In general, we have the following result:

Proposition 9.5. *The dihedral group D_N has $2N$ elements, namely:*

(1) *N symmetries.*
(2) *N rotations.*

Proof. This is clear, indeed. To be more precise, D_N consists of:

(1) The N symmetries with respect to the N possible symmetry axes, which are the N medians of the N-gon when N is odd, and are the $N/2$ diagonals plus the $N/2$ lines connecting the midpoints of opposite edges, when N is even.

(2) The N rotations, of angles $2k\pi/N$ with $k = 0, 1, \ldots, N-1$. □

It is possible to go beyond this, with a crossed product decomposition:

Theorem 9.6. *We have a crossed product decomposition of type*

$$D_N = \mathbb{Z}_N \rtimes \mathbb{Z}_2$$

with the group on the right being $\mathbb{Z}_N \times \mathbb{Z}_2$, with twisted multiplication.

Proof. This follows by using Proposition 9.5. To be more precise, the subgroup formed by the N rotations is obviously cyclic, and so we have an embedding as follows:

$$\mathbb{Z}_N \subset D_N$$

Thus, by using Proposition 9.5, at the level of the cardinalities, we have:

$$|D_N| = |\mathbb{Z}_N \times \mathbb{Z}_2|$$

Now observe that we cannot have $D_N = \mathbb{Z}_N \times \mathbb{Z}_2$, simply because $\mathbb{Z}_N \times \mathbb{Z}_2$ is abelian, and D_N is not. However, we can suitably twist the multiplication on $\mathbb{Z}_N \times \mathbb{Z}_2$, as to obtain D_N, and this leads to the conclusion in the statement. □

As a third basic example, we have the symmetric group S_N. This is a group that we already met, when talking about the determinant:

Theorem 9.7. *The permutations of $\{1, \ldots, N\}$ form a group, denoted S_N, and called symmetric group. This group has $N!$ elements. The signature map*

$$\varepsilon : S_N \to \mathbb{Z}_2$$

can be regarded as a group morphism, with values in $\mathbb{Z}_2 = \{\pm 1\}$.

Proof. These are things that we already know, from section 2 above. To be more precise, the group property is clear, and the formula $|S_N| = N!$ is clear as well.

To be more precise, in order to construct an element $\sigma \in S_N$, we have:

– N choices for the value of $\sigma(N)$.

– $(N-1)$ choices for the value of $\sigma(N-1)$.

– $(N-2)$ choices for the value of $\sigma(N-2)$.

⋮

⋮

– and so on, up to 1 choice for the value of $\sigma(1)$.

Summing up, the number of choices for a permutation $\sigma \in S_N$ is, as desired:

$$N(N-1)(N-2)\ldots\ldots 1 = N!$$

Regarding now the last assertion, recall the following formula for the signatures, that we know from section 2:

$$\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$$

But this gives the result. □

At an even more advanced level now, we have the hyperoctahedral group H_N.

This is by definition the group of symmetries of the N-cube.

We can count $|H_N|$, as follows:

Proposition 9.8. *We have the cardinality formula*

$$|H_N| = 2^N N!$$

coming from the fact that H_N is the symmetry group of the coordinate axes of $\mathbb{R}^N$.

Proof. Consider the standard cube in $\mathbb{R}^N$, centered at 0, and having as vertices the points having coordinates ± 1. With this picture in hand, it is clear that the symmetries of the cube coincide with the symmetries of the N coordinate axes of $\mathbb{R}^N$.

In order to count now these latter symmetries, observe first that we have $N!$ permutations of these N coordinate axes.

But each of these permutations of the coordinate axes $\sigma \in S_N$ can be further "decorated" by a sign vector $\varepsilon \in \{\pm 1\}^N$, consisting of the possible ± 1 flips which can be applied to each coordinate axis, at the arrival.

Thus, we have the following formula:

$$\begin{aligned} |H_N| &= |S_N| \cdot |\mathbb{Z}_2^N| \\ &= N! \cdot 2^N \end{aligned}$$

Thus, we are led to the conclusions in the statement. □

As in the dihedral group case, it is possible to go beyond this, with a crossed product decomposition, of quite special type, called wreath product decomposition:

Theorem 9.9. *We have a crossed product decomposition of type*

$$H_N = \mathbb{Z}_2 \wr S_N$$

with the group on the right being $S_N \times \mathbb{Z}_2^N$, with twisted multiplication.

Proof. This follows indeed by using Proposition 9.8 above. To be more precise, we know from there that at the level of cardinalities, we have:

$$|H_N| = |S_N \times \mathbb{Z}_2^N|$$

By proceeding now as in the proof of Theorem 9.6 above, we can deduce from this that we have a crossed product decomposition, as follows:

$$H_N = S_N \rtimes \mathbb{Z}_2^N$$

But this means exactly that we have:

$$H_N = \mathbb{Z}_2 \wr S_N$$

Thus, we are led to the conclusion in the statement. □

Summarizing, we have so far many interesting examples of finite groups, and as a sequence of main examples, we have the following groups:

$$\mathbb{Z}_N \subset D_N \subset S_N \subset H_N$$

We will be back to these fundamental finite groups later on, on several occasions, with further results on them.

We will be mostly interested in what follows in the groups of matrices, and more specifically in the compact groups of matrices.

In practice, this leads us to the closed subgroups of U_N:

Proposition 9.10. *Any closed subgroup of U_N is a compact group of matrices. Such a group is a set of matrices $G \subset U_N$ satisfying:*

(1) $U, V \in G \implies UV \in G$.
(2) $1 \in G$.
(3) $U \in G \implies U^{-1} \in G$.

Proof. This is clear, because closed inside compact means compact. □

It is possible to get beyond this, first with a result stating that any closed subgroup $G \subset U_N$ is a smooth manifold, and so is a compact Lie group, having a Lie algebra and so on. Moreover, and importantly, a converse of this fact is known to hold, in the sense that any compact Lie group appears as a closed subgroup $G \subset U_N$ of a unitary group.

However, all this is quite advanced, and we will not need it, in what follows.

Let us go back now to the finite groups. These appear as well as groups of matrices. Indeed, we usually have $G_N \subset S_N \subset O_N$, via permutation matrices:

Proposition 9.11. *We have a group embedding as follows, obtained by regarding S_N as the permutation group of the N coordinate axes of $\mathbb{R}^N$,*

$$S_N \subset O_N$$

and which makes $\sigma \in S_N$ correspond to the matrix having 1 on row i and column $\sigma(i)$, for any i, and having 0 entries elsewhere.

Proof. The first assertion is clear, because the permutations of the N coordinate axes of $\mathbb{R}^N$ are isometries, and so correspond to matrices in O_N.

Regarding now the explicit formula of this embedding, we have by definition:

$$\sigma(e_j) = e_{\sigma(j)}$$

Thus, the permutation matrix corresponding to σ is given by:

$$\sigma_{ij} = \begin{cases} 1 & \text{if } \sigma(j) = i \\ 0 & \text{otherwise} \end{cases}$$

Thus, we are led to the formula in the statement. □

In fact, in general, consider a finite group G, having order:

$$N = |G|$$

We have the Cayley theorem, which gives an embedding as follows:

$$G \subset S_N \subset U_N$$

Thus, any finite group is a group of unitary matrices, and our formalism here is quite general.

As already mentioned, there are as well abstract results in this sense:

Theorem 9.12. *Any finite group is a matrix group.*

Proof. This follows from the Cayley theorem, as explained above.

Assume indeed that we have a finite group G, having order $N = |G|$.

Our claim is that we have an embedding as follows:

$$G \subset S_N$$

$$g \to (h \to gh)$$

Indeed, we have a group morphism, whose kernel is $\{1\}$, as desired. □

In relation with the "basic" groups, we have:

Theorem 9.13. *Finite groups of matrices:*

(1) $\mathbb{Z}_N$, *the cyclic permutation matrices.*
(2) D_N, *the dihedral matrices.*
(3) S_N, *the permutation matrices.*
(4) H_N, *the signed permutation matrices.*

Proof. This is clear, indeed:

(1) The cyclic permutation matrices are as follows:

$$U = \begin{pmatrix} \ldots & \ldots & 1 & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & 1 & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & 1 \\ 1 & \ldots & \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & 1 & \ldots & \ldots & \ldots \end{pmatrix}$$

(2) The dihedral matrices form a group, indeed.

(3) These are just the permutation matrices.

(4) These are just the signed permutation matrices. □

We can extend our series of basic finite groups, in the following way:

Definition 9.14. *The complex reflection group $H_N^s \subset U_N$, depending on parameters*

$$N \in \mathbb{N} \quad , \quad s \in \mathbb{N} \cup \{\infty\}$$

is the group of permutation-type matrices with s-th roots of unity as entries,

$$H_N^s = M_N(\mathbb{Z}_s \cup \{0\}) \cap U_N$$

with the convention $\mathbb{Z}_\infty = \mathbb{T}$, at $s = \infty$.

Observe that at $s = 1, 2$ we obtain the following groups:

$$H_N^1 = S_N$$

$$H_N^2 = H_N$$

Another important particular case is $s = \infty$, where we obtain a group which is actually not finite, denoted as follows:

$$K_N \subset U_N$$

In general, in analogy with what we know about H_N, we have the following decomposition result, with the usual convention $\mathbb{Z}_\infty = \mathbb{T}$ at $s = \infty$:

$$H_N^s = \mathbb{Z}_s \rtimes S_N$$

We will be back later to finite groups, with more examples.

Let us discuss now in detail the structure of the finite abelian groups:

Theorem 9.15. *The finite abelian groups are of the form:*

$$G = \mathbb{Z}_{N_1} \times \ldots \times \mathbb{Z}_{N_k}$$

That is, they are the firect products of cyclic groups.

Proof. This is something quite standard. □

We have as well the following result:

Theorem 9.16. *Given a finite abelian group, the set of characters*

$$\widehat{G} = \{\chi : G \to \mathbb{T}\}$$

is a finite abelian group as well, isomorphic to it.

Proof. This is something quite standard, as well. □

As an application, we have:

Theorem 9.17. *Discrete Fourier transforms.*

Proof. This is something quite standard, which follows from the above results. □

There is a relation here with the complex Hadamard matrices, from the previous section. To be more precise, we have the following construction:

Theorem 9.18. *Given a finite abelian group G, with dual group*

$$\widehat{G} = \{\chi : G \to \mathbb{T}\}$$

consider the Fourier coupling $\mathcal{F}_G : G \times \widehat{G} \to \mathbb{T}$, given by $(i, \chi) \to \chi(i)$.

(1) *Via the standard isomorphism $G \simeq \widehat{G}$, this Fourier coupling can be regarded as a square matrix, $F_G \in M_G(\mathbb{T})$, which is a complex Hadamard matrix.*

(2) *In the case of the cyclic group $G = \mathbb{Z}_N$ we obtain in this way, via the standard identification $\mathbb{Z}_N = \{1, \ldots, N\}$, the Fourier matrix F_N.*

(3) *In general, when using a decomposition $G = \mathbb{Z}_{N_1} \times \ldots \times \mathbb{Z}_{N_k}$, the corresponding Fourier matrix is given by $F_G = F_{N_1} \otimes \ldots \otimes F_{N_k}$.*

Proof. This follows indeed from some basic facts from group theory:

(1) With the identification $G \simeq \widehat{G}$ made our matrix is given by $(F_G)_{i\chi} = \chi(i)$, and the scalar products between the rows are computed as follows:

$$\begin{aligned} < R_i, R_j > &= \sum_\chi \chi(i)\overline{\chi(j)} \\ &= \sum_\chi \chi(i-j) \\ &= |G| \cdot \delta_{ij} \end{aligned}$$

Thus, we obtain indeed a complex Hadamard matrix.

(2) This follows from the well-known and elementary fact that, via the identifications $\mathbb{Z}_N = \widehat{\mathbb{Z}_N} = \{1, \ldots, N\}$, the Fourier coupling here is $(i, j) \to w^{ij}$, with $w = e^{2\pi i/N}$.

(3) We use here the following well-known formula, for the duals of products:

$$\widehat{H \times K} = \widehat{H} \times \widehat{K}$$

At the level of the corresponding Fourier couplings, we obtain from this:

$$F_{H \times K} = F_H \otimes F_K$$

Now by decomposing G into cyclic groups, as in the statement, and by using (2) for the cyclic components, we obtain the formula in the statement. □

As a first application of the above result, we have:

Proposition 9.19. *The Walsh matrix, W_N with $N = 2^n$, which is given by*

$$W_N = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{\otimes n}$$

is the Fourier matrix of the finite abelian group $K_N = \mathbb{Z}_2^n$.

Proof. We know that the first Walsh matrix is a Fourier matrix, as follows:

$$W_2 = F_2 = F_{K_2}$$

Now by taking tensor powers we obtain from this that we have, for any $N = 2^n$:

$$\begin{aligned} W_N &= W_2^{\otimes n} \\ &= F_{K_2}^{\otimes n} \\ &= F_{K_2^n} \\ &= F_{K_N} \end{aligned}$$

Thus, we are led to the conclusion in the statement. □

10. Matrix groups

In this section we focus on the matrix groups, and we discuss a number of more specialized aspects. Let us first discuss the continuous case.

As basic examples here, we have the orthogonal group O_N, and the unitary group U_N. These are the groups of rotations in $\mathbb{R}^N$, $\mathbb{C}^N$:

Theorem 10.1. *We have the following results:*

(1) *The rotations of $\mathbb{R}^N$ form the orthogonal group O_N.*
(2) *The rotations of $\mathbb{C}^N$ form the unitary group U_N.*

In addition, we can restrict the attention to the corresponding spheres.

Proof. All this is clear, indeed. □

We have as well the groups SO_N and SU_N, constructed using the determinant.

These consist of the rotations which preserve the orientation:

Theorem 10.2. *The following are groups,*

$$SO_N = \{U \in O_N | \det U = 1\}$$

$$SU_N = \{U \in U_N | \det U = 1\}$$

consisting of the rotations which preserve the orientation.

Proof. All this is clear, indeed. □

It is possible to construct some further groups of this type, once again by using the determinant, but via a more general condition, as follows:

$$(\det U)^s = 1$$

We will be back to these groups, which are quite specialized, later on.

At a more specialized level as well, but not very far from basic, we have the groups B_N and C_N, consisting of the orthogonal and unitary bistochastic matrices.

Here "bistochastic" means having sum 1, on each row and each column. Note that, by unitarity, the row stochasticity is equivalent to the column stochasticity.

It is possible to show that these coincide with O_{N-1} and U_{N-1}, respectively:

Theorem 10.3. *The groups B_N and C_N, consisting of the bistochastic matrices, have the following properties:*

(1) *They are groups, indeed.*
(2) *They are isomorphic to O_{N-1} and U_{N-1}.*

Proof. All this is clear:

(1) This is clear, indeed.

(2) Let us pick $F \in U_N$ satisfying the following condition, where ξ is the all-one vector:

$$Fe_0 = \frac{1}{\sqrt{N}}\xi$$

The basic example here is the Fourier matrix, which with $w = e^{2\pi i/N}$ is:

$$F_N = \frac{1}{\sqrt{N}}(w^{ij})$$

We have then:

$$\begin{aligned} & u\xi = \xi \\ \iff \quad & uFe_0 = Fe_0 \\ \iff \quad & F^*uFe_0 = e_0 \\ \iff \quad & F^*uF = diag(1, w) \end{aligned}$$

Thus we have isomorphisms as in the statement, given by:

$$w_{ij} \to (F^*uF)_{ij}$$

But this gives both the assertions. □

Finally, as yet another basic example, we have the symplectic group Sp_N, consisting of symplectic matrices.

This is something more technical:

Theorem 10.4. *The symplectic group $Sp_N \subset U_N$ is given by*

$$Sp_2 = SU_2$$

and in general, by SU_2-patterned unitary matrices.

Proof. This is clear, indeed. □

We will be back to more examples, later on.

At the level of the basic examples, at small values of N, we have:

Theorem 10.5. *We have the following formula*

$$SU_2 = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \;\middle|\; |a|^2 + |b|^2 = 1 \right\}$$

which makes SU_2 isomorphic to a sphere.

Proof. Consider an arbitrary 2×2 matrix, written as follows:

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Assuming $\det U = 1$, the inverse is then given by:

$$U^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

On the other hand, assuming $U \in U_2$, the inverse must be the adjoint:

$$U^{-1} = \begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix}$$

We are therefore led to the following equations:

$$d = \bar{a}$$

$$c = -\bar{b}$$

Thus our matrix must be of the following form:

$$U = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$$

Since the determinant is 1, we must have, as stated:

$$|a|^2 + |b|^2 = 1$$

As for the converse, this is clear, the matrices in the statement being elements of SU_2.

Regarding now the last assertion, our computation of SU_2 has led us to the following formula:

$$SU_2 = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \;\middle|\; |a|^2 + |b|^2 = 1 \right\}$$

Now let us write:

$$a = x + iy$$

$$b = z + it$$

We have then the following alternative formula, which is very nice, because the parameters (x, y, z, t) range over the sphere of space-time:

$$SU_2 = \left\{ \begin{pmatrix} x + iy & z + it \\ -z + it & x - iy \end{pmatrix} \;\middle|\; x^2 + y^2 + z^2 + t^2 = 1 \right\}$$

Thus, we have proved the theorem. □

We have as well the following formula:

Theorem 10.6. *We have the following formula*

$$U_2 = \left\{ d\begin{pmatrix} a & b\\ -\bar{b} & \bar{a}\end{pmatrix} \;\middle|\; |a|^2 + |b|^2 = 1, |d| = 1 \right\}$$

but the parametrization is no longer bijective.

Proof. In one sense, this is clear, because we have:

$$|d| = 1 \implies dSU_2 \subset U_2$$

In the other sense, let $U \in U_2$. We have then:

$$\begin{aligned} & |\det(U)|^2\\ = \;& \det(U)\overline{\det(U)}\\ = \;& \det(U)\det(U^*)\\ = \;& \det(UU^*)\\ = \;& \det(1)\\ = \;& 1 \end{aligned}$$

Consider now the following complex number, up to a binary choice:

$$d = \sqrt{\det U}$$

We know that we have:

$$|d| = 1$$

Thus the matrix $V = U/d$ is unitary:

$$V \in U_N$$

Also, we have:

$$\begin{aligned} & \det(V)\\ = \;& \det(d^{-1}U)\\ = \;& d^{-2}\det(U)\\ = \;& \det(U)^{-1}\det(U)\\ = \;& 1 \end{aligned}$$

Thus we have $V \in SU_2$, and so we can write, with $|a|^2 + |b|^2 = 1$:

$$V = \begin{pmatrix} a & b\\ -\bar{b} & \bar{a}\end{pmatrix}$$

Thus $U = dV$ appears as in the statement, and we are done. □

We can now prove a theorem that we announced in the introduction:

Theorem 10.7. *We have a double cover map, obtained via the adjoint representation,*

$$SU_2 \to SO_3$$

and this map produces the Euler-Rodrigues formula, for the elements of SO_3.

Proof. The computation for SU_2 leads to the following formula:

$$SU_2 = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \;\middle|\; |a|^2 + |b|^2 = 1 \right\}$$

Let us write now our complex parameters a, b as follows:

$$a = x + iy$$

$$b = z + it$$

The real and imaginary parts must satisfy then:

$$x^2 + y^2 + z^2 + t^2 = 1$$

We have then the following alternative formula, which is very nice, because the parameters (x, y, z, t) range over the sphere of space-time:

$$SU_2 = \left\{ \begin{pmatrix} x + iy & z + it \\ -z + it & x - iy \end{pmatrix} \;\middle|\; x^2 + y^2 + z^2 + t^2 = 1 \right\}$$

Now let us appply the above-mentioned quotient map:

$$SU_2 \to SO_3$$

To be more precise, we can make act the elements $U \in SU_2$ by conjugation on $\mathbb{C}^2$, and by taking real parts, this gives the above quotient map.

We are led to the following formula, for the arbitrary elements $U \in SO_3$:

$$U = \begin{pmatrix} x^2 + y^2 - z^2 - t^2 & 2(yz - xt) & 2(xz + yt) \\ 2(xt + yz) & x^2 + z^2 - y^2 - t^2 & 2(zt - xy) \\ 2(yt - xz) & 2(xy + zt) & x^2 + t^2 - y^2 - z^2 \end{pmatrix}$$

Thus, we have obtained the Euler-Rodrigues formula, as claimed. □

We will see later on a more conceptual explanation for this formula.

Let us discuss now what can be done with matrix groups. We first have:

Definition 10.8. *Given a matrix group $G \subset U_N$, the function*

$$\chi : G \to \mathbb{C}$$

$$g \to Tr(g)$$

is called main character of the group.

We will see later on a number of motivations for the study of characters.

As a basic motivation, however, we have the results regarding the finite abelian groups, and their duals, consisting of characters, from the previous section. To be more precise, what we called "characters" there are characters of 1-dimensional representations.

As yet another motivation, some very interesting combinatorics appears when looking at the main character of S_N.

Let us start our study here with:

Proposition 10.9. *For the symmetric group $S_N \subset O_N$, the main character*

$$\chi : S_N \to \mathbb{N}$$

$$\sigma \to Tr(\sigma)$$

counts the number of fixed points of the permutations.

Proof. This is clear, indeed. □

Thus, we are led into some interesting combinatorics.

As a basic result here, which is something very beautiful, we have:

Theorem 10.10. *The probability for a random permutation*

$$\sigma \in S_N$$

to have no fixed points is

$$P \simeq \frac{1}{e}$$

in the $N \to \infty$ limit.

Proof. This is something very classical, which is best viewed by using the inclusion-exclusion principle. Consider indeed the following sets:

$$S_N^i = \left\{\sigma \in S_N \middle| \sigma(i) = i\right\}$$

The set of permutations having no fixed points is then:

$$X_N = \left(\bigcup_i S_N^i\right)^c$$

In order to compute now the cardinality $|X_N|$, consider as well the following sets, depending on indices $i_1 < \ldots < i_k$, obtained by taking intersections:

$$S_N^{i_1 \ldots i_k} = S_N^{i_1} \bigcap \ldots \bigcap S_N^{i_k}$$

Observe that we have the following formula:

$$S_N^{i_1\ldots i_k}=\left\{\sigma\in S_N\Big|\sigma(i_1)=i_1,\ldots,\sigma(i_k)=i_k\right\}$$

The inclusion-exclusion principle tells us that we have:

$$\begin{aligned}&\left|\left(\bigcup_i S_N^i\right)^c\right|\\ =\;&|S_N|-\sum_i|S_N^i|+\sum_{i<j}|S_N^i\cap S_N^j|-\ldots+(-1)^N\sum_{i_1<\ldots<i_N}|S_N^{i_1}\cup\ldots\cup S_N^{i_N}|\\ =\;&|S_N|-\sum_i|S_N^i|+\sum_{i<j}|S_N^{ij}|-\ldots+(-1)^N\sum_{i_1<\ldots<i_N}|S_N^{i_1\ldots i_N}|\end{aligned}$$

Thus, the probability that we are interested in is given by:

$$P=\frac{1}{N!}\left(|S_N|-\sum_i|S_N^i|+\sum_{i<j}|S_N^{ij}|-\ldots+(-1)^N\sum_{i_1<\ldots<i_N}|S_N^{i_1\ldots i_N}|\right)$$

Now observe that for any $i_1<\ldots<i_k$ we have:

$$|S_N^{i_1\ldots i_k}|=(N-k)!$$

We obtain from this:

$$\begin{aligned}P&=\frac{1}{N!}\sum_{k=0}^N(-1)^k\sum_{i_1<\ldots<i_k}|S_N^{i_1\ldots i_k}|\\ &=\frac{1}{N!}\sum_{k=0}^N(-1)^k\sum_{i_1<\ldots<i_k}(N-k)!\\ &=\frac{1}{N!}\sum_{k=0}^N(-1)^k\binom{N}{k}(N-k)!\\ &=\sum_{k=0}^N\frac{(-1)^k}{k!}\\ &=1-\frac{1}{1!}+\frac{1}{2!}-\ldots+(-1)^{N-1}\frac{1}{(N-1)!}+(-1)^N\frac{1}{N!}\end{aligned}$$

Since on the right we have the expansion of $\frac{1}{e}$, this gives the result. □

We will be back to this later, with several generalizations.

Let us do as well a computation for a continuous group. We have:

Theorem 10.11. *The main character of the group*

$$Sp_2 = SU_2$$

written as

$$Sp_2 = SU_2 = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \;\middle|\; |a|^2 + |b|^2 = 1 \right\}$$

is given by the formula

$$\chi = 2Re(a)$$

and follows a semicircle law.

Proof. This follows by identifying SU_2 with the sphere $S^3_{\mathbb{R}} \subset \mathbb{R}^4$, and the uniform measure on SU_2 with the uniform measure on this sphere.

To be more precise, let us recall that we can write our complex parameters a, b as follows:

$$a = x + iy$$
$$b = z + it$$

The real and imaginary parts must satisfy then:

$$x^2 + y^2 + z^2 + t^2 = 1$$

Thus we have the following alternative formula, with the parameters (x, y, z, t) ranging over the sphere in 4 dimensions:

$$SU_2 = \left\{ \begin{pmatrix} x + iy & z + it \\ -z + it & x - iy \end{pmatrix} \;\middle|\; x^2 + y^2 + z^2 + t^2 = 1 \right\}$$

We will be back to this later on, with full details. □

It is possible to work out some asymptotic results as well, for both Sp_N and SU_N, and for the other continuous groups as well. However, this is something which is not elementary, and we will be back to this later on, in section 16 below.

As a conclusion, all this leads us into probability theory.

11. Character laws

We discuss here in this section the basics of probability theory. Later on, at the end of this section, and in the next sections, we will do probability on groups.

Generally speaking, probability is best learned by starting with flipping coins and dices. There are a few nice exercices here, which are an excellent introduction to the notion of independence, that we will formally introduce later on.

At a more advanced level now, which is playing cards, we have:

Theorem 11.1. *The probabilities at poker are as follows:*

(1) *One pair:* 0.533.
(2) *Two pairs:* 0.120.
(3) *Three of a kind:* 0.053.
(4) *Full house:* 0.006.
(5) *Straight:* 0.005.
(6) *Four of a kind:* 0.001.
(7) *Flush:* 0.000.
(8) *Straight flush:* 0.000.

Proof. Let us consider indeed our deck of 32 cards:

$$7, 8, 9, 10, J, Q, K, A$$

The total number of possibilities is:

$$\begin{aligned}\binom{32}{5} &= \frac{32 \cdot 31 \cdot 30 \cdot 29 \cdot 28}{2 \cdot 3 \cdot 4 \cdot 5}\\ &= 32 \cdot 31 \cdot 29 \cdot 7\end{aligned}$$

(1) For having a pair, the number of possibilities is:

$$\begin{aligned}N &= \binom{8}{1}\binom{4}{2} \times \binom{7}{3}\binom{4}{1}^3\\ &= 8 \cdot 6 \cdot 35 \cdot 64\end{aligned}$$

Thus, the probability of having a pair is:

$$\begin{aligned}P &= \frac{8 \cdot 6 \cdot 35 \cdot 64}{32 \cdot 31 \cdot 29 \cdot 7}\\ &= \frac{6 \cdot 5 \cdot 16}{31 \cdot 29}\\ &= \frac{480}{899}\\ &= 0.533\end{aligned}$$

(2) For having two pairs, the number of possibilities is:

$$\begin{aligned} N &= \binom{8}{2}\binom{4}{2}^2 \times \binom{24}{1} \\ &= 28 \cdot 36 \cdot 24 \end{aligned}$$

Thus, the probability of having two pairs is:

$$\begin{aligned} P &= \frac{28 \cdot 36 \cdot 24}{32 \cdot 31 \cdot 29 \cdot 7} \\ &= \frac{36 \cdot 3}{31 \cdot 29} \\ &= \frac{108}{899} \\ &= 0.120 \end{aligned}$$

(3) For having three of a kind, the number of possibilities is:

$$\begin{aligned} N &= \binom{8}{1}\binom{4}{3} \times \binom{7}{2}\binom{4}{1}^2 \\ &= 8 \cdot 4 \cdot 21 \cdot 16 \end{aligned}$$

Thus, the probability of having three of a kind is:

$$\begin{aligned} P &= \frac{8 \cdot 4 \cdot 21 \cdot 16}{32 \cdot 31 \cdot 29 \cdot 7} \\ &= \frac{3 \cdot 16}{31 \cdot 29} \\ &= \frac{48}{899} \\ &= 0.053 \end{aligned}$$

(4) For having full house, the number of possibilities is:

$$\begin{aligned} N &= \binom{8}{1}\binom{4}{3} \times \binom{7}{1}\binom{4}{2} \\ &= 8 \cdot 4 \cdot 7 \cdot 6 \end{aligned}$$

Thus, the probability of having full house is:

$$\begin{aligned} P &= \frac{8 \cdot 4 \cdot 7 \cdot 6}{32 \cdot 31 \cdot 29 \cdot 7} \\ &= \frac{6}{31 \cdot 29} \\ &= \frac{6}{899} \\ &= 0.006 \end{aligned}$$

(5) For having a straight, the number of possibilities is:

$$\begin{aligned} N &= 4\left[\binom{4}{1}^4 - 4\right] \\ &= 16 \cdot 63 \end{aligned}$$

Thus, the probability of having a straight is:

$$\begin{aligned} P &= \frac{16 \cdot 63}{32 \cdot 31 \cdot 29 \cdot 7} \\ &= \frac{9}{2 \cdot 31 \cdot 29} \\ &= \frac{9}{1798} \\ &= 0.005 \end{aligned}$$

(6) For having four of a kind, the number of possibilities is:

$$\begin{aligned} N &= \binom{8}{1}\binom{4}{4} \times \binom{7}{1}\binom{4}{1} \\ &= 8 \cdot 7 \cdot 4 \end{aligned}$$

Thus, the probability of having four of a kind is:

$$\begin{aligned} P &= \frac{8 \cdot 7 \cdot 4}{32 \cdot 31 \cdot 29 \cdot 7} \\ &= \frac{1}{31 \cdot 29} \\ &= \frac{1}{899} \\ &= 0.001 \end{aligned}$$

(7) For having a flush, the number of possibilities is:

$$\begin{aligned} N &= 4\left[\binom{8}{4} - 4\right] \\ &= 4 \cdot 66 \end{aligned}$$

Thus, the probability of having a flush is:

$$\begin{aligned} P &= \frac{4 \cdot 66}{32 \cdot 31 \cdot 29 \cdot 7} \\ &= \frac{33}{4 \cdot 31 \cdot 29 \cdot 7} \\ &= \frac{9}{25172} \\ &= 0.000 \end{aligned}$$

(8) For having a straight flush, the number of possibilities is:

$$N = 4 \cdot 4$$

Thus, the probability of having a straight flush is:

$$\begin{aligned} P &= \frac{4 \cdot 4}{32 \cdot 31 \cdot 29 \cdot 7} \\ &= \frac{1}{2 \cdot 31 \cdot 29 \cdot 7} \\ &= \frac{1}{12586} \\ &= 0.000 \end{aligned}$$

Thus, we have obtained the numbers in the statement. □

Summarizing, probability is basically about binomials and factorials.

We will see later that, in connection with more advanced questions, some standard calculus comes into play as well.

Let us discuss now the general theory. The fundamental result in probability is the Central Limit Theorem (CLT), and our first task will be that of explaining this.

With the idea in mind of doing things a bit abstractly, our starting point will be:

Definition 11.2. *Let X be a probability space, that is to say, a space with a probability measure, and with the corresponding integration denoted $\mathbb{E}$, and called expectation.*

(1) *The random variables are the real functions as follows:*

$$f \in L^\infty(X)$$

(2) *The moments of such a variable are the numbers:*

$$M_k(f) = \mathbb{E}(f^k)$$

(3) *The law of such a variable is the measure given by:*

$$M_k(f) = \int_{\mathbb{R}} x^k d\mu_f(x)$$

Here the fact that μ_f exists indeed is not trivial. By linearity, we would like to have a real probability measure making hold the following formula, for any $P \in \mathbb{R}[X]$:

$$\mathbb{E}(P(f)) = \int_{\mathbb{R}} P(x) d\mu_f(x)$$

By using a continuity argument, it is enough to have this formula for the characteristic functions χ_I of the arbitrary measurable sets of real numbers $I \subset \mathbb{R}$:

$$\mathbb{E}(\chi_I(f)) = \int_{\mathbb{R}} \chi_I(x) d\mu_f(x)$$

Thus, we would like to have a measure μ_f such that:

$$\mathbb{P}(f \in I) = \mu_f(I)$$

But this latter formula can serve as a definition for μ_f, with the axioms of real probability measures being trivially satisfied, and so we are done.

Next in line, we need to talk about independence. Once again with the idea of doing things a bit abstractly, the definition here is as follows:

Definition 11.3. *Two variables $f, g \in L^\infty(X)$ are called independent when*

$$\mathbb{E}(f^k g^l) = \mathbb{E}(f^k) \cdot \mathbb{E}(g^l)$$

happens, for any $k, l \in \mathbb{N}$.

Once again, this definition hides some non-trivial things. Indeed, by linearity, we would like to have a formula as follows, valid for any polynomials $P, Q \in \mathbb{R}[X]$:

$$\mathbb{E}(P(f)Q(g)) = \mathbb{E}(P(f)) \cdot \mathbb{E}(Q(g))$$

By continuity, it is enough to have this formula for characteristic functions χ_I, χ_J of the arbitrary measurable sets of real numbers $I, J \subset \mathbb{R}$:

$$\mathbb{E}(\chi_I(f)\chi_J(g)) = \mathbb{E}(\chi_I(f)) \cdot \mathbb{E}(\chi_J(g))$$

Thus, we are led to the usual definition of independence, namely:

$$\mathbb{P}(f \in I, g \in J) = \mathbb{P}(f \in I) \cdot \mathbb{P}(g \in J)$$

All this might seem a bit abstract, but in practice, the idea is of course that f, g must be independent, in an intuitive, real-life sense.

Here is now our first result, regarding this notion of independence:

Proposition 11.4. *Assuming that $f, g \in L^\infty(X)$ are independent, we have*

$$\mu_{f+g} = \mu_f * \mu_g$$

where $*$ is the convolution of real probability measures.

Proof. We have the following computation, using the independence of f, g:

$$\begin{aligned}
& M_k(f+g)\\
= \ & \mathbb{E}((f+g)^k)\\
= \ & \sum_l \binom{k}{l}\mathbb{E}(f^l g^{k-l})\\
= \ & \sum_l \binom{k}{l}M_l(f)M_{k-l}(g)
\end{aligned}$$

On the other hand, by using the Fubini theorem, we have as well:

$$\begin{aligned}
& \int_{\mathbb{R}} x^k d(\mu_f * \mu_g)(x)\\
= \ & \int_{\mathbb{R}\times\mathbb{R}} (x+y)^k d\mu_f(x)d\mu_g(y)\\
= \ & \sum_l \binom{k}{l}\int_{\mathbb{R}} x^k d\mu_f(x)\int_{\mathbb{R}} y^l d\mu_g(y)\\
= \ & \sum_l \binom{k}{l}M_l(f)M_{k-l}(g)
\end{aligned}$$

Thus the measures μ_{f+g} and $\mu_f * \mu_g$ have the same moments:

$$M_k(\mu_{f+g}) = M_k(\mu_f * \mu_g)$$

We conclude that these two measures coincide, as stated. □

Here is now our second result, which is something more advanced, providing us with some efficient tools for the study of the independence:

Theorem 11.5. *Assuming that $f, g \in L^\infty(X)$ are independent, we have*

$$F_{f+g} = F_f F_g$$

where $F_f(x) = \mathbb{E}(e^{ixf})$ is the Fourier transform.

Proof. We have the following computation, using Proposition 11.4 and Fubini:

$$\begin{aligned}
& F_{f+g}(x) \\
= & \int_{\mathbb{R}} e^{ixy} d\mu_{f+g}(y) \\
= & \int_{\mathbb{R}} e^{ixy} d(\mu_f * \mu_g)(y) \\
= & \int_{\mathbb{R}\times\mathbb{R}} e^{ix(y+z)} d\mu_f(y) d\mu_g(z) \\
= & \int_{\mathbb{R}} e^{ixy} d\mu_f(y) \int_{\mathbb{R}} e^{ixz} d\mu_g(z) \\
= & F_f(x) F_g(x)
\end{aligned}$$

Thus, we are led to the conclusion in the statement. □

Let us discuss now the normal distributions. These are defined as follows:

Definition 11.6. *The normal law of parameter* 1 *is the following measure:*

$$g_1 = \frac{1}{\sqrt{2\pi}} e^{-x^2/2} dx$$

More generally, the normal law of parameter $t > 0$ *is the following measure:*

$$g_t = \frac{1}{\sqrt{2\pi t}} e^{-x^2/2t} dx$$

These are also called Gaussian distributions, with "g" standing for Gauss.

As a first remark, the above laws have indeed mass 1, as they should. This follows indeed from the Gauss formula, which gives, with $x = y/\sqrt{2t}$:

$$\int_{\mathbb{R}} e^{-y^2/2t} dy = \sqrt{2\pi t}$$

Generally speaking, the normal laws appear as bit everywhere, in real life. The reasons behind this phenomenon come from the Central Limit Theorem (CLT), that we will explain in a moment, after developing the needed general theory.

As a first result regarding the normal laws, we have:

Proposition 11.7. *We have the variance formula*

$$V(g_t) = t$$

valid for any $t > 0$.

Proof. The first moment is 0, because our normal law g_t is centered:

$$M_1 = 0$$

As for the second moment, this can be computed as follows:

$$\begin{aligned}
M_2 &= \frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} x^2 e^{-x^2/2t}dx\\
&= \frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} (tx)\left(-e^{-x^2/2t}\right)'dx\\
&= \frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} te^{-x^2/2t}dx\\
&= \sqrt{\frac{t}{2\pi}}\int_{\mathbb{R}} e^{-x^2/2t}dx\\
&= \sqrt{\frac{t}{2\pi}}\times\sqrt{2\pi t}\\
&= t
\end{aligned}$$

We conclude from this that the variance is $V = t$. □

We will be back to this later, with formulae for the higher moments as well.

Here is now another result, which is very useful in practice:

Theorem 11.8. *We have the following formula, for any $t > 0$:*

$$F_{g_t}(x) = e^{-tx^2/2}$$

In particular, the normal laws satisfy

$$g_s * g_t = g_{s+t}$$

for any $s, t > 0$.

Proof. The Fourier transform formula can be established as follows:

$$\begin{aligned}
& F_{g_t}(x) \\
= \ & \frac{1}{\sqrt{2\pi t}} \int_{\mathbb{R}} e^{-y^2/2t+ixy} dy \\
= \ & \frac{1}{\sqrt{2\pi t}} \int_{\mathbb{R}} e^{-(y/\sqrt{2t}-\sqrt{t/2}ix)^2-tx^2/2} dy \\
= \ & \frac{1}{\sqrt{2\pi t}} \int_{\mathbb{R}} e^{-z^2-tx^2/2}\sqrt{2t} dz \\
= \ & \frac{1}{\sqrt{\pi}} e^{-tx^2/2} \int_{\mathbb{R}} e^{-z^2} dz \\
= \ & \frac{1}{\sqrt{\pi}} e^{-tx^2/2} \cdot \sqrt{\pi} \\
= \ & e^{-tx^2/2}
\end{aligned}$$

As for the last assertion, this follows from the linearization result from Theorem 11.5 (2) above, because $\log F_{g_t}$ is linear in t. □

We are now ready to state and prove the CLT, as follows:

Theorem 11.9 (CLT)**.** *Given random variables*

$$f_1, f_2, f_3, \ldots \in L^\infty(X)$$

which are i.i.d., centered, and with variance $t > 0$, we have, with $n \to \infty$, in moments,

$$\frac{1}{\sqrt{n}} \sum_{i=1}^{n} f_i \sim g_t$$

where g_t is the Gaussian law of parameter t, having as density $\frac{1}{\sqrt{2\pi t}} e^{-y^2/2t} dy$.

Proof. We use the Fourier transform, which is by definition given by:

$$F_f(x) = \mathbb{E}(e^{ixf})$$

In terms of moments, we have the following formula:

$$\begin{aligned}
& F_f(x) \\
= \ & \mathbb{E}\left(\sum_{k=0}^{\infty}\frac{(ixf)^k}{k!}\right) \\
= \ & \sum_{k=0}^{\infty}\frac{(ix)^k\mathbb{E}(f^k)}{k!} \\
= \ & \sum_{k=0}^{\infty}\frac{i^kM_k(f)}{k!}\,x^k
\end{aligned}$$

Thus, the Fourier transform of the variable in the statement is:

$$\begin{aligned}
F(x) &= \left[F_f\left(\frac{x}{\sqrt{n}}\right)\right]^n \\
&= \left[1-\frac{tx^2}{2n}+O(n^{-2})\right]^n \\
&\simeq \left[1-\frac{tx^2}{2n}\right]^n \\
&\simeq e^{-tx^2/2}
\end{aligned}$$

But this latter function being the Fourier transform of g_t, we obtain the result. □

Let us discuss now some further properties of the normal law. We first have:

Proposition 11.10. *The moments of the normal law are the numbers*

$$M_k(g_t)=t^{k/2}\times k!!$$

where the double factorials are by definition given by

$$k!!=1\cdot 3\cdot 5\ldots(k-1)$$

with the convention $k!!=0$ when k is odd.

Proof. We have the following computation:

$$\begin{aligned} M_k &= \frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} x^k e^{-x^2/2t}dx \\ &= \frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} (tx^{k-1})\left(-e^{-x^2/2t}\right)' dx \\ &= \frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} t(k-1)x^{k-2}e^{-x^2/2t}dx \\ &= t(k-1)\times\frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} x^{k-2}e^{-x^2/2t}dx \\ &= t(k-1)M_{k-2} \end{aligned}$$

Now recall from the proof of Proposition 11.7 above that we have:

$$M_0 = 1$$

$$M_1 = 0$$

Thus by recurrence, the even moments all vanish, and the odd moments are given by the formula in the statement. □

We can improve the above result, as follows:

Proposition 11.11. *The moments of the normal law are the numbers*

$$M_k(g_t) = t^{k/2}|P_2(k)|$$

where $P_2(k)$ is the set of pairings of $\{1,\ldots,k\}$.

Proof. Let us count the pairings of $\{1,\ldots,k\}$. In order to have such a pairing, we must pair 1 with one of $2,\ldots,k$, and then use a pairing of the remaining $k-2$ points.

Thus, we have the following recurrence formula:

$$|P_2(k)| = (k-1)|P_2(k-2)|$$

As for the initial data, this is:

$$P_1 = 0$$

$$P_2 = 1$$

We therefore obtain, by recurrence:

$$|P_2(k)| = k!!$$

Thus, we are led to the conclusion in the statement. □

We are done done yet, and here is one more improvement:

Theorem 11.12. *The moments of the normal law are the numbers*

$$M_k(g_t) = \sum_{\pi\in P_2(k)} t^{|\pi|}$$

where $P_2(k)$ is the set of pairings of $\{1,\ldots,k\}$, and $|.|$ is the number of blocks.

Proof. This follows indeed from Proposition 11.11 above, because the number of blocks of a pairing of $\{1,\ldots,k\}$ is trivially $k/2$, independently of the pairing. □

We will see later on that many other interesting probability distributions are subject to similar formulae regarding their moments, involving partitions, and a lot of interesting combinatorics. Discussing this will be in fact a main theme of the present book.

As a first application, we have the following result:

Theorem 11.13. *The moments of the hyperspherical variables are*

$$\int_{S_{\mathbb{R}}^{N-1}} x_i^k dx = \frac{(N-1)!!k!!}{(N+k-1)!!}$$

and the normalized variables

$$y_i = \frac{x_i}{\sqrt{N}}$$

become normal with $N\to\infty$.

Proof. The formula in the statement follows from the general integration formula over the sphere, established in section 6 above, which is as follows:

$$\int_{S_{\mathbb{R}}^{N-1}} x_{i_1}\ldots x_{i_k}\,dx = \frac{(N-1)!!l_1!!\ldots l_N!!}{(N+\sum l_i-1)!!}$$

Now observe that with $N\to\infty$ we have:

$$\begin{aligned}\int_{S_{\mathbb{R}}^{N-1}} x_i^k dx &\simeq N^{k/2}k!!\\ &= N^{k/2}M_k(g_1)\end{aligned}$$

Thus, we are led to the conclusions in the statement. □

As a comment here, the rescaled variables $x_i/\sqrt{N}$ can be shown as well to become independent with $N\to\infty$. We will be back to this.

We can talk as well about rotations, as follows:

Theorem 11.14. *We have the integration formula*

$$\int_{O_N} U_{ij}^k dU = \frac{(N-1)!!k!!}{(N+k-1)!!}$$

and the normalized variables

$$V_{ij} = \frac{U_{ij}}{\sqrt{N}}$$

become normal with $N \to \infty$.

Proof. We use the well-known fact that we have an embedding as follows, for any i, which makes correspond the respective integration functionals:

$$C(S_{\mathbb{R}}^{N-1}) \subset C(O_N)$$

$$x_i \to U_{1i}$$

With this identification made, the result follows from Theorem 11.13. □

As a comment here, the rescaled variables $U_{ij}/\sqrt{N}$ can be shown as well to become independent with $N \to \infty$. We will be back to this.

Let us discuss now the "discrete" counterpart of the above results, which involve the Poisson laws p_t, which appear via the Poisson Limit Theorem (PLT).

Let us start with the following definition:

Definition 11.15. *The Poisson law of parameter 1 is the following measure,*

$$p_1 = \frac{1}{e} \sum_k \frac{\delta_k}{k!}$$

and the Poisson law of parameter $t > 0$ is the following measure,

$$p_t = e^{-t} \sum_k \frac{t^k}{k!} \delta_k$$

with the letter "p" standing for Poisson.

Observe that these laws have indeed mass 1, as they should, and this due to the following well-known formula, which is the foundational formula of calculus:

$$e^t = \sum_k \frac{t^k}{k!}$$

We will see in the moment why these measures appear a bit everywhere, in discrete contexts, the reasons behind this coming from the Poisson Limit Theorem (PLT).

Let us first develop some general theory. We first have:

Theorem 11.16. *We have the following formula, for any $s, t > 0$,*

$$p_s * p_t = p_{s+t}$$

so the Poisson laws form a convolution semigroup.

Proof. The convolution of Dirac masses is given by:

$$\delta_k * \delta_l = \delta_{k+l}$$

By using this formula and the binomial formula, we obtain:

$$\begin{aligned}
p_s * p_t &= e^{-s} \sum_k \frac{s^k}{k!} \delta_k * e^{-t} \sum_l \frac{t^l}{l!} \delta_l \\
&= e^{-s-t} \sum_{kl} \frac{s^k t^l}{k!l!} \delta_{k+l} \\
&= e^{-s-t} \sum_n \delta_n \sum_{k+l=n} \frac{s^k t^l}{k!l!} \\
&= e^{-s-t} \sum_n \frac{\delta_n}{n!} \sum_{k+l=n} \frac{n!}{k!l!} s^k t^l \\
&= e^{-s-t} \sum_n \frac{(s+t)^n}{n!} \delta_n \\
&= p_{s+t}
\end{aligned}$$

Thus, we are led to the conclusion in the statement. □

We will see later another proof of this fact, using the Fourier transform.

We have as well the following result:

Theorem 11.17. *The Poisson laws appear as exponentials*

$$p_t = \sum_k \frac{t^k (\delta_1 - \delta_0)^{*k}}{k!}$$

with respect to the convolution of measures $*$.

Proof. By using the binomial formula, the measure at right is:

$$\begin{aligned}
\mu &= \sum_k \frac{t^k}{k!} \sum_{p+q=k} (-1)^q \frac{k!}{p!q!} \delta_p \\
&= \sum_k t^k \sum_{p+q=k} (-1)^q \frac{\delta_p}{p!q!} \\
&= \sum_p \frac{t^p \delta_p}{p!} \sum_q \frac{(-1)^q}{q!} \\
&= \frac{1}{e} \sum_p \frac{t^p \delta_p}{p!} \\
&= p_t
\end{aligned}$$

Thus, we are led to the conclusion in the statement. □

The Fourier transform computation is as follows:

Theorem 11.18. *The Fourier transform of p_t is given by*

$$F_{p_t}(x) = \exp\left((e^{ix} - 1)t\right)$$

for any $t > 0$.

Proof. We have by definition:

$$F_f(x) = \mathbb{E}(e^{ixf})$$

We therefore obtain:

$$\begin{aligned}
F_{p_t}(x) &= e^{-t} \sum_k \frac{t^k}{k!} F_{\delta_k}(x) \\
&= e^{-t} \sum_k \frac{t^k}{k!} e^{ikx} \\
&= e^{-t} \sum_k \frac{(e^{ix}t)^k}{k!} \\
&= \exp(-t) \exp(e^{ix}t) \\
&= \exp\left((e^{ix} - 1)t\right)
\end{aligned}$$

Thus, we obtain the formula in the statement. □

Observe that we obtain in this way another proof for the convolution semigroup property.

We can now establish the Poisson Limit Theorem (PLT), as follows:

Theorem 11.19. *We have the following convergence, in moments,*

$$\left(\left(1-\frac{t}{n}\right)\delta_0+\frac{t}{n}\delta_1\right)^{*n}\to p_t$$

for any $t>0$.

Proof. Let us denote by μ_n the measure under the convolution sign:

$$\mu_n=\left(1-\frac{t}{n}\right)\delta_0+\frac{t}{n}\delta_1$$

We have the following computation:

$$\begin{aligned}
& F_{\delta_r}(x)=e^{irx}\\
\implies\quad & F_{\mu_n}(x)=\left(1-\frac{t}{n}\right)+\frac{t}{n}e^{ix}\\
\implies\quad & F_{\mu_n^{*n}}(x)=\left(\left(1-\frac{t}{n}\right)+\frac{t}{n}e^{ix}\right)^n\\
\implies\quad & F_{\mu_n^{*n}}(x)=\left(1+\frac{(e^{ix}-1)t}{n}\right)^n\\
\implies\quad & F(x)=\exp\left((e^{ix}-1)t\right)
\end{aligned}$$

Thus, we obtain the Fourier transform of p_t, as desired. □

At the level of moments now, things are quite subtle, and we first have:

Theorem 11.20. *The moments of p_1 are the Bell numbers,*

$$M_k(p_1)=|P(k)|$$

where $P(k)$ is the set of partitions of $\{1,\ldots,k\}$.

Proof. The moments of p_1 are given by the following formula:

$$M_k=\frac{1}{e}\sum_s\frac{s^k}{s!}$$

We have the following recurrence formula for these moments:

$$\begin{aligned}
M_{k+1} &= \frac{1}{e}\sum_s \frac{(s+1)^{k+1}}{(s+1)!} \\
&= \frac{1}{e}\sum_s \frac{(s+1)^k}{s!} \\
&= \frac{1}{e}\sum_s \frac{s^k}{s!}\left(1+\frac{1}{s}\right)^k \\
&= \frac{1}{e}\sum_s \frac{s^k}{s!}\sum_r \binom{k}{r} s^{-r} \\
&= \sum_r \binom{k}{r}\cdot\frac{1}{e}\sum_s \frac{s^{k-r}}{s!} \\
&= \sum_r \binom{k}{r} M_{k-r}
\end{aligned}$$

Let us try now to find a recurrence for the Bell numbers:

$$B_k = |P(k)|$$

A partition of $\{1,\ldots,k+1\}$ appears by choosing r neighbors for 1, among the k numbers available, and then partitioning the $k-r$ elements left. Thus, we have:

$$B_{k+1} = \sum_r \binom{k}{r} B_{k-r}$$

Thus, the numbers M_k satisfy the same recurrence as the numbers B_k.

Regarding now the initial values, for the moments of p_1, these are:

$$M_0 = 1$$

$$M_1 = 1$$

Indeed, the formula $M_0 = 1$ is clear, and the formula $M_1 = 1$ follows from:

$$\begin{aligned}
M_1 &= \frac{1}{e}\sum_s \frac{s}{s!} \\
&= \frac{1}{e}\sum_s \frac{1}{(s-1)!} \\
&= \frac{1}{e}\times e \\
&= 1
\end{aligned}$$

Now by using the above recurrence we obtain from this:

$$\begin{aligned} M_2 &= \sum_r \binom{1}{r} M_{k-r} \\ &= 1+1 \\ &= 2 \end{aligned}$$

Thus, we can say that the initial values for the moments are:

$$M_1 = 1$$

$$M_2 = 2$$

As for the Bell numbers, here the initial values are:

$$B_1 = 1$$

$$B_2 = 2$$

Thus the initial values coincide, and so these numbers are equal, as stated. □

Quite remarkably, the Bell numbers cannot be explicitely computed. However, there are many interesting formulae for them, and we refer here to the literature.

More generally, we have the following result:

Theorem 11.21. *The moments of p_t are given by*

$$M_k(p_t) = \sum_{\pi \in P(k)} t^{|\pi|}$$

where $|.|$ is the number of blocks.

Proof. Observe first that the formula in the statement generalizes the one in Theorem 11.20 above, because at $t = 1$ we obtain, as we should:

$$\begin{aligned} M_k(p_1) &= \sum_{\pi \in P(k)} 1^{|\pi|} \\ &= |P(k)| \\ &= B_k \end{aligned}$$

In general now, the moments of p_t with $t > 0$ are given by:

$$M_k = e^{-t} \sum_s \frac{t^s s^k}{s!}$$

By doing some combinatorics, we are therefore led into the Stirling numbers, and into the conclusion in the statement. □

Observe the analogy with the moment formulae for g_t and G_t, discussed before. We will be back later with some more conceptual explanations for these results.

Let us get back now to groups, and compute laws of characters.

First, we have:

Proposition 11.22. *For the cyclic group $\mathbb{Z}_N \subset O_N$ we have*

$$\chi(g) = N\delta_{g0}$$

and the corresponding distribution is a Bernoulli law:

$$law(\chi) = \left(1 - \frac{1}{N}\right)\delta_0 + \frac{1}{N}\delta_N$$

Proof. The cyclic matrices have 0 on the diagonal, and so trace 0, expect for the identity, having 1 on the diagonal, and trace N. □

We have as well the following result:

Proposition 11.23. *For the dihedral group $D_N \subset S_N$ we have:*

$$law(\chi) = \begin{cases} \left(\frac{3}{4} - \frac{1}{2N}\right)\delta_0 + \frac{1}{4}\delta_2 + \frac{1}{2N}\delta_N & (N \text{ even}) \\ \left(\frac{1}{2} - \frac{1}{2N}\right)\delta_0 + \frac{1}{2}\delta_1 + \frac{1}{2N}\delta_N & (N \text{ odd}) \end{cases}$$

Proof. The dihedral group D_N consists indeed of:

(1) N symmetries, having 1 fixed point when N is odd, and having 0 or 2 fixed points, $50 - 50$, when N is even.

(2) N rotations, having 0 fixed points, except for the identity, which has N fixed points.

Thus, we are led to the formulae in the statement. □

Observe that the asymptotics are not interesting for D_N.

At a more advanced level now, we have:

Theorem 11.24. *For the symmetric group $S_N \subset O_N$ we have*

$$\chi \sim p_1$$

in the $N \to \infty$ limit.

Proof. This is best viewed by using the inclusion-exclusion principle. Let us set:

$$S_N^{i_1 \ldots i_k} = \left\{\sigma \in S_N \middle| \sigma(i_1) = i_1, \ldots, \sigma(i_k) = i_k\right\}$$

By using the inclusion-exclusion principle, we have:

$$\begin{aligned}&\mathbb{P}(\chi=0)\\ =\ &\frac{1}{N!}\left(|S_N|-\sum_i|S_N^i|+\sum_{i<j}|S_N^{ij}|-\ldots+(-1)^N\sum_{i_1<\ldots<i_N}|S_N^{i_1\ldots i_N}|\right)\end{aligned}$$

Now observe that we have, for any $i_1<\ldots<i_k$:

$$|S_N^{i_1\ldots i_k}|=(N-k)!$$

Wse obtain from this:

$$\begin{aligned}&\mathbb{P}(\chi=0)\\ =\ &1-\frac{1}{1!}+\frac{1}{2!}-\ldots+(-1)^{N-1}\frac{1}{(N-1)!}+(-1)^N\frac{1}{N!}\end{aligned}$$

Since on the right we have the expansion of $\frac{1}{e}$, we conclude that we have:

$$\lim_{N\to\infty}\mathbb{P}(\chi=0)=\frac{1}{e}$$

More generally, by modifying the above proof, we obtain:

$$\lim_{N\to\infty}\mathbb{P}(\chi=k)=\frac{1}{ek!}$$

Thus, we are led to the conclusion in the statement. □

Observe that the convergence is very fast.

In order to further build on this, let us formulate the following definition:

Definition 11.25. *Given a matrix group $G\subset U_N$, the functions*

$$\chi_t:G\to\mathbb{C}$$

$$g\to\sum_{i=1}^{[tN]}g_{ii}$$

with $t\in(0,1]$ are called main truncated characters of the group.

We will see later on a number of motivations for the study of characters.

As a basic motivation, however, we have:

Proposition 11.26. *For the symmetric group $S_N\subset O_N$, the truncated character*

$$\chi_t:S_N\to\mathbb{R}$$

$$\sigma\to Tr(\sigma)$$

counts the number of fixed points of the permutations,among $\{1,\ldots,[tN]\}$.

Proof. This is something trivial. □

At a more advanced level now, we have:

Theorem 11.27. *For the symmetric group $S_N \subset O_N$ we have*

$$\chi_t \sim p_t$$

in the $N \to \infty$ limit.

Proof. This is best viewed by using the inclusion-exclusion principle. Let us set:

$$S_N^{i_1 \ldots i_k} = \left\{ \sigma \in S_N \middle| \sigma(i_1) = i_1, \ldots, \sigma(i_k) = i_k \right\}$$

By using the inclusion-exclusion principle, we have:

$$\mathbb{P}(\chi = 0) = \frac{1}{N!} \left(|S_N| - \sum_i |S_N^i| + \sum_{i<j} |S_N^{ij}| - \ldots + (-1)^N \sum_{i_1 < \ldots < i_N} |S_N^{i_1 \ldots i_N}| \right)$$

Now observe that we have, for any $i_1 < \ldots < i_k$:

$$|S_N^{i_1 \ldots i_k}| = (N-k)!$$

We obtain from this:

$$\mathbb{P}(\chi = 0) = 1 - \frac{1}{1!} + \frac{1}{2!} - \ldots + (-1)^{N-1} \frac{1}{(N-1)!} + (-1)^N \frac{1}{N!}$$

Since on the right we have the expansion of $\frac{1}{e}$, we conclude that we have:

$$\lim_{N \to \infty} \mathbb{P}(\chi = 0) = \frac{1}{e}$$

More generally, by modifying the above proof, we obtain:

$$\lim_{N \to \infty} \mathbb{P}(\chi = k) = \frac{1}{ek!}$$

At $t > 0$ the computation is similar.
Thus, we are led to the conclusion in the statement. □

We will be back to this, with computations for other finite groups.

In the continuous case now, let us record the following result, which deals as well with truncated characters, at the special value of the truncation parameter $t = 1/N$:

Theorem 11.28. *For the orthogonal group O_N we have*

$$\frac{u_{11}}{\sqrt{N}} \sim g_1$$

in the $N \to \infty$ limit.

Proof. This follows from the fact that u_{11} follows a hyperspherical law, and so we can compute its asymptotics by using the formulae in section 6 above. □

We have as well a complex version of this result:

Theorem 11.29. *For the unitary group U_N we have*

$$\frac{u_{11}}{\sqrt{N}} \sim G_1$$

in the $N \to \infty$ limit.

Proof. This follows from the fact that u_{11} follows a complex hyperspherical law, and so we can compute its asymptotics by using the formulae in section 6 above. □

We will be back to O_N, U_N later on, after developing appropriate tools.

x

12. Reflection groups

We have seen so far that there are many interesting examples of compact groups of unitary matrices $G \subset U_N$, and that an interesting question regarding such groups is the computation of the laws of the truncated characters, given by:

$$\chi_t(g) = \sum_{i=1}^{[tN]} g_{ii}$$

In this section we focus on the finite group case, with a number of advanced results.

The continuous group case, which is more complicated, and requires substantial preliminaries, will be discussed later on, in sections 13-16 below.

Getting back to the list of examples of finite groups $G \subset U_N$ that we have, from sections 9 and 10 above, this is basically as follows:

$$\mathbb{Z}_N \subset D_N \subset S_N \subset H_N$$

In addition, we have the following general series of reflection groups $H_N^s \subset U_N$, which generalize S_N, H_N, which appear at $s = 1, 2$:

$$H_N^s = \mathbb{Z}_s \wr S_N$$

For the groups $\mathbb{Z}_N, D_N$ the computations, done in section 11 above, are not very interesting, with nothing going on with $N \to \infty$. Thus, our plan will be that of reviewing first the computation for S_N, then doing as well the computation for H_N, and then studying the complex reflection groups H_N^s, generalizing S_N, H_N.

Let us first get back to the symmetric group S_N, with a new proof for the character results that we have. We can indeed use the following formula:

Theorem 12.1. *Consider the symmetric group S_N, with its standard coordinates:*

$$g_{ij} = \chi\left(\sigma \in S_N \middle| \sigma(j) = i\right)$$

The products of these coordinates span the algebra $C(S_N)$, and the arbitrary integrals over S_N are given, modulo linearity, by the formula

$$\int_{S_N} g_{i_1 j_1} \ldots g_{i_k j_k} = \begin{cases} \frac{(N - |\ker i|)!}{N!} & \text{if } \ker i = \ker j \\ 0 & \text{otherwise} \end{cases}$$

where $\ker i$ denotes as usual the partition of $\{1, \ldots, k\}$ whose blocks collect the equal indices of i, and where $|.|$ denotes the number of blocks.

Proof. The first assertion follows from the Stone-Weierstrass theorem, because the standard coordinates g_{ij} separate the points of S_N, and so the algebra $< g_{ij} >$ that they generate must be equal to the whole function algebra $C(S_N)$:

$$< g_{ij} >= C(S_N)$$

Regarding now the second assertion, according to the definition of g_{ij}, the integrals in the statement are given by:

$$\int_{S_N} g_{i_1j_1} \ldots g_{i_kj_k} = \frac{1}{N!} \# \left\{ \sigma \in S_N \middle| \sigma(j_1) = i_1, \ldots, \sigma(j_k) = i_k \right\}$$

Now observe that the existence of $\sigma \in S_N$ as above requires:

$$i_m = i_n \iff j_m = j_n$$

Thus, the above integral vanishes when:

$$\ker i \neq \ker j$$

Regarding now the case $\ker i = \ker j$, if we denote by $b \in \{1, \ldots, k\}$ the number of blocks of this partition $\ker i = \ker j$, we have $N - b$ points to be sent bijectively to $N - b$ points, and so $(N - b)!$ solutions, and the integral is $\frac{(N-b)!}{N!}$, as claimed. □

As an illustration for the above formula, we can recover the computation of the asymptotic laws of the truncated characters χ_t. We have indeed:

Theorem 12.2. *For the symmetric group $S_N \subset O_N$, regarded as a compact group of matrices, $S_N \subset O_N$, via the standard permutation matrices, the truncated character*

$$\chi_t(g) = \sum_{i=1}^{[tN]} g_{ii}$$

counts the number of fixed points among $\{1, \ldots, [tN]\}$, and its law with respect to the counting measure becomes, with $N \to \infty$, a Poisson law of parameter t.

Proof. The first assertion comes from the following formula:

$$g_{ij} = \chi \left(\sigma \middle| \sigma(j) = i \right)$$

Regarding now the second assertion, we use the integration formula in Theorem 12.1. With S_{kb} being the Stirling numbers, we have:

$$\begin{aligned}
&\int_{S_N}\chi_t^k\\
&=\sum_{i_1\ldots i_k=1}^{[tN]}\int_{S_N}g_{i_1i_1}\ldots g_{i_ki_k}\\
&=\sum_{\pi\in P(k)}\frac{[tN]!}{([tN]-|\pi|!)}\cdot\frac{(N-|\pi|!)}{N!}\\
&=\sum_{b=1}^{[tN]}\frac{[tN]!}{([tN]-b)!}\cdot\frac{(N-b)!}{N!}\cdot S_{kb}
\end{aligned}$$

In particular with $N\to\infty$ we obtain the following formula:

$$\lim_{N\to\infty}\int_{S_N}\chi_t^k=\sum_{b=1}^{k}S_{kb}t^b$$

But this is the k-th moment of the Poisson law p_t, and so we are done. □

Summarizing, the integration formula in Theorem 12.1 is extremely simple and efficient.

We will regularly use it in what follows, for other questions, to be formulated later.

Finally, as a last topic regarding S_N, here is a useful related formula:

Theorem 12.3. *We have the law formula*

$$\text{law}(g_{11}+\ldots+g_{ss})=\frac{s!}{N!}\sum_{p=0}^{s}\frac{(N-p)!}{(s-p)!}\cdot\frac{(\delta_1-\delta_0)^{*p}}{p!}$$

where g_{ij} are the standard coordinates of $S_N\subset O_N$.

Proof. We have the following moment formula, where m_f is the number of permutations of $\{1,\ldots,N\}$ having exactly f fixed points in the set $\{1,\ldots,s\}$:

$$\int(u_{11}+\ldots+u_{ss})^k=\frac{1}{N!}\sum_{f=0}^{s}m_ff^k$$

Thus the law in the statement, say ν_{sN}, is the following average of Dirac masses:

$$\nu_{sN}=\frac{1}{N!}\sum_{f=0}^{s}m_f\,\delta_f$$

Now observe that the permutations contributing to m_f are obtained by choosing f points in the set $\{1,\ldots,s\}$, then by permuting the remaining $N-f$ points in $\{1,\ldots,n\}$ in such a way that there is no fixed point in $\{1,\ldots,s\}$.

These latter permutations are counted as follows: we start with all permutations, we substract those having one fixed point, we add those having two fixed points, and so on. We obtain:

$$\begin{aligned}
&\nu_{sN}\\
&= \frac{1}{N!}\sum_{f=0}^{s}\binom{s}{f}\left(\sum_{k=0}^{s-f}(-1)^k\binom{s-f}{k}(N-f-k)!\right)\delta_f\\
&= \sum_{f=0}^{s}\sum_{k=0}^{s-f}(-1)^k\frac{1}{N!}\cdot\frac{s!}{f!(s-f)!}\cdot\frac{(s-f)!(N-f-k)!}{k!(s-f-k)!}\,\delta_f\\
&= \frac{s!}{N!}\sum_{f=0}^{s}\sum_{k=0}^{s-f}\frac{(-1)^k(N-f-k)!}{f!k!(s-f-k)!}\,\delta_f
\end{aligned}$$

We can proceed as follows, by using the new index $p=f+k$:

$$\begin{aligned}
&\nu_{sN}\\
&= \frac{s!}{N!}\sum_{p=0}^{s}\sum_{k=0}^{p}\frac{(-1)^k(N-p)!}{(p-k)!k!(s-p)!}\,\delta_{p-k}\\
&= \frac{s!}{N!}\sum_{p=0}^{s}\frac{(N-p)!}{(s-p)!p!}\sum_{k=0}^{p}(-1)^k\binom{p}{k}\,\delta_{p-k}\\
&= \frac{s!}{N!}\sum_{p=0}^{s}\frac{(N-p)!}{(s-p)!}\cdot\frac{(\delta_1-\delta_0)^{*p}}{p!}
\end{aligned}$$

Here $*$ is convolution of real measures, and the assertion follows. □

We can use the above formula, as follows:

Theorem 12.4. *Let g_{ij} be the standard coordinates of $C(S_N)$.*

(1) *$u_{11}+\ldots+u_{ss}$ with $s=o(N)$ is a projection of trace s/N.*
(2) *$u_{11}+\ldots+u_{ss}$ with $s=tN+o(N)$ is Poisson of parameter t.*

Proof. We use the formula in Theorem 12.3 above.

(1) With s fixed and $N\to\infty$ we have the following estimate:

$$\begin{aligned}&\text{law}(u_{11}+\ldots+u_{ss})\\ =\ &\sum_{p=0}^{s}\frac{(N-p)!}{N!}\cdot\frac{s!}{(s-p)!}\cdot\frac{(\delta_1-\delta_0)^{*p}}{p!}\\ =\ &\delta_0+\frac{s}{N}(\delta_1-\delta_0)+O(N^{-2})\end{aligned}$$

But the law on the right is that of a projection of trace s/N, as desired.

(2) We have a law formula of the following type:

$$\text{law}(u_{11}+\ldots+u_{ss})=\sum_{p=0}^{s}c_p\cdot\frac{(\delta_1-\delta_0)^{*p}}{p!}$$

The coefficients c_p can be estimated by using the Stirling formula, as follows:

$$\begin{aligned}&c_p\\ =\ &\frac{(tN)!}{N!}\cdot\frac{(N-p)!}{(tN-p)!}\\ \simeq\ &\frac{(tN)^{tN}}{N^N}\cdot\frac{(N-p)^{N-p}}{(tN-p)^{tN-p}}\\ =\ &\left(\frac{tN}{tN-p}\right)^{tN-p}\left(\frac{N-p}{N}\right)^{N-p}\left(\frac{tN}{N}\right)^{p}\end{aligned}$$

The last expression can be estimated by using the definition of exponentials:

$$\begin{aligned}c_p&\simeq e^pe^{-p}t^p\\ &=t^p\end{aligned}$$

We compute now the Fourier transform with respect to a variable y:

$$\mathcal{F}\left(\text{law}(u_{11}+\ldots+u_{ss})\right)\simeq\sum_{p=0}^{s}t^p\cdot\frac{(e^y-1)^p}{p!}$$

The sum of the series on the right is:

$$S=e^{t(e^y-1)}$$

But this is known to be the Fourier transform of the Poisson law ν_t. This gives the second assertion. □

There are of course many other interesting formulae regarding S_N.

Regarding now the hyperoctahedral group H_N, we have here:

Theorem 12.5. *For the hyperoctahedral group $H_N \subset O_N$, the law of the variable*

$$\chi_t = \sum_{i=1}^{[tN]} g_{ii}$$

is in the $N \to \infty$ limit the measure

$$b_t = e^{-t} \sum_{k=-\infty}^{\infty} \delta_k \sum_{p=0}^{\infty} \frac{(t/2)^{|k|+2p}}{(|k|+p)!p!}$$

where δ_k is the Dirac mass at $k \in \mathbb{Z}$.

Proof. We regard H_N as being the symmetry group of the graph $I_N = \{I^1, \ldots, I^N\}$ formed by N segments. The diagonal coefficients are given by:

$$u_{ii}(g) = \begin{cases} 0 & \text{if } g \text{ moves } I^i \\ 1 & \text{if } g \text{ fixes } I^i \\ -1 & \text{if } g \text{ returns } I^i \end{cases}$$

We denote by $\uparrow g, \downarrow g$ the number of segments among $\{I^1, \ldots, I^s\}$ which are fixed, respectively returned by an element $g \in H_N$. With this notation, we have:

$$u_{11} + \ldots + u_{ss} = \uparrow g - \downarrow g$$

We denote by P_N probabilities computed over the group H_N. The density of the law of $u_{11} + \ldots + u_{ss}$ at a point $k \geq 0$ is given by the following formula:

$$\begin{aligned} & D(k) \\ = \ & P_N(\uparrow g - \downarrow g = k) \\ = \ & \sum_{p=0}^{\infty} P_N(\uparrow g = k + p, \downarrow g = p) \end{aligned}$$

Assume first that we have $t = 1$. We use the fact that the probability of $\sigma \in S_N$ to have no fixed points is asymptotically:

$$P_0 = 1/e$$

Thus the probability of $\sigma \in S_N$ to have m fixed points is asymptotically:

$$P_m = 1/(em!)$$

In terms of probabilities over H_N, we get:

$$\begin{aligned}
&\lim_{N\to\infty} D(k)\\
=\ &\lim_{N\to\infty}\sum_{p=0}^{\infty}(1/2)^{k+2p}\binom{k+2p}{k+p}P_N(\uparrow g+\downarrow g=k+2p)\\
=\ &\sum_{p=0}^{\infty}(1/2)^{k+2p}\binom{k+2p}{k+p}\frac{1}{e(k+2p)!}\\
=\ &\frac{1}{e}\sum_{p=0}^{\infty}\frac{(1/2)^{k+2p}}{(k+p)!p!}
\end{aligned}$$

The general case $0<t\leq 1$ follows by performing some modifications in the above computation. The asymptotic density is computed as follows:

$$\begin{aligned}
\lim_{N\to\infty} D(k) &= \lim_{N\to\infty}\sum_{p=0}^{\infty}(1/2)^{k+2p}\binom{k+2p}{k+p}P_N(\uparrow g+\downarrow g=k+2p)\\
&= \sum_{p=0}^{\infty}(1/2)^{k+2p}\binom{k+2p}{k+p}\frac{t^{k+2p}}{e^t(k+2p)!}\\
&= e^{-t}\sum_{p=0}^{\infty}\frac{(t/2)^{k+2p}}{(k+p)!p!}
\end{aligned}$$

Together with $D(-k)=D(k)$, this gives the formula in the statement. □

The above result is quite interesting, because the densities there are the Bessel functions of the first kind.

Due to this fact, the limiting measures are called Bessel laws:

Definition 12.6. *The Bessel law of parameter $t>0$ is the measure*

$$b_t=e^{-t}\sum_{k=-\infty}^{\infty}\delta_k\, f_k(t/2)$$

with the density being the Bessel function of the first kind:

$$f_k(t)=\sum_{p=0}^{\infty}\frac{t^{|k|+2p}}{(|k|+p)!p!}$$

Let us study now these Bessel laws. We first have the following result:

Theorem 12.7. *The Bessel laws b_t have the property*

$$b_s * b_t = b_{s+t}$$

so they form a truncated one-parameter semigroup with respect to convolution.

Proof. We use the formula in Definition 12.6, namely:

$$b_t = e^{-t} \sum_{k=-\infty}^{\infty} \delta_k \, f_k(t/2)$$

The Fourier transform of this measure is given by:

$$Fb_t(y) = e^{-t} \sum_{k=-\infty}^{\infty} e^{ky} \, f_k(t/2)$$

We compute now the derivative with respect to t:

$$Fb_t(y)' = -Fb_t(y) + \frac{e^{-t}}{2} \sum_{k=-\infty}^{\infty} e^{ky} \, f_k'(t/2)$$

On the other hand, the derivative of f_k with $k \geq 1$ is given by:

$$\begin{aligned}
& f_k'(t) \\
= \; & \sum_{p=0}^{\infty} \frac{(k+2p)t^{k+2p-1}}{(k+p)!p!} \\
= \; & \sum_{p=0}^{\infty} \frac{(k+p)t^{k+2p-1}}{(k+p)!p!} + \sum_{p=0}^{\infty} \frac{p\,t^{k+2p-1}}{(k+p)!p!} \\
= \; & \sum_{p=0}^{\infty} \frac{t^{k+2p-1}}{(k+p-1)!p!} + \sum_{p=1}^{\infty} \frac{t^{k+2p-1}}{(k+p)!(p-1)!} \\
= \; & \sum_{p=0}^{\infty} \frac{t^{(k-1)+2p}}{((k-1)+p)!p!} + \sum_{p=1}^{\infty} \frac{t^{(k+1)+2(p-1)}}{((k+1)+(p-1))!(p-1)!} \\
= \; & f_{k-1}(t) + f_{k+1}(t)
\end{aligned}$$

This computation works in fact for any k, so we get:

$$\begin{aligned} & Fb_t(y)' \\ = \ & -Fb_t(y) + \frac{e^{-t}}{2} \sum_{k=-\infty}^{\infty} e^{ky}(f_{k-1}(t/2) + f_{k+1}(t/2)) \\ = \ & -Fb_t(y) + \frac{e^{-t}}{2} \sum_{k=-\infty}^{\infty} e^{(k+1)y} f_k(t/2) + e^{(k-1)y} f_k(t/2) \\ = \ & -Fb_t(y) + \frac{e^y + e^{-y}}{2} Fb_t(y) \\ = \ & \left(\frac{e^y + e^{-y}}{2} - 1 \right) Fb_t(y) \end{aligned}$$

Thus the log of the Fourier transform is linear in t, and we get the assertion. □

In order to further discuss this, we will need a number of probabilistic preliminaries.

We have the following notion, extending the Poisson limit theory from section 11:

Definition 12.8. *Associated to any compactly supported positive measure ν on $\mathbb{R}$ is the probability measure*

$$p_\nu = \lim_{n \to \infty} \left(\left(1 - \frac{c}{n} \right) \delta_0 + \frac{1}{n} \nu \right)^{*n}$$

where $c = mass(\nu)$, called compound Poisson law.

In what follows we will be interested in the case where ν is discrete, as is for instance the case for $\nu = t\delta_1$ with $t > 0$, which produces the Poisson laws.

We will see that the extension to the case of the uniform measure on the roots of unity of arbitrary order is interesting as well.

The following result allows one to detect compound Poisson laws:

Proposition 12.9. *For a discrete measure, written as*

$$\nu = \sum_{i=1}^{s} c_i \delta_{z_i}$$

with $c_i > 0$ and $z_i \in \mathbb{R}$, we have

$$F_{p_\nu}(y) = \exp \left(\sum_{i=1}^{s} c_i (e^{iyz_i} - 1) \right)$$

where F denotes the Fourier transform.

Proof. Let μ_n be the measure appearing in Definition 12.8, under the convolution signs, namely:

$$\mu_n = \left(1 - \frac{c}{n}\right)\delta_0 + \frac{1}{n}\nu$$

We have the following computation:

$$\begin{aligned} & F_{\mu_n}(y) = \left(1 - \frac{c}{n}\right) + \frac{1}{n}\sum_{i=1}^{s} c_i e^{iyz_i} \\ \implies \quad & F_{\mu_n^{*n}}(y) = \left(\left(1 - \frac{c}{n}\right) + \frac{1}{n}\sum_{i=1}^{s} c_i e^{iyz_i}\right)^n \\ \implies \quad & F_{p_\nu}(y) = \exp\left(\sum_{i=1}^{s} c_i(e^{iyz_i} - 1)\right) \end{aligned}$$

Thus, we have obtained the formula in the statement. □

We have as well the following result, providing an alternative to Definition 12.8:

Theorem 12.10. *For a discrete measure, written as*

$$\nu = \sum_{i=1}^{s} c_i \delta_{z_i}$$

with $c_i > 0$ and $z_i \in \mathbb{R}$, we have

$$p_\nu = \text{law}\left(\sum_{i=1}^{s} z_i \alpha_i\right)$$

where the variables α_i are Poisson (c_i), independent.

Proof. Let α be the sum of Poisson variables in the statement:

$$\alpha = \sum_{i=1}^{s} z_i \alpha_i$$

We will show that the Fourier transform of α is given by the formula in Proposition 12.9.

Indeed, by using some well-known Fourier transform formulae, we have:

$$\begin{aligned} & F_{\alpha_i}(y) = \exp(c_i(e^{iy} - 1)) \\ \implies \quad & F_{z_i\alpha_i}(y) = \exp(c_i(e^{iyz_i} - 1)) \\ \implies \quad & F_\alpha(y) = \exp\left(\sum_{i=1}^{s} c_i(e^{iyz_i} - 1)\right) \end{aligned}$$

Thus we have indeed the same formula as in Proposition 12.9. □

Getting back now to the Bessel laws, we have:

Theorem 12.11. *The Bessel laws b_t are compound Poisson laws, given by*

$$b_t = p_{t\varepsilon}$$

where:

$$\varepsilon = \frac{1}{2}(\delta_{-1} + \delta_1)$$

Proof. This follows indeed by comparing the formula of the Fourier transform of b_t, from the proof of Theorem 12.7 above, with the formula in Proposition 12.9. □

Summarizing, we have a good understanding of H_N, and everything is finally quite similar to what happens for S_N.

Our next task will be that of generalizing the results that we have for S_N, H_N. For this purpose, let us consider the following family of groups:

Definition 12.12. *The complex reflection group $H_N^s \subset U_N$, depending on parameters*

$$N \in \mathbb{N} \quad , \quad s \in \mathbb{N} \cup \{\infty\}$$

are the groups of permutation-type matrices with s-th roots of unity as entries,

$$H_N^s = M_N(\mathbb{Z}_s \cup \{0\}) \cap U_N$$

with the convention $\mathbb{Z}_\infty = \mathbb{T}$, at $s = \infty$.

Observe that at $s = 1, 2$ we obtain S_N, H_N:

$$H_N^1 = S_N$$

$$H_N^2 = H_N$$

Another important particular case is $s = \infty$, where we obtain a group which is actually not finite, denoted as follows:

$$H_N^\infty = K_N$$

In order to do now the character computations for H_N^s, in general, we need a number of further probabilistic preliminaries.

Let us start with:

Definition 12.13. *The Bessel law of level $s \in \mathbb{N} \cup \{\infty\}$ and parameter $t > 0$ is*

$$b_t^s = p_{t\varepsilon_s}$$

with ε_s being the uniform measure on the s-th roots of unity.

Observe that at $s = 1, 2$ we obtain p_t, b_t:

$$b_t^1 = p_t$$

$$b_t^2 = b_t$$

Another important particular case is $s = \infty$, where we obtain a measure which is actually not discrete, denoted as follows:

$$b_t^\infty = B_t$$

As a basic result on these laws, generalizing those about p_t, b_t, we have:

Theorem 12.14. *The generalized Bessel laws b_t^s have the property*

$$b_t^s * b_{t'}^s = b_{t+t'}^s$$

so they form a truncated one-parameter semigroup with respect to convolution.

Proof. This follows indeed from the Fourier transform formulae from Proposition 12.9, because the log of these Fourier transforms are linear in t. □

We will see later some other results regarding these laws.

Regarding now the moments, the result here is as follows:

Theorem 12.15. *The moments of the Bessel law b_t^s are the numbers*

$$M_k = |P^s(k)|$$

where $P^s(k)$ is the set of partitions of $\{1, \ldots, k\}$ satisfying

$$\#\circ = \#\bullet\,(s)$$

as a weighted sum, in each block.

Proof. Observe first that the formula holds indeed at $s = 1$, where $b_t^1 = p_t$ is the Poisson law of parameter $t > 0$, and where $P^1 = P$ is the set of all partitions.

At $s = 2$ we have $P^2 = P_{even}$, and the result is elementary as well.

In general, this follows by doing some combinatorics. □

Summarizing, we have full generalizations of our various results regarding p_t, b_t.

We can go back now to the reflection groups, and we have:

Theorem 12.16. *For the complex reflection group*

$$H_N^s = \mathbb{Z}_s \wr S_N$$

we have, with $N \to \infty$, the estimate

$$\chi_t \sim b_t^s$$

where $b_t^s = p_{t\varepsilon_s}$, with ε_s being the uniform measure on the s-th roots of unity.

Proof. This follows indeed by doing some computations, by using the inclusion-exclusion principle, generalizing those at $s = 1$ for S_N, and at $s = 2$ for H_N. □

Here is now the full theory, from the original papers. First, we have:

Definition 12.17. *The Bessel laws p_{st} and the modified Bessel laws $\tilde{p}_{st}$ with $s \in \mathbb{N}$ are given by*

$$p_{st} = \text{law}\left(\sum_{k=1}^{s} w^k a_k\right)^s$$

$$\tilde{p}_{st} = \text{law}\left(\sum_{k=1}^{s} w^k a_k\right)$$

where $a_1, \ldots, a_s$ are independent random variables, each of them following the Poisson law of parameter t/s, and $w = e^{2\pi i/s}$.

As a first remark, at $s = 1$ we get the Poisson law of parameter t:

$$p_{1t} = \tilde{p}_{1t} = e^{-t} \sum_{r=0}^{\infty} \frac{t^r}{r!}\, \delta_r$$

In what follows we present a number of results, which show that $p_{st}, \tilde{p}_{st}$ are indeed the classical analogues of $\pi_{st}, \tilde{\pi}_{st}$, for any $s \in \mathbb{N}$.

We discuss now the additivity property and the Poisson limit convergence for Bessel laws. We use the level s exponential function:

$$\exp_s z = \sum_{k=0}^{\infty} \frac{z^{sk}}{(sk)!}$$

We have the following formula, in terms of $w = e^{2\pi i/s}$:

$$\exp_s z = \frac{1}{s} \sum_{k=1}^{s} \exp(w^k z)$$

Observe that we have $\exp_1 = \exp$ and $\exp_2 = \cosh$. We have:

Theorem 12.18. *The Fourier transform of $\tilde{p}_{st}$ is given by*

$$\log \tilde{F}_{st}(z) = t\,(\exp_s z - 1)$$

so in particular the measures $\tilde{p}_{st}$ are additive with respect to t.

Proof. Consider the following variable:

$$a = \sum w^k a_k$$

For the Poisson law of parameter t we have:

$$\log F(z) = t(e^z - 1)$$

We use now the following identity:

$$F_{qa}(z) = F_a(qz)$$

We obtain in this way:

$$\begin{aligned}\log F_a(z) &= \sum_{k=1}^{s} \log F_{a_k}(w^k z)\\ &= \sum_{k=1}^{s} \frac{t}{s}\left(\exp(w^k z) - 1\right)\end{aligned}$$

This gives the following formula:

$$\begin{aligned}\log F_a(z) &= t\left(\left(\frac{1}{s}\sum_{k=1}^{s}\exp(w^k z)\right) - 1\right)\\ &= t\left(\exp_s(z) - 1\right)\end{aligned}$$

Now since $\tilde{p}_{st}$ is the law of a, this gives the formula in the statement. □

Next, we have the following result:

Theorem 12.19. *We have the Poisson limit type convergence*

$$\left(\left(1 - \frac{1}{n}\right)\delta_0 + \frac{1}{n}\,\rho\right)^{*n} \to \tilde{p}_{s1}$$

where ρ is the uniform measure on the s-roots of unity.

Proof. We compute first the Fourier transform of the measure on the left:

$$\begin{aligned}\mu &= \left(1 - \frac{1}{n}\right)\delta_0 + \frac{1}{n}\,\rho\\ \implies F &= \left(1 - \frac{1}{n}\right) + \frac{1}{n}\exp_s(z)\end{aligned}$$

This shows that the Fourier transform of μ^{*n} is given by:

$$\begin{aligned} F &= \left(\left(1-\frac{1}{n}\right)+\frac{1}{n}\exp_s(z)\right)^n \\ &= \left(1+\frac{\exp_s(z)-1}{n}\right)^n \\ &\simeq \exp(\exp_s(z)-1) \end{aligned}$$

Thus in the limit $n\to\infty$ we have:

$$\log F=\exp_s z-1$$

But this gives the result. □

We study now the densities of $p_{st},\tilde{p}_{st}$. At $s=2$ this will lead to Bessel functions, which will justify the terminology. We first have:

Theorem 12.20. *We have the formulae*

$$p_{st}=e^{-t}\sum_{p_1=0}^{\infty}\cdots\sum_{p_s=0}^{\infty}\frac{1}{p_1!\ldots p_s!}\left(\frac{t}{s}\right)^{p_1+\ldots+p_s}\delta\left(\sum_{k=1}^{s}w^kp_k\right)^s$$

$$\tilde{p}_{st}=e^{-t}\sum_{p_1=0}^{\infty}\cdots\sum_{p_s=0}^{\infty}\frac{1}{p_1!\ldots p_s!}\left(\frac{t}{s}\right)^{p_1+\ldots+p_s}\delta\left(\sum_{k=1}^{s}w^kp_k\right)$$

where $w=e^{2\pi i/s}$, and the δ symbol is a Dirac mass.

Proof. It is enough to prove the formula for $\tilde{p}_{st}$. For this purpose, we compute the Fourier transform of the measure on the right. This is given by:

$$\begin{aligned} & F(z) \\ = \;& e^{-t}\sum_{p_1=0}^{\infty}\cdots\sum_{p_s=0}^{\infty}\frac{1}{p_1!\ldots p_s!}\left(\frac{t}{s}\right)^{p_1+\ldots+p_s}F\delta\left(\sum_{k=1}^{s}w^kp_k\right)(z) \\ = \;& e^{-t}\sum_{p_1=0}^{\infty}\cdots\sum_{p_s=0}^{\infty}\frac{1}{p_1!\ldots p_s!}\left(\frac{t}{s}\right)^{p_1+\ldots+p_s}\exp\left(\sum_{k=1}^{s}w^kp_kz\right) \\ = \;& e^{-t}\sum_{r=0}^{\infty}\left(\frac{t}{s}\right)^r\sum_{\Sigma p_i=r}\frac{\exp\left(\sum_{k=1}^{s}w^kp_kz\right)}{p_1!\ldots p_s!} \end{aligned}$$

We multiply by e^t, and we compute the derivative with respect to t:

$$\begin{aligned}
&(e^tF(z))'\\
=\ &\sum_{r=1}^{\infty}\frac{r}{s}\left(\frac{t}{s}\right)^{r-1}\sum_{\Sigma p_i=r}\frac{\exp\left(\sum_{k=1}^s w^kp_kz\right)}{p_1!\ldots p_s!}\\
=\ &\frac{1}{s}\sum_{r=1}^{\infty}\left(\frac{t}{s}\right)^{r-1}\sum_{\Sigma p_i=r}\left(\sum_{l=1}^s p_l\right)\frac{\exp\left(\sum_{k=1}^s w^kp_kz\right)}{p_1!\ldots p_s!}\\
=\ &\frac{1}{s}\sum_{r=1}^{\infty}\left(\frac{t}{s}\right)^{r-1}\sum_{\Sigma p_i=r}\sum_{l=1}^s\frac{\exp\left(\sum_{k=1}^s w^kp_kz\right)}{p_1!\ldots p_{l-1}!(p_l-1)!p_{l+1}!\ldots p_s!}
\end{aligned}$$

By using the variable $u=r-1$, we get:

$$\begin{aligned}
&(e^tF(z))'\\
=\ &\frac{1}{s}\sum_{u=0}^{\infty}\left(\frac{t}{s}\right)^{u}\sum_{\Sigma q_i=u}\sum_{l=1}^s\frac{\exp\left(w^lz+\sum_{k=1}^s w^kq_kz\right)}{q_1!\ldots q_s!}\\
=\ &\left(\frac{1}{s}\sum_{l=1}^s\exp(w^lz)\right)\left(\sum_{u=0}^{\infty}\left(\frac{t}{s}\right)^{u}\sum_{\Sigma q_i=u}\frac{\exp\left(\sum_{k=1}^s w^kq_kz\right)}{q_1!\ldots q_s!}\right)\\
=\ &(\exp_s z)(e^t\tilde{F}_{st}(z))
\end{aligned}$$

On the other hand, consider the function:

$$\Phi(t)=\exp(t\exp_s z)$$

This function satisfies as well the equation:

$$\Phi'(t)=(\exp_s z)\Phi(t)$$

Thus we have:

$$e^tF(z)=\Phi(t)$$

But this gives:

$$\begin{aligned}
&\log F\\
=\ &\log(e^{-t}\exp(t\exp_s z))\\
=\ &\log(\exp(t(\exp_s z-1)))\\
=\ &t(\exp_s z-1)
\end{aligned}$$

This gives the formulae in the statement. □

Recall now that the Bessel function of the first kind is given by:

$$\varphi_r(t)=\sum_{p=0}^{\infty}\frac{t^{2p+r}}{p!(p+r)!}$$

The following result justifies the terminology used here:

Theorem 12.21. *We have the formulae*

$$p_{2t}=e^{-t}\sum_{r=-\infty}^{\infty}\varphi_{|r|}\left(\frac{t}{2}\right)\delta_{r^2}$$

$$\tilde{p}_{2t}=e^{-t}\sum_{r=-\infty}^{\infty}\varphi_{|r|}\left(\frac{t}{2}\right)\delta_{r}$$

where φ_r is the Bessel function of the first kind.

Proof. At $s=2$ the primitive root of unity is $w=-1$, and we get:

$$\begin{aligned}
&\tilde{p}_{2t}\\
=\;&e^{-t}\sum_{p=0}^{\infty}\sum_{q=0}^{\infty}\frac{(t/2)^{p+q}}{p!q!}\,\delta_{p-q}\\
=\;&e^{-t}\sum_{r=-\infty}^{\infty}\sum_{p-q=r}\frac{(t/2)^{p+q}}{p!q!}\,\delta_r\\
=\;&e^{-t}\left(\sum_{r=0}^{\infty}\sum_{q=0}^{\infty}\frac{(t/2)^{r+2q}}{(r+q)!q!}\delta_r+\sum_{r=-\infty}^{-1}\sum_{p=0}^{\infty}\frac{(t/2)^{2p-r}}{p!(p-r)!}\delta_r\right)
\end{aligned}$$

Thus the density of $\tilde{p}_{2t}$ is given indeed by the Bessel function:

$$\begin{aligned}
&\tilde{p}_{2t}\\
=\;&e^{-t}\left(\sum_{r=0}^{\infty}\sum_{q=0}^{\infty}\frac{(t/2)^{r+2q}}{(r+q)!q!}\delta_r+\sum_{r=-\infty}^{-1}\sum_{p=0}^{\infty}\frac{(t/2)^{2p+|r|}}{p!(p+|r|)!}\delta_r\right)\\
=\;&e^{-t}\sum_{r=-\infty}^{\infty}\sum_{p=0}^{\infty}\frac{(t/2)^{|r|+2p}}{(|r|+p)!p!}\,\delta_r
\end{aligned}$$

This gives the formulae in the statement. □

We know that p_{1t},p_{2t} are supported by $\mathbb{N},\mathbb{Z}$. In the general case the situation is a bit more complicated: the support is formed by the s powers of certain elements in $\mathbb{Z}[w]$, so we can only say that it is contained in $\mathbb{Z}[w]$.

As for the density, this should be thought of as being a kind of s-dimensional Bessel function.

We have the following result:

Theorem 12.22. *For H_n^s with $n \to \infty$ we have:*

$$\text{law}(\chi_t) \to \tilde{p}_{st}$$

Proof. We work out first the case $t = 1$. Since the limit probability for a random permutation to have exactly k fixed points is $e^{-1}/k!$, we get:

$$\lim_{n\to\infty} \text{law}(\chi_1) = e^{-1} \sum_{k=0}^{\infty} \frac{1}{k!} \rho^{*k}$$

On the other hand, we have:

$$\begin{aligned}
& \tilde{p}_{s1} \\
= \ & \lim_{n\to\infty} \left(\left(1 - \frac{1}{n}\right) \delta_0 + \frac{1}{n} \rho \right)^{*n} \\
= \ & \lim_{n\to\infty} \sum_{k=0}^{n} \binom{n}{k} \left(1 - \frac{1}{n}\right)^{n-k} \frac{1}{n^k} \rho^{*k} \\
= \ & e^{-1} \sum_{k=0}^{\infty} \frac{1}{k!} \rho^{*k}
\end{aligned}$$

This gives the assertion for $t = 1$. Now in the case $t > 0$ arbitrary, we can use the same method, by performing the following modifications:

$$\begin{aligned}
& \lim_{n\to\infty} \text{law}(\chi_t) \\
= \ & e^{-t} \sum_{k=0}^{\infty} \frac{t^k}{k!} \rho^{*k} \\
= \ & \lim_{n\to\infty} \left(\left(1 - \frac{1}{n}\right) \delta_0 + \frac{1}{n} \rho \right)^{*[tn]} \\
= \ & \tilde{p}_{st}
\end{aligned}$$

This finishes the proof. □

Finally, we have the general series of complex reflection groups H_N^{sd}. Here the determinant does not really contribute, in the $N \to \infty$ limit.

13. Representations

We have seen so far some interesting theory for the finite subgroups $G \subset U_N$. We discuss in what follows the case of the arbitrary closed subgroups $G \subset U_N$. The main examples that we have in mind are the orthogonal and unitary groups O_N, U_N.

We will be interested as well in other continuous groups, such as the bistochastic groups B_N, C_N, and the symplectic groups Sp_N.

Also, we have of course as examples the various finite groups $G \subset U_N$, and in particular the following groups:

$$\mathbb{Z}_N \subset D_N \subset S_N \subset H_N^s$$

There are of course many other examples.

There is a lot of theory to be developed, and we will do this gradually.

The main notion that we will be interested in is that of a representation:

Definition 13.1. *A representation of a closed subgroup*

$$G \subset U_N$$

is a continuous group morphism into a unitary group:

$$\rho : G \to U_n$$

The character of such a representation is the function

$$\chi : G \to \mathbb{C}$$

$$\chi(g) = Tr(\rho(g))$$

where Tr is the usual trace of the $n \times n$ matrices.

As a basic example, we have the fundamental representation:

$$\pi : G \subset U_N$$

Another basic example is the trivial representation:

$$1 : G \to U_1$$

We will see in a moment that there are many other examples.

Observe that the characters are central functions, in the sense that they satisfy the following condition:

$$\chi(gh) = \chi(hg)$$

We will be back to this, with a result stating that any smooth central function on our group G is a linear combination of characters.

We have the following operations on the representations:

Proposition 13.2. *The representations are subject to the following operations:*

(1) *Making sums:*

$$\rho+\nu=diag(\rho,\nu)$$

(2) *Making tensor products:*

$$(\rho\otimes\nu)_{ia,jb}=\rho_{ij}\nu_{ab}$$

(3) *Taking conjugates:*

$$(\bar{\rho})_{ij}=\bar{\rho}_{ij}$$

(4) *Spinning by unitaries:*

$$\rho\to U\rho U^*$$

Proof. All the assertions are elementary:

(1) This follows from the fact that if U,V are unitaries, then so is:

$$diag(U,V)$$

(2) This follows from the fact that if U,V are unitaries, then so is:

$$U\otimes V$$

(3) This follows from the fact that if U is unitary, then so is:

$$\bar{U}$$

(4) This follows from the fact that if U,V are unitaries, then so is:

$$UVU^*$$

Thus, we have proved the result. □

By using the above constructions, we can construct a whole family of representations, starting with the fundamental one $\pi:G\subset U_N$, as follows:

Definition 13.3. *We denote by $\pi^{\otimes k}$, with $k=\circ\bullet\bullet\circ\ldots$ being a colored integer, the various tensor products between $\pi,\bar{\pi}$, indexed according to the rules*

$$\pi^{\otimes\emptyset}=1$$

$$\pi^{\otimes\circ}=\pi$$

$$\pi^{\otimes\bullet}=\bar{u}$$

and multiplicativity,

$$\pi^{\otimes kl}=\pi^{\otimes k}\otimes\pi^{\otimes l}$$

and call them Peter-Weyl representations.

Here are a few examples of such representations, namely those coming from the colored integers of length 2, to be often used in what follows:

$$\pi^{\otimes\circ\circ} = \pi \otimes \pi$$

$$\pi^{\otimes\circ\bullet} = \pi \otimes \bar{\pi}$$

$$\pi^{\otimes\bullet\circ} = \bar{\pi} \otimes \pi$$

$$\pi^{\otimes\bullet\bullet} = \bar{\pi} \otimes \bar{\pi}$$

Observe that, since the tensor product of representations is commutative, we have:

$$\pi^{\otimes\circ\bullet} = \pi^{\otimes\bullet\circ}$$

Thus we can replace if we want our colored integers $k \in \mathbb{N} * \mathbb{N}$ by colored integers $k \in \mathbb{N} \times \mathbb{N}$, by moving all $\circ$ components to the left. We will not need this.

In relation now with characters, we have the following result:

Theorem 13.4. *We have the following formulae, regarding characters:*

(1) $\chi_{\rho+\nu} = \chi_\rho + \chi_\nu$.
(2) $\chi_{\rho\otimes\nu} = \chi_\rho\chi_\nu$.
(3) $\chi_{\bar{\rho}} = \bar{\chi}_\rho$.
(4) $\chi_{U\rho U^*} = \chi_\rho$.

In particular, for the Peter-Weyl representations we have:

$$\chi_{\pi^{\otimes k}} = \chi_\pi^k$$

Proof. All these assertions are elementary:

(1) This follows from the fact that if U, V are unitaries, then:

$$Tr(diag(U, V)) = Tr(U) + Tr(V)$$

(2) This follows from the fact that if U, V are unitaries, then:

$$Tr(U \otimes V) = Tr(U)Tr(V)$$

(3) This follows from the fact that if U is unitary, then:

$$Tr(\bar{U}) = \overline{Tr(U)}$$

(4) This follows from the fact that if U, V are unitaries, then:

$$Tr(UVU^*) = Tr(V)$$

Finally, the last assertion is clear from (2,3). □

In order to understand the structure of the representations of a given closed subgroup $G \subset U_N$, we must develop some abstract theory. Let us start with:

Definition 13.5. *Given two representations $\rho : G \to U_n, \nu : G \to U_m$, we set*

$$Hom(\rho, \nu) = \left\{T \in M_{m\times n}(\mathbb{C})\Big|T\rho(g) = \nu(g)T\right\}$$

and we use the following conventions:

(1) *We use the notations $Fix(\rho) = Hom(1, \rho)$, and $End(\rho) = Hom(\rho, \rho)$.*
(2) *We write $\rho \sim \nu$ when $Hom(\rho, \nu)$ contains an invertible element.*
(3) *We say that ρ is irreducible, and write $\rho \in Irr(G)$, when $End(\rho) = \mathbb{C}1$.*

The terminology here is standard, with Hom and End standing respectively for "homomorphisms" and "endomorphisms".

Here are now a few basic results, regarding the above Hom spaces:

Proposition 13.6. *We have the following results:*

(1) $T \in Hom(\rho, \nu), S \in Hom(\nu, \eta) \implies ST \in Hom(\rho, \eta)$.
(2) $S \in Hom(\rho, \nu), T \in Hom(\eta, \sigma) \implies S \otimes T \in Hom(\rho \otimes \eta, \nu \otimes \sigma)$.
(3) $T \in Hom(\rho, \nu) \implies T^* \in Hom(\nu, \rho)$.

In other words, the Hom spaces form a tensor $*$-category.

Proof. All the assertions are clear from definitions. □

We will be back to tensor categories later on, in sections 14 and 15 below.

As a main consequence of the above result, the spaces $End(\rho) \subset M_n(\mathbb{C})$ are unital subalgebras stable under the involution $*$, and so are C^*-algebras.

In order to exploit this fact, we will need a basic result, complementing the operator algebra theory developed in section 7 above, namely:

Theorem 13.7. *Let $A \subset M_n(\mathbb{C})$ be a C^*-algebra.*

(1) *We can write $1 = q_1 + \ldots + q_k$, with $q_i \in A$ central minimal projections.*
(2) *Each of the linear spaces $A_i = q_iAq_i$ is a non-unital $*$-subalgebra of A.*
(3) *We have a non-unital $*$-algebra sum decomposition $A = A_1 \oplus \ldots \oplus A_k$.*
(4) *We have unital $*$-algebra isomorphisms $A_i \simeq M_{r_i}(\mathbb{C})$, where $r_i = rank(q_i)$.*
(5) *Thus, we have a C^*-algebra isomorphism $A \simeq M_{r_1}(\mathbb{C}) \oplus \ldots \oplus M_{r_k}(\mathbb{C})$.*

Proof. This is something well-known, with the proof of the assertions (1,2,3,4,5) in the statement being something elementary, and routine:

(1) This is rather a definition.

(2) This is something clear.

(3) The direct sum conditions are indeed easy to check.

(4) This comes from the fact that each q_i was chosen central minimal.

(5) This follows from (3,4). □

We can now formulate our first Peter-Weyl type theorem, as follows:

Theorem 13.8. *Let $\rho : G \to U_n$ be a representation, consider the C^*-algebra $A = End(\rho)$, and write its unit as $1 = q_1 + \ldots + q_k$, as above. We have then*

$$\rho = \rho_1 + \ldots + \rho_k$$

with each ρ_i being an irreducible representation, obtained by restricting ρ to $Im(q_i)$.

Proof. This can be deduced by using Theorem 13.7 above, as follows:

(1) We first associate to our representation $\rho : G \to U_n$ the corresponding action map on $\mathbb{C}^n$. If a linear subspace $V \subset \mathbb{C}^n$ is invariant, the restriction of the action map to V is an action map too, which must come from a subrepresentation $\nu \subset \rho$.

(2) Consider now a projection $q \in End(\rho)$. From $q\rho = \rho q$ we obtain that the linear space $V = Im(q)$ is invariant under ρ, and so this space must come from a subrepresentation $\nu \subset \rho$. It is routine to check that the operation $q \to \nu$ maps subprojections to subrepresentations, and minimal projections to irreducible representations.

(3) With these preliminaries in hand, let us decompose the algebra $End(\rho)$ as in Theorem 13.7 above, by using the decomposition $1 = q_1 + \ldots + q_k$ into minimal projections. If we denote by $\rho_i \subset \rho$ the subrepresentation coming from the vector space $V_i = Im(q_i)$, then we obtain in this way a decomposition $\rho = \rho_1 + \ldots + \rho_k$, as in the statement. □

In order to formulate our second Peter-Weyl theorem, we need to talk about coefficients, and smoothness. Things here are quite tricky, and best is to proceed as follows:

Definition 13.9. *Given a representation $\rho : G \to U_n$, its space of coefficients is:*

$$C_\rho = \left\{ f \circ \rho \middle| f \in M_n(\mathbb{C})^* \right\}$$

In other words, by delinearizing, $C_\rho \subset C(G)$ is the following linear space:

$$C_\rho = span\left[g \to \rho(g)_{ij} \right]$$

We say that ρ is smooth if its matrix coefficients $g \to \rho(g)_{ij}$ appear as polynomials in the standard matrix coordinates $g \to g_{ij}$, and their conjugates $g \to \overline{g}_{ij}$.

As a basic example of coefficient we have, besides the matrix coefficients $g \to \rho(g)_{ij}$, the character, which appears as the diagonal sum of these coefficients:

$$\chi(g) = \sum_i \rho(g)_{ii}$$

Regarding the notion of smoothness, things are quite tricky here, the idea being that any closed subgroup $G \subset U_N$ can be shown to be a Lie group, and that, with this result in hand, a representation $\rho : G \to U_n$ is smooth precisely when the condition on coefficients

from the above definition is satisfied. All this is quite technical, and we will not get into it. We will simply use Definition 13.9 as such, and further comment on this later on.

Here is now our second Peter-Weyl theorem, complementing Theorem 13.8:

Theorem 13.10. *Each irreducible smooth representation $\rho : G \to U_n$ appears inside a tensor product of the fundamental representation π and its adjoint $\bar{\pi}$.*

Proof. Given an arbitrary representation $\rho : G \to U_n$, consider its space of coefficients, as in Definition 10.9 above:

$$C_\rho = span\Big[g \to \rho(g)_{ij}\Big]$$

In order to prove the result, we will use the following three elementary facts, regarding these spaces of coefficients:

(1) The construction $\rho \to C_\rho$ is functorial, in the sense that it maps subrepresentations into linear subspaces. This is indeed something which is routine to check.

(2) Our smoothness assumption on $\rho : G \to U_n$, as formulated in Definition 13.9, means that we have an inclusion of linear spaces as follows:

$$C_\rho \subset < g_{ij} >$$

(3) By definition of the Peter-Weyl representations, as arbitrary tensor products between the fundamental representation π and its conjugate $\bar{\pi}$, we have:

$$< g_{ij} >= \sum_k C_{\pi^{\otimes k}}$$

Now by putting together (2,3) we conclude that we must have an inclusion as follows, for certain exponents $k_1, \ldots, k_p$:

$$C_\rho \subset C_{\pi^{\otimes k_1} \oplus \ldots \oplus \pi^{\otimes k_p}}$$

By using now the functoriality result from (1), we deduce from this that we have an inclusion of representations, as follows:

$$\rho \subset \pi^{\otimes k_1} \oplus \ldots \oplus \pi^{\otimes k_p}$$

Together with Theorem 13.8, this leads to the conclusion in the statement. □

We will be back to Peter-Weyl theory after a short break.

In order to further advance, indeed, with some finer results, we need to integrate over G. This is something quite technical, the idea being that the uniform measure μ over G can be constructed by starting with an arbitrary probability measure ν, and setting:

$$\mu = \lim_{n \to \infty} \frac{1}{n} \sum_{k=1}^{n} \nu^{*k}$$

Thus, our next task will be that of proving this result. Note that this is something that we need only in the continuous case, because when the group G is finite the uniform measure is simply the counting measure, rescaled by $1/|G|$, as to have mass 1.

In short, we have to do now some technical functional analysis.

It is convenient, for this purpose, to work with the integration functionals with respect to the various measures on G, instead of the measures themselves.

Let us begin with the following key result:

Proposition 13.11. *Given a unital positive linear form $\varphi : C(G) \to \mathbb{C}$, the limit*

$$\int_\varphi f = \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \varphi^{*k}(f)$$

exists, and for a coefficient of a representation

$$f = (\tau \otimes id)\rho$$

we have the formula

$$\int_\varphi f = \tau(P)$$

where P is the orthogonal projection onto the 1-eigenspace of $(id \otimes \varphi)\rho$.

Proof. By linearity and continuity, it is enough to prove the first assertion for elements of the following type, where v is one of the Peter-Weyl corepresentations, and τ is a linear form:

$$a = (\tau \otimes id)v$$

Thus we are led into the second assertion, and more precisely we can have the whole result proved if we can establish the following formula, with $a = (\tau \otimes id)v$:

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \varphi^{*k}(a) = \tau(P)$$

In order to prove this latter formula, observe that we have:

$$\begin{aligned} \varphi^{*k}(a) &= (\tau \otimes \varphi^{*k})v \\ &= \tau((id \otimes \varphi^{*k})v) \end{aligned}$$

Consider now the following matrix:

$$M = (id \otimes \varphi)v$$

In terms of this matrix, we have the following formula:

$$\begin{aligned}&((id\otimes\varphi^{*k})v)_{i_0i_{k+1}}\\ =\ &\sum_{i_1\ldots i_k}M_{i_0i_1}\ldots M_{i_ki_{k+1}}\\ =\ &(M^k)_{i_0i_{k+1}}\end{aligned}$$

Thus we have, for any $k\in\mathbb{N}$:

$$(id\otimes\varphi^{*k})v=M^k$$

It follows that our Cesàro limit is given by:

$$\begin{aligned}&\lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{n}\varphi^{*k}(a)\\ =\ &\lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{n}\tau(M^k)\\ =\ &\tau\left(\lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{n}M^k\right)\end{aligned}$$

Now since v is unitary we have $||v||=1$, and so:

$$||M||\leq 1$$

Thus the Cesàro limit on the right converges, and equals the orthogonal projection onto the 1-eigenspace of M:

$$\lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{n}M^k=P$$

Thus our initial Cesàro limit converges as well, to $\tau(P)$, as desired. □

When φ is chosen faithful, we have the following finer result:

Proposition 13.12. *Given a faithful unital linear form $\varphi\in A^*$, the limit*

$$\int_\varphi a=\lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{n}\varphi^{*k}(a)$$

exists, and is independent of φ, given on coefficients of corepresentations by

$$\left(id\otimes\int_\varphi\right)v=P$$

where P is the orthogonal projection onto $Fix(v)=\{\xi\in\mathbb{C}^n|v\xi=\xi\}$.

Proof. In view of Proposition 13.11, it remains to prove that when φ is faithful, the 1-eigenspace of $M = (id \otimes \varphi)v$ equals the following fixed point space:

$$Fix(v) = \left\{\xi \in \mathbb{C}^n \middle| v\xi = \xi\right\}$$

"$\supset$" This is clear, and for any φ, because we have:

$$v\xi = \xi \implies M\xi = \xi$$

"$\subset$" Here we must prove that, when φ is faithful, we have:

$$M\xi = \xi \implies v\xi = \xi$$

For this purpose, assume that we have $M\xi = \xi$, and consider the following element:

$$a = \sum_i \left(\sum_j v_{ij}\xi_j - \xi_i\right)\left(\sum_k v_{ik}\xi_k - \xi_i\right)^*$$

We must prove that we have $a = 0$. Since v is biunitary, we have:

$$\begin{aligned}
& a \\
= & \sum_i \left(\sum_j \left(v_{ij}\xi_j - \frac{1}{N}\xi_i\right)\right)\left(\sum_k \left(v_{ik}^*\bar{\xi}_k - \frac{1}{N}\bar{\xi}_i\right)\right) \\
= & \sum_{ijk} v_{ij}v_{ik}^*\xi_j\bar{\xi}_k - \frac{1}{N}v_{ij}\xi_j\bar{\xi}_i - \frac{1}{N}v_{ik}^*\xi_i\bar{\xi}_k + \frac{1}{N^2}\xi_i\bar{\xi}_i \\
= & \sum_j |\xi_j|^2 - \sum_{ij} v_{ij}\xi_j\bar{\xi}_i - \sum_{ik} v_{ik}^*\xi_i\bar{\xi}_k + \sum_i |\xi_i|^2 \\
= & ||\xi||^2 - < v\xi, \xi > - \overline{< v\xi, \xi >} + ||\xi||^2 \\
= & 2(||\xi||^2 - Re(< v\xi, \xi >))
\end{aligned}$$

By using now our assumption $M\xi = \xi$, we obtain from this:

$$\begin{aligned}
& \varphi(a) \\
= & 2\varphi(||\xi||^2 - Re(< v\xi, \xi >)) \\
= & 2(||\xi||^2 - Re(< M\xi, \xi >)) \\
= & 2(||\xi||^2 - ||\xi||^2) \\
= & 0
\end{aligned}$$

Now since φ is faithful, this gives $a = 0$, and so $v\xi = \xi$, as claimed. □

We can now formulate a main result, as follows:

Theorem 13.13. *Any compact group has a unique Haar integration, which can be constructed by starting with any faithful positive unital state $\varphi \in A^*$, and setting*

$$\int_G = \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \varphi^{*k}$$

where $\phi * \psi = (\phi \otimes \psi)\Delta$. Moreover, for any representation v we have

$$\left(id \otimes \int_G\right) v = P$$

where P is the orthogonal projection onto $Fix(v) = \{\xi \in \mathbb{C}^n | v\xi = \xi\}$.

Proof. Let us first go back to the general context of Proposition 13.11 above. Since convolving one more time with φ will not change the Cesàro limit appearing there, the functional $\int_\varphi \in A^*$ constructed there has the following invariance property:

$$\int_\varphi *\varphi = \varphi * \int_\varphi = \int_\varphi$$

In the case where φ is assumed to be faithful, as in Proposition 13.12 above, our claim is that we have the following formula, valid this time for any $\psi \in A^*$:

$$\int_\varphi *\psi = \psi * \int_\varphi = \psi(1) \int_\varphi$$

It is enough to prove this formula on a coefficient of a corepresentation:

$$a = (\tau \otimes id)v$$

In order to do so, let us set:

$$P = (id \otimes \int_\varphi)v$$

$$Q = (id \otimes \psi)v$$

We have then:

$$\begin{aligned}\left(\int_\varphi *\psi\right) a &= \left(\tau \otimes \int_\varphi \otimes \psi\right)(v_{12}v_{13}) \\ &= \tau(PQ)\end{aligned}$$

Similarly, we have the following computation:

$$\begin{aligned}\left(\psi * \int_\varphi\right) a &= \left(\tau \otimes \psi \otimes \int_\varphi\right)(v_{12}v_{13}) \\ &= \tau(QP)\end{aligned}$$

Finally, regarding the term on the right, this is given by:

$$\psi(1)\int_\varphi a=\psi(1)\tau(P)$$

Thus, our claim is equivalent to the following equality:

$$PQ=QP=\psi(1)P$$

But this latter equality follows from the fact, coming from Proposition 13.12 above, that $P=(id\otimes\int_\varphi)v$ equals the orthogonal projection onto:

$$Fix(v)=\left\{\xi\in\mathbb{C}^n\Big|v\xi=\xi\right\}$$

Thus, we have proved our claim. Now observe that our formula can be written as:

$$\begin{aligned}\psi\left(\int_\varphi\otimes id\right)\Delta&=\psi\left(id\otimes\int_\varphi\right)\Delta\\&=\psi\int_\varphi(.)1\end{aligned}$$

This formula being true for any $\psi\in A^*$, we can simply delete ψ, and we conclude that the invariance formula holds indeed, with:

$$\int_G=\int_\varphi$$

Finally, assuming that we have two invariant integrals $\int_G,\int'_G$, we have:

$$\begin{aligned}\left(\int_G\otimes\int'_G\right)\Delta&=\left(\int'_G\otimes\int_G\right)\Delta\\&=\int_G(.)1\\&=\int'_G(.)1\end{aligned}$$

Thus we have $\int_G=\int'_G$, and this finishes the proof. □

Summarizing, we can now integrate over G.

In order to further develop the Peter-Weyl theory, we will need the following result, which is of independent interest:

Proposition 13.14. *We have a Frobenius type isomorphism*

$$Hom(v,w)\simeq Fix(v\otimes\bar{w})$$

valid for any two corepresentations v,w.

Proof. According to the definitions, we have the following equivalences:

$$\begin{aligned} & T \in Hom(v, w) \\ \iff \quad & Tv = wT \\ \iff \quad & \sum_j T_{aj} v_{ji} = \sum_b w_{ab} T_{bi}, \forall a, i \end{aligned}$$

On the other hand, we have as well the following equivalences:

$$\begin{aligned} & T \in Fix(v \otimes \bar{w}) \\ \iff \quad & (v \otimes \bar{w})T = \xi \\ \iff \quad & \sum_{jb} v_{ij} w_{ab}^* T_{bj} = T_{ai} \forall a, i \end{aligned}$$

With these formulae in hand, both inclusions follow from the biunitarity of v, w. □

We can now formulate our third Peter-Weyl theorem, as follows:

Theorem 13.15. *The dense subalgebra $\mathcal{A} \subset A$ decomposes as a direct sum*

$$\mathcal{A} = \bigoplus_{v \in Irr(A)} M_{\dim(v)}(\mathbb{C})$$

with this being an isomorphism of $*$-coalgebras, and with the summands being pairwise orthogonal with respect to the scalar product given by

$$< a, b >= \int_G ab^*$$

where $\int_G$ is the Haar integration over G.

Proof. By combining the previous two Peter-Weyl results, we deduce that we have a linear space decomposition as follows:

$$\begin{aligned} \mathcal{A} &= \sum_{v \in Irr(A)} C_v \\ &= \sum_{v \in Irr(A)} M_{\dim(v)}(\mathbb{C}) \end{aligned}$$

Thus, in order to conclude, it is enough to prove that for any two irreducible corepresentations $v, w \in Irr(A)$, the corresponding spaces of coefficients are orthogonal:

$$v \not\sim w \implies C_v \perp C_w$$

But this follows from Theorem 13.13, via Proposition 13.14. Let us set indeed:

$$P_{ia,jb} = \int_G v_{ij} w_{ab}^*$$

Then P is the orthogonal projection onto the following vector space:

$$\begin{aligned} Fix(v \otimes \bar{w}) &\simeq Hom(v, w) \\ &= \{0\} \end{aligned}$$

Thus we have $P = 0$, and this gives the result. □

Finally, we have the following result, completing the Peter-Weyl theory:

Theorem 13.16. *The characters of irreducible corepresentations belong to the algebra*

$$\mathcal{A}_{central} = \left\{ a \in \mathcal{A} \middle| \Sigma\Delta(a) = \Delta(a) \right\}$$

of "smooth central functions" on G, and form an orthonormal basis of it.

Proof. As a first remark, the linear space $\mathcal{A}_{central}$ defined above is indeed an algebra.

In the classical case, we obtain the usual algebra of smooth central functions.

Also, in the group dual case, we have:

$$\Sigma\Delta = \Delta$$

Thus, in this case, we obtain the whole convolution algebra.

Observe also that $\mathcal{A}_{central}$ contains all the characters, because we have:

$$\begin{aligned} \Delta(\chi_v) &= \Delta\left(\sum_i v_{ii}\right) \\ &= \sum_{ij} v_{ij} \otimes v_{ji} \end{aligned}$$

Conversely, consider an element $a \in \mathcal{A}$, written as:

$$a = \sum_{v \in Irr(A)} a_v$$

The condition $a \in \mathcal{A}_{central}$ is then equivalent to the following condition, for any $v \in Irr(A)$:

$$a_v \in \mathcal{A}_{central}$$

But $a_v \in \mathcal{A}_{central}$ means that a_v must be a scalar multiple of χ_v, and so the characters form a basis of $\mathcal{A}_{central}$, as stated.

Finally, the fact that we have an orthogonal basis follows from Theorem 13.15. As for the fact that the characters have norm 1, this follows from:

$$\begin{aligned}\int_G \chi_v\chi_v^* &= \sum_{ij}\int_G v_{ii}v_{jj}^*\\ &= \sum_i \frac{1}{N}\\ &= 1\end{aligned}$$

Here we have used the fact, coming from Theorem 13.15, that the integrals $\int_G v_{ij}v_{kl}^*$ form the orthogonal projection onto the following vector space:

$$\begin{aligned}Fix(v\otimes\bar{v}) &\simeq End(v)\\ &= \mathbb{C}1\end{aligned}$$

Thus, the proof of our theorem is now complete. □

As a basic illustration for all this, in the abelian group case the irreducible representations are all 1-dimensional, and form a discrete abelian group, called dual group.

14. Diagrams, easiness

We have seen in the previous section that the representations of a closed subgroup $G \subset U_N$ are subject to a number of non-trivial results, collectively known as Peter-Weyl theory. In this section we discuss how all this can be used for integrating characters.

In order to get started, let us recall the following fundamental result, which follows from the Peter-Weyl theory:

Theorem 14.1. *Given a representation $\rho : G \to U_n$, we have:*

$$\int_G \chi_\rho(g)dg = \dim(Fix(\rho))$$

More generally, for any colored integer k, we have the formula

$$\int_G \chi_\rho(g)^k dg = \dim(Fix(\rho^{\otimes k}))$$

and these numbers uniquely determine the law of χ_ρ.

Proof. The first formula follows from the Peter-Weyl theory. The second formula follows from the first one, by applying it to $\rho^{\otimes k}$, and using:

$$\chi_{\rho^{\otimes k}} = \chi_\rho^k$$

As for the last assertion, this is standard probability theory. □

We are mostly interested in the character of the fundamental representation, and the result here is as follows:

Theorem 14.2. *Given a closed subgroup $G \subset_\pi U_N$, the moments of the main character*

$$\chi(g) = Tr(g)$$

whose knowledge determines $law(\chi)$, are the following numbers:

$$M_k = dim(Fix(\pi^{\otimes k}))$$

In addition, the spaces $Fix(\pi^{\otimes k})$ uniquely determine $\int_G$, because the numbers

$$P_{i_1\ldots i_k, j_1\ldots j_k} = \int_G g_{i_1 j_1} \ldots g_{i_k j_k} dg$$

form altogether the orthogonal projection P onto the space $Fix(\pi^{\otimes k})$.

Proof. Here the first assertion follows from Theorem 14.1, with $\rho = \pi$, and the second assertion is something that we know too, from the construction of $\int_G$. □

Summarizing, the computation of $law(\chi)$, or of more complicated quantities, such as the laws of truncated characters χ_t, which require the explicit knowledge of $\int_G$, lead us into the same fundamental question, namely the computation of the spaces $Fix(\pi^{\otimes k})$.

In order to discuss this question, let us introduce the following notion:

Definition 14.3. *Given a closed subgroup $G \subset_\pi U_N$, the collection of vector spaces*

$$C_{kl} = Hom(\pi^{\otimes k}, \pi^{\otimes l})$$

is called Tannakian category associated to G.

As a first observation, the knowledge of the Tannakian category is more or less the same thing as the knowledge of the fixed point spaces:

$$C_{0k} = Fix(\pi^{\otimes k})$$

To be more precise, these latter spaces determine all spaces C_{kl}, because of the Frobenius isomorphisms:

$$Hom(\rho, \nu) \simeq Fix(\rho \otimes \bar{\nu})$$

In practice, it is much better to study the spaces C_{kl} instead of the spaces $Fix(\pi^{\otimes k})$, because, as already pointed out in the previous section, $C = (C_{kl})$ is a category. Thus, we have far more structure in this setting, that we can exploit.

We have the following fundamental result, due to Tannaka and Krein:

Theorem 14.4. *The closed subgroups $G \subset_\pi U_N$ are in correspondence with the Tannakian categories $C = (C_{kl})$ modelled over $\mathbb{C}^N$, in one sense the construction being*

$$C_{kl} = Hom(\pi^{\otimes k}, \pi^{\otimes l})$$

and in the other sense the construction being

$$G = \left\{ g \in U_N \middle| Tg^{\otimes k} = g^{\otimes l} T \ , \ \forall k, l, \forall T \in C_{kl} \right\}$$

with k, l being as usual colored integers.

Proof. This is something quite technical, which follows from Peter-Weyl theory. □

We should mention that these are as well some finer results in this sense, due to Deligne and to Doplicher-Roberts, stating that the assumption that $C = (C_{kl})$ is modelled over $\mathbb{C}^N$ can be dropped. However, all this is considerably deeper that what we need, for our purposes here. In what follows we will use Theorem 14.4 above, as it is.

We will be interested in what follows in the closed subgroups $G \subset U_N$ whose Tannakian category is of the "simplest type", from a combinatorial viewpoint. As we will soon see, such groups include O_N, U_N, as well as B_N, C_N, and also Sp_N, by slightly modifying the formalism. Also, we will have S_N, H_N, and more generally H_N^s, as examples.

In order to introduce such groups, that we will call "easy", let us begin with a general definition, of categorical flavor, as follows:

Definition 14.5. *Let $P(k,l)$ be the set of partitions between an upper colored integer k, and a lower colored integer l. A collection of sets*

$$D = \bigsqcup_{k,l} D(k,l)$$

with $D(k,l) \subset P(k,l)$ is called a category of partitions when it has the following properties:

(1) *Stability under the horizontal concatenation, $(\pi, \sigma) \to [\pi\sigma]$.*
(2) *Stability under vertical concatenation $(\pi, \sigma) \to [\begin{smallmatrix}\sigma\\ \pi\end{smallmatrix}]$, with matching middle symbols.*
(3) *Stability under the upside-down turning $*$, with switching of colors, $\circ \leftrightarrow \bullet$.*
(4) *Each set $P(k,k)$ contains the identity partition $|| \ldots ||$.*
(5) *The sets $P(\emptyset, \circ\bullet)$ and $P(\emptyset, \bullet\circ)$ contain the semicircle $\cap$.*
(6) *The various sets $P(\cdot\cdot, \cdot\cdot)$ contain the basic crossing $\diagup\!\!\diagdown$.*

As a basic example, we have P itself.
Another basic example if the category P_2 of all pairings.
We have as well the category P_{12} of all singletons and pairings.

There are many other examples, that we will gradually introduce, in what follows.

Here are a few basic examples of such linear maps:

Proposition 14.6. *The correspondence $\pi \to T_\pi$ has the following properties:*

(1) $T_\cap = (1 \to \sum_i e_i \otimes e_i)$.
(2) $T_\cup = (e_i \otimes e_j \to \delta_{ij})$.
(3) $T_{||\ldots||} = id$.
(4) $T_{\diagup\!\!\diagdown} = (a \otimes b \to b \otimes a)$.

Proof. We can assume if we want that all the upper and lower legs of π are colored $\circ$. With this assumption made, the proof goes as follows:

(1) We have $\cap \in P_2(\emptyset, \circ\circ)$, and so the corresponding operator is a certain linear map, as follows:

$$T_\cap : \mathbb{C} \to \mathbb{C}^N \otimes \mathbb{C}^N$$

The formula of this map is as follows, as claimed:

$$\begin{aligned} T_\cap(1) &= \sum_{ij} \delta_\cap(i\ j) e_i \otimes e_j \\ &= \sum_{ij} \delta_{ij} e_i \otimes e_j \\ &= \sum_i e_i \otimes e_i \end{aligned}$$

(2) Here we have $\cup\in P_2(\circ\circ,\emptyset)$, and so the corresponding operator is a certain linear form:

$$T_\cap:\mathbb{C}^N\otimes\mathbb{C}^N\to\mathbb{C}$$

The formula of this linear form is then as follows:

$$\begin{aligned}T_\cap(e_i\otimes e_j)&=\delta_\cap(i\ j)\\&=\delta_{ij}\end{aligned}$$

(3) Consider indeed the "identity" pairing $||\ldots||\in P_2(k,k)$, with $k=\circ\circ\ldots\circ\circ$. The corresponding linear map is then the identity, because we have:

$$\begin{aligned}T_{||\ldots||}(e_{i_1}\otimes\ldots\otimes e_{i_k})&=\sum_{j_1\ldots j_k}\delta_{||\ldots||}\begin{pmatrix}i_1&\ldots&i_k\\j_1&\ldots&j_k\end{pmatrix}e_{j_1}\otimes\ldots\otimes e_{j_k}\\&=\sum_{j_1\ldots j_k}\delta_{i_1j_1}\ldots\delta_{i_kj_k}e_{j_1}\otimes\ldots\otimes e_{j_k}\\&=e_{i_1}\otimes\ldots\otimes e_{i_k}\end{aligned}$$

(4) In the case of the basic crossing $\diagdown\!\!\diagup\in P_2(\circ\circ,\circ\circ)$, the corresponding linear map is as follows:

$$T_{\diagdown\!\!\diagup}:\mathbb{C}^N\otimes\mathbb{C}^N\to\mathbb{C}^N\otimes\mathbb{C}^N$$

This map can be computed as follows:

$$\begin{aligned}T_{\diagdown\!\!\diagup}(e_i\otimes e_j)&=\sum_{kl}\delta_{\diagdown\!\!\diagup}\begin{pmatrix}i&j\\k&l\end{pmatrix}e_k\otimes e_l\\&=\sum_{kl}\delta_{il}\delta_{jk}e_k\otimes e_l\\&=e_j\otimes e_i\end{aligned}$$

Thus we obtain the flip operator $\Sigma(a\otimes b)=b\otimes a$, as claimed. □

The relation with the Tannakian categories comes from the following result:

Theorem 14.7. *Each $\pi\in P(k,l)$ produces a linear map $T_\pi:(\mathbb{C}^N)^{\otimes k}\to(\mathbb{C}^N)^{\otimes l}$,*

$$T_\pi(e_{i_1}\otimes\ldots\otimes e_{i_k})=\sum_{j_1\ldots j_l}\delta_\pi\begin{pmatrix}i_1&\ldots&i_k\\j_1&\ldots&j_l\end{pmatrix}e_{j_1}\otimes\ldots\otimes e_{j_l}$$

with the Kronecker type symbols $\delta_\pi\in\{0,1\}$ depending on whether the indices fit or not. The assignement $\pi\to T_\pi$ is categorical, in the sense that we have

$$T_\pi\otimes T_\sigma=T_{[\pi\sigma]}$$

$$T_\pi T_\sigma=N^{c(\pi,\sigma)}T_{[\frac{\sigma}{\pi}]}$$

$$T_\pi^*=T_{\pi^*}$$

where $c(\pi,\sigma)$ are certain integers, coming from the erased components in the middle.

Proof. This follows from some routine computations, as follows:

(1) The concatenation axiom follows from the following computation:

$$\begin{aligned}
&(T_\pi\otimes T_\sigma)(e_{i_1}\otimes\ldots\otimes e_{i_p}\otimes e_{k_1}\otimes\ldots\otimes e_{k_r})\\
&=\sum_{j_1\ldots j_q}\sum_{l_1\ldots l_s}\delta_\pi\begin{pmatrix}i_1&\ldots&i_p\\j_1&\ldots&j_q\end{pmatrix}\delta_\sigma\begin{pmatrix}k_1&\ldots&k_r\\l_1&\ldots&l_s\end{pmatrix}e_{j_1}\otimes\ldots\otimes e_{j_q}\otimes e_{l_1}\otimes\ldots\otimes e_{l_s}\\
&=\sum_{j_1\ldots j_q}\sum_{l_1\ldots l_s}\delta_{[\pi\sigma]}\begin{pmatrix}i_1&\ldots&i_p&k_1&\ldots&k_r\\j_1&\ldots&j_q&l_1&\ldots&l_s\end{pmatrix}e_{j_1}\otimes\ldots\otimes e_{j_q}\otimes e_{l_1}\otimes\ldots\otimes e_{l_s}\\
&=T_{[\pi\sigma]}(e_{i_1}\otimes\ldots\otimes e_{i_p}\otimes e_{k_1}\otimes\ldots\otimes e_{k_r})
\end{aligned}$$

(2) The composition axiom follows from the following computation:

$$\begin{aligned}
&T_\pi T_\sigma(e_{i_1}\otimes\ldots\otimes e_{i_p})\\
&=\sum_{j_1\ldots j_q}\delta_\sigma\begin{pmatrix}i_1&\ldots&i_p\\j_1&\ldots&j_q\end{pmatrix}\sum_{k_1\ldots k_r}\delta_\pi\begin{pmatrix}j_1&\ldots&j_q\\k_1&\ldots&k_r\end{pmatrix}e_{k_1}\otimes\ldots\otimes e_{k_r}\\
&=\sum_{k_1\ldots k_r}N^{c(\pi,\sigma)}\delta_{[\frac{\sigma}{\pi}]}\begin{pmatrix}i_1&\ldots&i_p\\k_1&\ldots&k_r\end{pmatrix}e_{k_1}\otimes\ldots\otimes e_{k_r}\\
&=N^{c(\pi,\sigma)}T_{[\frac{\sigma}{\pi}]}(e_{i_1}\otimes\ldots\otimes e_{i_p})
\end{aligned}$$

(3) Finally, the involution axiom follows from the following computation:

$$\begin{aligned}
&T_\pi^*(e_{j_1}\otimes\ldots\otimes e_{j_q})\\
&=\sum_{i_1\ldots i_p}<T_\pi^*(e_{j_1}\otimes\ldots\otimes e_{j_q}),e_{i_1}\otimes\ldots\otimes e_{i_p}>e_{i_1}\otimes\ldots\otimes e_{i_p}\\
&=\sum_{i_1\ldots i_p}\delta_\pi\begin{pmatrix}i_1&\ldots&i_p\\j_1&\ldots&j_q\end{pmatrix}e_{i_1}\otimes\ldots\otimes e_{i_p}\\
&=T_{\pi^*}(e_{j_1}\otimes\ldots\otimes e_{j_q})
\end{aligned}$$

Summarizing, our correspondence is indeed categorical. □

In relation with the compact groups, we have the following result:

Theorem 14.8. *Each category of partitions $D=(D(k,l))$ produces a family of compact groups*

$$G=(G_N)$$

one for each $N\in\mathbb{N}$, via the formula

$$Hom(u^{\otimes k},u^{\otimes l})=span\left(T_\pi\Big|\pi\in D(k,l)\right)$$

and the Tannakian duality correspondence.

Proof. According to Theorem 14.7, the spaces in the statement form a Tannakian category. Thus the Tannakian duality result applies and gives the result. □

We can now formulate a key definition, as follows:

Definition 14.9. *A closed subgroup $G \subset U_N$ is called easy when we have*

$$Hom(u^{\otimes k}, u^{\otimes l}) = span\left(T_\pi \middle| \pi \in D(k,l)\right)$$

for any colored integers k, l, for a certain category of partitions $D \subset P$.

In other words, a closed subgroup $G \subset U_N$ is called "easy" when its Tannakian category appears in the simplest possible way: from set-theoretic partitions.

All this goes back to some old work of Brauer, regarding the orthogonal group O_N, and the unitary group U_N. In the present framework, the Brauer theorem is as follows:

Theorem 14.10. *We have the following results:*

(1) *The unitary group U_N is easy, coming from the category $\mathcal{P}_2$.*
(2) *The orthogonal group O_N is easy as well, coming from the category P_2.*

Proof. As already mentioned, this result is due to Brauer. The classical proof is via classical Tannakian duality, for the usual closed subgroups $G \subset U_N$. □

In order to enlarge now our list of examples, and develop some general theory as well, we have several directions to be explored.

A first natural question is that of computing the quantum group associated to the category P itself, and we have here:

Theorem 14.11. *The symmetric group S_N, regarded as group of unitary matrices,*

$$S_N \subset O_N \subset U_N$$

via the permutation matrices, is easy, coming from the category of all partitions P.

Proof. Consider indeed the symmetric group S_N, regarded as a group of unitary matrices, with each permutation $\sigma \in S_N$ corresponding to the associated permutation matrix:

$$\sigma(e_i) = e_{\sigma(i)}$$

Consider as well the easy group $G \subset O_N$ coming from the category of all partitions P. Since P is generated by the one-block partition $\mu \in P(2,1)$, we have:

$$C(G) = C(O_N)\Big/\left\langle T_\mu \in Hom(\pi^{\otimes 2}, \pi)\right\rangle$$

The linear map associated to μ is given by the following formula:

$$T_\mu(e_i \otimes e_j) = \delta_{ij} e_i$$

Thus, we have the following formulae, using indices:

$$\pi = (\pi_{ij})_{ij}$$

$$\pi^{\otimes 2} = (\pi_{ij}\pi_{kl})_{ik,jl}$$

$$T_\mu = (\delta_{ijk})_{i,jk}$$

We therefore obtain the following formula:

$$\begin{aligned}(T_\mu\pi^{\otimes 2})_{i,jk} &= \sum_{lm}(T_\mu)_{i,lm}(\pi^{\otimes 2})_{lm,jk}\\ &= \pi_{ij}\pi_{ik}\end{aligned}$$

We have as well the following formula:

$$\begin{aligned}(\pi T_\mu)_{i,jk} &= \sum_{l}\pi_{il}(T_\mu)_{l,jk}\\ &= \delta_{jk}\pi_{ij}\end{aligned}$$

Thus, the relation defining $G \subset O_N$ reformulates as follows:

$$T_\mu \in Hom(\pi^{\otimes 2}, \pi) \iff \pi_{ij}\pi_{ik} = \delta_{jk}\pi_{ij}, \forall i, j, k$$

In other words, the elements π_{ij} must be projections, and these projections must be pairwise orthogonal on the rows of $\pi = (\pi_{ij})$. We conclude that $G \subset O_N$ is the subgroup of matrices $g \in O_N$ having the property:

$$g_{ij} \in \{0, 1\}$$

Thus we have $G = S_N$, as desired. □

We have as well the following result:

Theorem 14.12. *We have a diagram as follows,*

$$\begin{array}{ccc} O_N & \longrightarrow & U_N \\ \uparrow & & \uparrow \\ B_N & \longrightarrow & C_N \end{array}$$

and all these groups are easy.

Proof. The corresponding categories of partitions are indeed as follows, with 12 standing for "singletons and pairings", in the same way as the symbol 2 stands for "pairings":

$$\begin{array}{ccc} P_2 & \longleftarrow & \mathcal{P}_2 \\ \downarrow & & \downarrow \\ P_{12} & \longleftarrow & \mathcal{P}_{12} \end{array}$$

All this follows, as usual, from Tannakian duality. □

In the discrete case now, we have the following result:

Theorem 14.13. *The complex reflection group $H_N^s = \mathbb{Z}_s \wr S_N$ is easy, the corresponding category consisting of the partitions satisfying the following condition, in each block:*

$$\#\circ = \#\bullet\ (s)$$

In particular, we have the following results:

(1) *S_N is easy, coming from the category P.*
(2) *H_N is easy, coming from the category P_{even}.*
(3) *K_N is easy, coming from the category $\mathcal{P}_{even}$.*

Proof. This is something that we already know at $s = 1$, from Theorem 14.11 above. In general, the proof is similar, based on Tannakian duality. □

In what follows we will be interested in computing laws of characters, for the main examples of groups that we have. In the easy group case, we have:

Proposition 14.14. *Let G be an easy group, coming from a category of partitions $D = (D(k,l))$. The moments of the main character are then given by*

$$\int_G \chi^k = \dim\left(span\left(\xi_\pi \middle| \pi \in D(k)\right)\right)$$

where

$$D(k) = D(\emptyset, k)$$

and where for $\pi \in D(k)$ we use the notation $\xi_\pi = T_\pi$.

Proof. We recall that for an easy group $G \subset U_N$, coming from a category of partitions $D = (D(k,l))$, we have equalities as follows:

$$Hom(u^{\otimes k}, u^{\otimes l}) = span\left(T_\pi \middle| \pi \in D(k,l)\right)$$

By interchanging $k \leftrightarrow l$ in this formula, and then setting $l = \emptyset$, we obtain:

$$Fix(u^{\otimes k}) = span\left(\xi_\pi \middle| \pi \in D(k)\right)$$

By using now Theorem 14.6 above, we obtain the result. □

Thus, in the easy case, we are led into linear independence questions for the vectors ξ_π.

In order to investigate these questions, we will use the Gram matrix of these vectors. Let us begin with some standard combinatorial definitions, as follows:

Definition 14.15. *Let $P(k)$ be the set of partitions of $\{1,\ldots,k\}$, and let $\pi,\sigma\in P(k)$.*

(1) *We write $\pi\leq\sigma$ if each block of π is contained in a block of σ.*
(2) *We let $\pi\vee\sigma\in P(k)$ be the partition obtained by superposing π,σ.*

As an illustration here, at $k=2$ we have $P(2)=\{||,\sqcap\}$, and we have:

$$||\leq\sqcap$$

Also, at $k=3$ we have $P(3)=\{|||,\sqcap|,|\sqcap,\sqcap\!\sqcap,\sqcap\!|\}$, and the order relation is as follows:

$$|||\leq\sqcap|,|\sqcap,\sqcap\!\sqcap,\sqcap\!|$$

Observe also that we have:

$$\pi,\sigma\leq\pi\vee\sigma$$

In fact, $\pi\vee\sigma$ is the smallest partition with this property. Due to this fact, $\pi\vee\sigma$ is called supremum of π,σ.

Now back to the easy groups, we have:

Proposition 14.16. *The Gram matrix*

$$G_{kN}(\pi,\sigma)=<\xi_\pi,\xi_\sigma>$$

is given by

$$G_{kN}(\pi,\sigma)=N^{|\pi\vee\sigma|}$$

where $|.|$ is the number of blocks.

Proof. According to the formula of the vectors ξ_π, we have:

$$\begin{aligned}
&<\xi_\pi,\xi_\sigma>\\
=&\sum_{i_1\ldots i_k}\delta_\pi(i_1,\ldots,i_k)\delta_\sigma(i_1,\ldots,i_k)\\
=&\sum_{i_1\ldots i_k}\delta_{\pi\vee\sigma}(i_1,\ldots,i_k)\\
=&N^{|\pi\vee\sigma|}
\end{aligned}$$

Thus, we have obtained the formula in the statement. □

In order to study the Gram matrix, and more specifically to compute its determinant, we will use several standard facts about the partitions.

We have the following standard definition:

Definition 14.17. *The Möbius function of any lattice, and so of P, is given by*

$$\mu(\pi,\sigma)=\begin{cases}1 & \text{if } \pi=\sigma\\ -\sum_{\pi\leq\tau<\sigma}\mu(\pi,\tau) & \text{if } \pi<\sigma\\ 0 & \text{if } \pi\not\leq\sigma\end{cases}$$

with the construction being performed by recurrence.

As an illustration here, let us go back to the set of 2-point partitions, $P(2)=\{||,\sqcap\}$. We have by definition:

$$\mu(||,||)=\mu(\sqcap,\sqcap)=1$$

Also, we know that we have $||<\sqcap$, with no intermediate partition in between, and so the above recurrence procedure gives:

$$\mu(||,\sqcap)=-\mu(||,||)=-1$$

Finally, we have $\sqcap\not\leq||$, and so:

$$\mu(\sqcap,||)=0$$

Thus, as a conclusion, the Möbius matrix $M_{\pi\sigma}=\mu(\pi,\sigma)$ of the lattice $P(2)=\{||,\sqcap\}$ is as follows:

$$M=\begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix}$$

The interest in the Möbius function comes from the Möbius inversion formula:

$$f(\sigma)=\sum_{\pi\leq\sigma}g(\pi)\implies g(\sigma)=\sum_{\pi\leq\sigma}\mu(\pi,\sigma)f(\pi)$$

In linear algebra terms, the statement and proof of this formula are as follows:

Proposition 14.18. *The inverse of the adjacency matrix of P, given by*

$$A_{\pi\sigma}=\begin{cases}1 & \text{if } \pi\leq\sigma\\ 0 & \text{if } \pi\not\leq\sigma\end{cases}$$

is the Möbius matrix of P, given by $M_{\pi\sigma}=\mu(\pi,\sigma)$.

Proof. This is well-known, coming for instance from the fact that A is upper triangular. Indeed, when inverting, we are led into the recurrence from Definition 14.17. □

As a first illustration, for $P(2)$ the formula $M = A^{-1}$ appears as follows:

$$\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1}$$

Also, for $P(3) = \{|||, \sqcap|, |\sqcap, \sqcap\sqcap\}$ the formula $M = A^{-1}$ reads:

$$\begin{pmatrix} 1 & -1 & -1 & -1 & 2 \\ 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}^{-1}$$

In general, the formula $M = A^{-1}$ is quite similar.

Now back to our Gram matrix considerations, we have the following result:

Proposition 14.19. *The Gram matrix is given by $G_{kN} = AL$, where*

$$L(\pi, \sigma) = \begin{cases} N(N-1)\ldots(N-|\pi|+1) & \text{if } \sigma \leq \pi \\ 0 & \text{otherwise} \end{cases}$$

and where $A = M^{-1}$ is the adjacency matrix of $P(k)$.

Proof. We have indeed the following computation:

$$\begin{aligned} & N^{|\pi\vee\sigma|} \\ = \ & \#\left\{i_1, \ldots, i_k \in \{1, \ldots, N\} \,\middle|\, \ker i \geq \pi \vee \sigma\right\} \\ = \ & \sum_{\tau \geq \pi\vee\sigma} \#\left\{i_1, \ldots, i_k \in \{1, \ldots, N\} \,\middle|\, \ker i = \tau\right\} \\ = \ & \sum_{\tau \geq \pi\vee\sigma} N(N-1)\ldots(N-|\tau|+1) \end{aligned}$$

According to Proposition 14.18 and to the definition of A, L, this formula reads:

$$\begin{aligned} (G_{kN})_{\pi\sigma} &= \sum_{\tau \geq \pi} L_{\tau\sigma} \\ &= \sum_{\tau} A_{\pi\tau} L_{\tau\sigma} \\ &= (AL)_{\pi\sigma} \end{aligned}$$

Thus, we obtain in this way the formula in the statement. □

As an illustration for the above result, at $k=2$ we have $P(2)=\{||,\sqcap\}$, and the above formula $G_{kN}=AL$ appears as follows:

$$\begin{pmatrix}N^2 & N\\ N & N\end{pmatrix}=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix}N^2-N & 0\\ N & N\end{pmatrix}$$

At $k=3$ we have $P(3)=\{|||,\sqcap|,|\sqcap,\sqcap\!\sqcap\}$, which leads to a similar formula.

With the above result in hand, we can now investigate the linear independence properties of the vectors ξ_π.

To be more precise, we have the following result:

Theorem 14.20. *The determinant of the Gram matrix G_{kN} is given by*

$$\det(G_{kN})=\prod_{\pi\in P(k)}\frac{N!}{(N-|\pi|)!}$$

and in particular, for $N\geq k$, the vectors $\{\xi_\pi|\pi\in P(k)\}$ are linearly independent.

Proof. According to the formula in Proposition 14.19 above, we have:

$$\det(G_{kN})=\det(A)\det(L)$$

Now if we order $P(k)$ as above, with respect to the number of blocks, and then lexicographically, we see that A is upper triangular, and that L is lower triangular.

Thus $\det(A)$ can be computed simply by making the product on the diagonal, and we obtain 1. As for $\det(L)$, this can computed as well by making the product on the diagonal, and we obtain the number in the statement, with the technical remark that in the case $N<k$ the convention is that we obtain a vanishing determinant. □

Now back to the laws of characters, we can formulate:

Theorem 14.21. *For an easy group $G=(G_N)$, coming from a category of partitions $D=(D(k,l))$, the asymptotic moments of the main character are given by*

$$\lim_{N\to\infty}\int_{G_N}\chi^k=\#D(k)$$

where $D(k)=D(\emptyset,k)$, with the limiting sequence on the left consisting of certain integers, and being stationary at least starting from the k-th term.

Proof. This follows indeed from the general formula from Proposition 14.14, by using the linear independence result from Theorem 14.20 above. □

Our next purpose will be that of understanding what happens for the basic classes of easy quantum groups. In order to deal with the orthogonal case, we will need:

Proposition 14.22. *We have the formula*

$$\#P_2(2k) = (2k)!!$$

with the following convention:

$$(2k)!! = 1.3.5 \ldots (2k-3)(2k-1)$$

Proof. We have to count the pairings of $\{1, \ldots, 2k\}$. But, in order to construct such a pairing, we have $2k-1$ choices for the pair of the number 1, then $2k-3$ choices for the pair of the next number left, and so on. Thus, we obtain $(2k)!!$, as claimed. □

With these preliminaries in hand, we can now state and prove:

Theorem 14.23. *In the $N \to \infty$ limit, the law of the main character χ_u is as follows:*

(1) *For O_N we obtain a Gaussian law, $\frac{1}{\sqrt{2\pi}} e^{-x^2/2} dx$.*

(2) *For U_N we obtain a complex Gaussian law G_1.*

Proof. These results follow from the general formula from Theorem 14.21 above, by using the knowledge of the associated categories of partitions, then the counting formula from Proposition 14.12, and finally by doing some calculus:

(1) For O_N the associated category of partitions is P_2, so the asymptotic moments of the main character are as follows, with the convention $k!! = 0$ when k is odd:

$$\begin{aligned} M_k &= \#P_2(k) \\ &= k!! \end{aligned}$$

In order to recapture now the corresponding measure, there are some tools here, such as the Stieltjes inversion formula, but all this is quite advanced and technical, so perhaps best is to use our intuition. A bit of thinking at O_N, and at the associated sphere S^{N-1} as well, leads to the conclusion that our asymptotic law is probably Gaussian.

With this guess in mind, what we have to do is simply take the Gaussian law, and compute its moments. And the computation here, by partial integration, gives:

$$\begin{aligned} & \frac{1}{\sqrt{2\pi}} \int_{\mathbb{R}} e^{-x^2/2} x^k dx \\ = \; & (k-1) \frac{1}{\sqrt{2\pi}} \int_{\mathbb{R}} e^{-x^2/2} x^{k-2} dx \end{aligned}$$

By recurrence, we obtain from this the following moment formula:

$$\frac{1}{\sqrt{2\pi}} \int_{\mathbb{R}} e^{-x^2/2} x^k dx = k!!$$

Thus our guess was right, and we have proved our result.

(2) This follows from some combinatorics. To be more precise, the asymptotic moments of the main character, with respect to the colored integers, are as follows:

$$M_k = \#\mathcal{P}_2(k)$$

Consider now the following variable, where a, b are real and independent, each following the law g_1:

$$\frac{1}{\sqrt{2}}(a + ib)$$

By doing some combinatorics, the moments of this variable are given by the same formula. □

There are of course many other applications of the above results.

15. Gram determinants

Let $\mathcal{P}_s$ be the category of all partitions. That is, $\mathcal{P}_s(k,l)$ is the set of partitions between an upper row of k points and a lower row of l points, and the categorical operations are the horizontal and vertical concatenation, and the upside-down turning.

A category of partitions $\mathcal{P} \subset \mathcal{P}_s$ is by definition a collection of sets $\mathcal{P}(k,l) \subset \mathcal{P}_s(k,l)$, which is stable under the categorical operations. We have the following examples.

Proposition 15.1. *The following are categories of partitions:*

(1) $\mathcal{P}_o/\mathcal{P}_o^+$*: all pairings/all noncrossing pairings.*
(2) $\mathcal{P}_o^*$*: pairings with each string having an odd leg and an even leg.*
(3) $\mathcal{P}_b/\mathcal{P}_b^+$*: singletons plus pairings/noncrossing pairings.*
(4) $\mathcal{P}_s/\mathcal{P}_s^+$*: all partitions/all noncrossing partitions.*
(5) $\mathcal{P}_h/\mathcal{P}_h^+$*: partitions/noncrossing partitions with blocks of even size.*
(6) $\mathcal{P}_h^*$*: partitions with blocks having the same number of odd and even legs.*

Proof. This is clear from definitions. Note that $\mathcal{P}_g^\times$ corresponds via Tannakian duality [197], [197] to the easy quantum group $G^\times = (G_n^\times)$, with the notations in [18], [25]. □

We use the notation $\mathcal{P}(k) = \mathcal{P}(0,k)$. We denote by $\vee$ and $\wedge$ the set-theoretic sup and inf of partitions, always taken with respect to $\mathcal{P}_s$, and by $|.|$ the number of blocks.

Definition 15.2. *Associated to any category of partitions $\mathcal{P}$ and to any numbers $k, n \geq 0$ are the following matrices, with entries indexed by $\pi, \sigma \in \mathcal{P}(k)$:*

(1) *Gram matrix:* $G_{kn}(\pi,\sigma) = n^{|\pi\vee\sigma|}$.
(2) *Weingarten matrix:* $W_{kn} = G_{kn}^{-1}$.

In order for G_{kn} to be invertible, n must be big enough, and $n \geq k$ is known to be sufficient. The precise bounds depend on the category of partitions, and can be deduced from the various explicit formulae of $\det(G_{kn})$, to be given later on in this paper.

The interest in the above matrices comes from the fact that in the case $\mathcal{P} = \mathcal{P}_g^\times$, they describe the integration over the corresponding easy quantum group $G_n^\times$.

Theorem 15.3. *We have the Weingarten formula*

$$\int_{G_n^\times} u_{i_1j_1} \ldots u_{i_kj_k}\, du = \sum_{\pi,\sigma\in\mathcal{P}_g^\times(k)} \delta_\pi(i)\delta_\sigma(j) W_{kn}(\pi,\sigma)$$

where the δ symbols are 0 or 1, depending on whether the indices fit or not.

Proof. This follows by using a classical argument from [189], [50]. See [18], [25]. □

The exact computation of the Weingarten matrix is a quite subtle problem. A precise result is available only in the finite group case, where the formula is given in terms of the Möbius function μ on $\mathcal{P}$ as follows.

Proposition 15.4. *For S_n, H_n the Weingarten function is given by*

$$W_{kn}(\pi,\sigma)=\sum_{\tau\leq\pi\wedge\sigma}\mu(\tau,\pi)\mu(\tau,\sigma)\frac{(n-|\tau|)!}{n!}$$

and satisfies $W_{kn}(\pi,\sigma)=n^{-|\pi\wedge\sigma|}(\mu(\pi\wedge\sigma,\pi)\mu(\pi\wedge\sigma,\sigma)+O(n^{-1}))$.

Proof. The first assertion follows from the Weingarten formula: in that formula the integrals on the left are known, and this allows the computation of the right term, via the Möbius inversion formula. The second assertion follows from the first one. □

In the general case we have the following result, which is useful for applications.

Proposition 15.5. *For $\pi\leq\sigma$ we have the estimate*

$$W_{kn}(\pi,\sigma)=n^{-|\pi|}(\mu(\pi,\sigma)+O(n^{-1}))$$

and for π,σ arbitrary we have $W_{kn}(\pi,\sigma)=O(n^{|\pi\vee\sigma|-|\pi|-|\sigma|})$.

Proof. Once again this follows by using a classical argument, see [18]. □

In this paper, we will be mainly interested in the computation of $\det(G_{kn})$. Let us being with some simple observations, coming from definitions.

Proposition 15.6. *Let $D_k(n)=\det(G_{kn})$, viewed as element of $\mathbb{Z}[n]$.*

(1) *D_k is monic, of degree $s_k=\sum_{\pi\in\mathcal{P}(k)}|\pi|$.*

(2) *We have $n^{b_k}|D_k$, where $b_k=\#\mathcal{P}(k)$.*

Proof. (1) This follows from $|\pi\vee\sigma|\leq|\pi|$, with equality if and only if $\sigma\leq\pi$. Indeed, from the inequality we get $\deg(D_k)\leq s_k$. Now the coefficient of n^{s_k} is the signed number of permutations $f:\mathcal{P}(k)\to\mathcal{P}(k)$ satisfying $f(\pi)\leq\pi$ for any π, and since there is only one such permutation, namely the identity, we obtain that this coefficient is 1.

(2) This is clear from the definition of D_k, and from $|\pi\vee\sigma|\geq 1$. □

The above result raises the question of computing the numbers $b_k=\#\mathcal{P}(k)$ and $s_k=\sum_{\pi\in\mathcal{P}(k)}|\pi|$. It is convenient here to introduce as well the related numbers $m_k=s_k/b_k$ and $a_k=2s_k-kb_k=(2m_k-k)b_k$, which will appear several times in what follows.

Proposition 15.7. *The numbers b_k,s_k,m_k,a_k are as follows:*

(1) *O_n,O_n^*,O_n^+: $b_{2l}=(2l)!!,l!$, $\frac{1}{l+1}\binom{2l}{l}$, $s_{2l}=lb_{2l}$, $m_{2l}=l$, $a_{2l}=0$.*

(2) *S_n: $b_k=Bell$, $s_k=b_{k+1}-b_k$, $m_k=\frac{b_{k+1}}{b_k}-1$, $a_k=2b_{k+1}-(k+2)b_k$.*

(3) *S_n^+: $b_k=\frac{1}{k+1}\binom{2k}{k}$, $s_k=\frac{1}{2}\binom{2k}{k}$, $m_k=\frac{k+1}{2}$, $a_k=b_k$.*

(4) *H_n^+: $b_{2l}=\frac{1}{2l+1}\binom{3l}{l}$, $s_{2l}=\binom{3l-1}{l-1}$, $m_{2l}=\frac{2l+1}{3}$, $a_{2l}=-2\binom{3l-1}{l-2}$.*

Proof. All these results are well-known. □

For the remaining quantum groups, namely B_n, B_n^+, H_n, H_n^*, the numbers b_k, s_k, m_k, a_k are given by quite complicated formulae. The best approach to their computation is via the trace of the Gram matrix, and its analytic interpretations.

So, let us first reformulate Proposition 2.1, in the following way.

Proposition 15.8. *With $D_k(n) = \det(G_{kn})$ and $T_k(t) = Tr(G_{kt})$, we have:*

(1) $D_k(n) = n^{s_k}(1 + O(n^{-1}))$ *as* $n \to \infty$, *where* $s_k = T_k'(1)$.

(2) $D_k(n) = O(n^{b_k})$ *as* $n \to 0$, *where* $b_k = T_k(1)$.

Proof. This is indeed just a reformulation of Proposition 2.1, using a variable t around 1. Note that in (2) we regard the variable n as a formal parameter, going to 0. □

The trace can be understood in terms of the associated Stirling numbers.

Proposition 15.9. *We have the formula*

$$T_k(t) = \sum_{r=1}^{k} S_{kr} t^r$$

where $S_{kr} = \#\{\pi \in \mathcal{P}(k) : |\pi| = r\}$ are the Stirling numbers.

Proof. This is clear from definitions. □

Another interpretation of the trace, analytic this time, is as follows.

Proposition 15.10. *For any $t \in (0, 1]$ we have the formula*

$$T_k(t) = \lim_{n\to\infty} \int_{G_n^\times} \chi_t^k$$

where $\chi_t = \sum_{i=1}^{[tn]} u_{ii}$ are the truncated characters of the quantum group.

Proof. As explained in [25], [18], this follows from the Weingarten formula. □

In general, the Stirling numbers S_{kr} and the trace $T_k(t)$ are given by quite complicated formulae, unless we are in the situation of one of the quantum groups in Proposition 2.2. Here these invariants are well-known in the O, S cases, and for H^+ we have:

$$T_{2l}(t) = \sum_{r=1}^{l} \frac{1}{r}\binom{l-1}{r-1}\binom{2l}{r-1} t^r$$

See [13]. In general now, the conceptual result concerns the asymptotic measures of truncated characters, i.e. the probability measures μ_t satisfying:

$$T_k(t) = \int x^k d\mu_t(x)$$

We have the following result:

Theorem 15.11. *The asymptotic measures of truncated characters are as follows:*

(1) S_n/S_n^+*: Poisson/free Poisson.*
(2) O_n/O_n^+*: Gaussian/semicircular.*
(3) H_n/H_n^+*: Bessel/free Bessel.*
(4) B_n/B_n^+*: shifted Gaussian/shifted semicircular.*
(5) O_n^*/H_n^**: symmetrized Rayleigh/squeezed* ∞*-Bessel.*

Proof. The one-parameter measures in the statement are best found via a direct computation, by using classical and free cumulants. See [25], [18], [19]. □

We discuss now the explicit computation of the Gram determinants. The basic formula here is as follows.

Theorem 15.12. *For* S_n, H_n, H_n^* *we have*

$$\det(G_{kn}) = \prod_{\pi\in\mathcal{P}(k)} \frac{n!}{(n-|\pi|)!}$$

where $|.|$ *is the number of blocks.*

Proof. We use the fact that the partitions have the property of forming semilattices under $\vee$. The proof uses the upper triangularization procedure together with the explicit knowledge of the Möbius function on $\mathcal{P}(k)$. Consider the following matrix, obtained by making determinant-preserving operations:

$$G'_{kn}(\pi,\sigma) = \sum_{\pi\leq\tau} \mu(\pi,\tau) n^{|\tau\vee\sigma|}$$

It follows from the Möbius inversion formula that we have:

$$G'_{kn}(\pi,\sigma) = \begin{cases} n(n-1)\ldots(n-|\sigma|+1) & \text{if } \pi\leq\sigma \\ 0 & \text{if not} \end{cases}$$

Thus the matrix is upper triangular, and by computing the product on the diagonal we obtain the formula in the statement. □

A first remarkable feature of the above result is that the determinant for S_n, H_n, H_n^* can be computed from the trace: indeed, the Gram trace gives the Stirling numbers, which in turn give the Gram determinant. However, the connecting formula is quite complicated, so let us just record here an improvement of the first estimate in Proposition 2.3.

Proposition 15.13. *With* $D_k(n) = \det(G_{kn})$ *and* $T_k(t) = Tr(G_{kt})$ *we have*

$$D_k(n) = n^{s_k}\left(1 - \frac{z_k}{2}\,n^{-1} + O(n^{-2})\right)$$

where $s_k = T_k'(1)$ *and* $z_k = T_k''(1)$.

Proof. In terms of Stirling numbers, the formula in Theorem 3.1 reads:

$$D_k(n)=\prod_{r=1}^{k}\left(\frac{n!}{(n-r)!}\right)^{S_{kr}}$$

We use now the following basic estimate:

$$\frac{n!}{(n-r)!}=n^r\prod_{s=1}^{r-1}\left(1-\frac{s}{n}\right)=n^r\left(1-\frac{r(r-1)}{2}\,n^{-1}+O(n^{-2})\right)$$

Together with $T_k(t)=\sum_{r=1}^{k}S_{kr}t^r$, this gives the result. □

The above discussion raises the general question on whether the Gram determinant can be computed or not from the Gram trace, or from the measures in Theorem 2.6.

Since the connecting formula for S_n,H_n,H_n^* is already quite complicated, let us formulate for the moment a more modest conjecture, as follows.

Proposition 15.14. *For any easy quantum group we have a formula of type*

$$\det(G_{kn})=\prod_{\pi\in\mathcal{P}(k)}\varphi(\pi)$$

with the "contributions" being given by an explicit function $\varphi:\mathcal{P}(k)\to\mathbb{Q}(n)$.

This statement is of course quite vague, depending of the meaning of the above word "explicit". As already mentioned, one would expect φ to come from the Gram trace, or from the Stirling numbers, or, even better, from the measures in Theorem 2.6. Such a decomposition could potentially clarify the behavior of the Gram determinants under the "liberation" procedure $G\to G^+$.

This kind of general question appears to be quite difficult. In what follows we will obtain some evidence towards such general decomposition results.

We discuss now the cases O,B,O^*. Here the combinatorics is that of the Young diagrams. We denote by $|.|$ the number of boxes, and we use quantity f^λ, which gives the number of standard Young tableaux of shape λ.

Theorem 15.15. *For O_n we have*

$$\det(G_{kn})=\prod_{|\lambda|=k/2}f_n(\lambda)^{f^{2\lambda}}$$

where $f_n(\lambda)=\prod_{(i,j)\in\lambda}(n+2j-i-1)$.

Proof. This follows from the results of Collins and Matsumoto. Indeed, it is known from there that the Gram matrix is diagonalizable, as follows:

$$G_{kn}=\sum_{|\lambda|=k/2}f_n(\lambda)P_{2\lambda}$$

Here $1 = \Sigma P_{2\lambda}$ is the standard partition of unity associated to the Young diagrams having $k/2$ boxes, and the coefficients $f_n(\lambda)$ are those in the statement. Now since we have $Tr(P_{2\lambda}) = f^{2\lambda}$, this gives the result. □

Theorem 15.16. *For B_n we have*

$$\det(G_{kn}) = n^{a_k} \prod_{|\lambda| \leq k/2} f_n(\lambda)^{\binom{k}{2|\lambda|} f^{2\lambda}}$$

where $a_k = \sum_{\pi \in \mathcal{P}(k)} (2|\pi| - k)$, and $f_n(\lambda) = \prod_{(i,j) \in \lambda} (n + 2j - i - 2)$.

Proof. We recall from [25] that we have an isomorphism $B_n \simeq O_{n-1}$, given by $u = v + 1$, where u, v are the fundamental representations of B_n, O_{n-1}. We get:

$$Fix(u^{\otimes k}) = Fix\left((v+1)^{\otimes k}\right) = Fix\left(\sum_{r=0}^{k} \binom{k}{r} v^{\otimes r}\right)$$

Now if we denote by $\det', f'$ the objects in Theorem 4.1, we obtain:

$$\det(G_{kn}) = n^{a_k} \prod_{r=1}^{k} \det{}'(G_{r,n-1})^{\binom{k}{r}} = n^{a_k} \prod_{r=1}^{k} \left(\prod_{|\lambda| = r/2} f'_{n-1}(\lambda)^{f^{2\lambda}} \right)^{\binom{k}{r}}$$

This gives the formula in the statement. □

We have:

Theorem 15.17. *For O_n^* we have*

$$\det(G_{kn}) = \prod_{|\lambda| = k/2} f_n(\lambda)^{f^{\lambda^2}}$$

where $f_n(\lambda) = \prod_{(i,j) \in \lambda} (n + j - i)$.

Proof. We use the isomorphism of projective versions $PO_n^* = PU_n$, established in [25]. This isomorphism shows that the Gram matrices for O_n^* are the same as those for U_n. But for U_n it is known that the Gram matrix is diagonalizable, as follows:

$$G_{kn} = \sum_{|\lambda| = k/2} f_n(\lambda) P_\lambda$$

Here $1 = \Sigma P_\lambda$ is the standard partition of unity associated to the Young diagrams having $k/2$ boxes, and the coefficients $f_n(\lambda)$ are those in the statement. Now since we have $Tr(P_\lambda) = f^{\lambda^2}$, this gives the result. □

Observe that the above results provide a kind of answer to Conjecture 3.3, but with the Young diagrams contributing to the determinant, instead of the partitions. The remaining problems are to find the relevant surjective map from diagrams to partitions, and to see if the above formulae further simplify by using this surjective map.

We discuss now the computation of the Gram matrix determinant, in the free cases $O_n^+, B_n^+, S_n^+, H_n^+$.

Let P_r be the Chebycheff polynomials, given by:

$$P_0 = 1$$

$$P_1 = X$$

$$P_{r+1} = XP_r - P_{r-1}$$

Consider also the following numbers, depending on $k, r \in \mathbb{Z}$:

$$f_{kr} = \binom{2k}{k-r} - \binom{2k}{k-r-1}$$

We set $f_{kr} = 0$ for $k \notin \mathbb{Z}$. The following key result was proved in [77]:

Theorem 15.18. *The determinant of the Gram matrix for O_N^+ is given by*

$$\det(G_{kN}) = \prod_{r=1}^{[k/2]} P_r(N)^{d_{k/2,r}}$$

where $d_{kr} = f_{kr} - f_{k+1,r}$.

Proof. As already mentioned, the result is from [77]. We present below a short proof. The result holds when k is odd, all the exponents being 0, so we assume that k is even.

Step 1. We establish a useful formula of the following type:

$$G_{kN}(\pi, \sigma) =< f_\pi, f_\sigma >$$

For this purpose, let Γ be a locally finite bipartite graph, with distinguished vertex 0 and adjacency matrix A, and let μ be an eigenvector of A, with eigenvalue N.

Let L_k be the set of length k loops $l = l_1 \ldots l_k$ based at 0, and set:

$$H_k = span(L_k)$$

For $\pi \in \mathcal{P}_{o^+}(k)$ define $f_\pi \in H_k$ by:

$$f_\pi = \sum_{l \in L_k} \left(\prod_{i \sim_\pi j} \delta(l_i, l_j^o) \gamma(l_i) \right) l$$

Here $e \to e^o$ is the edge reversing, and the "spin factor" is as follows, where s, t are the source and target of the edges:

$$\gamma = \sqrt{\mu(t)/\mu(s)}$$

The point is that we have:

$$G_{kN}(\pi, \sigma) =< f_\pi, f_\sigma >$$

We refer to [107] for details regarding all this.

Step 2. With a suitable choice of (Γ,μ), we obtain a fomula of type:

$$G_{kN}=T_{kN}T_{kN}^t$$

Indeed, let us choose $\Gamma=\mathbb{N}$ to be the Cayley graph of O_N^+, and the eigenvector entries $\mu(r)$ to be the Chebycheff polynomials $P_r(N)$, i.e. the orthogonal polynomials for O_N^+.

In this case, we have a bijection $\mathcal{P}_{o^+}(k)\to L_k$, constructed as follows. For $\pi\in\mathcal{P}_{o^+}(k)$ and $0\leq i\leq k$ we define $h_\pi(i)$ to be the number of $1\leq j\leq i$ which are joined by π to a number strictly larger than i. We then define a loop $l(\pi)=l(\pi)_1\ldots l(\pi)_k$, where $l(\pi)_i$ is the edge from $h_\pi(i-1)$ to $h_\pi(i)$. Consider now the following matrix:

$$T_{kN}(\pi,\sigma)=\prod_{i\sim_\pi j}\delta(l(\sigma)_i,l(\sigma)_j^o)\gamma(l(\sigma)_i)$$

We have then:

$$f_\pi=\sum_\sigma T_{kn}(\pi,\sigma)\cdot l(\sigma)$$

Thus we obtain, as desired:

$$G_{kN}=T_{kN}T_{kN}^t$$

Step 3. We show that, with suitable conventions, T_{kN} is lower triangular.

Indeed, consider the partial order on $\mathcal{P}_{o^+}(k)$ given by $\pi\leq\sigma$ if $h_\pi(i)\leq h_\sigma(i)$ for $i=1,\ldots,k$. Our claim is that $\sigma\not\leq\pi$ implies:

$$T_{kN}(\pi,\sigma)=0$$

Indeed, suppose that $\sigma\not\leq\pi$, and let j be the least number with $h_\sigma(j)>h_\pi(j)$. Note that we must have $h_\sigma(j-1)=h_\pi(j-1)$ and $h_\sigma(j)=h_\pi(j)+2$. It follows that we have $i\sim_\pi j$ for some $i<j$. From the definitions of T_{kn} and $l(\sigma)$, if $T_{kn}(\pi,\sigma)\neq 0$ then we must have $h_\sigma(i-1)=h_\sigma(j)=h_\pi(j)+2$. But we also have $h_\pi(i-1)=h_\pi(j)$, so that $h_\sigma(i-1)=h_\pi(i-1)+2$, which contradicts the minimality of j.

Step 4. End of the proof, by computing the determinant of T_{kN}.

Since T_{kN} is lower triangular we have:

$$\begin{aligned}\det(T_{kN})&=\prod_\pi T_{kN}(\pi,\pi)\\&=\prod_\pi\prod_{i\sim_\pi j}\sqrt{\frac{P_{h_{\pi(i)}}}{P_{h_{\pi(i)-1}}}}\\&=\prod_{r=1}^{k/2}P_r^{e_{kr}/2}\end{aligned}$$

Here the exponents appearing on the right are by definition as follows:

$$e_{kr} = \sum_{\pi} \sum_{i \sim_{\pi} j} \delta_{h_\pi(i),r} - \delta_{h_\pi(i),r+1}$$

Our claim now, which finishes the proof, is that for $1 \leq r \leq k/2$ we have:

$$\sum_{\pi} \sum_{i \sim_{\pi} j} \delta_{h_\pi(i)r} = f_{k/2,r}$$

Indeed, note that the left term counts the number of times that the edge $(r, r+1)$ appears in all loops in L_k. Define a shift operator S on the edges of Γ by:

$$S(s,t) = (s+1, t+1)$$

Given a loop $l = l_1 \ldots l_k$ and $1 \leq s \leq k$ with $l_s = (r, r+1)$, define a path:

$$S^r(l_s) \ldots S^r(l_k) l_{s-1}^o \ldots l_1^o$$

Observe that this is a path in Γ from $2r$ to 0 whose first edge is $(2r, 2r+1)$ and first reaches $r-1$ after $k-s+1$ steps.

Conversely, given a path $f_1 \ldots f_k$ in Γ from $2r$ to 0 whose first edge is $(2r, 2r+1)$ and first reaches $r-1$ after s steps, define a loop:

$$f_k^o \ldots f_s^o S^{-r}(f_1) \ldots S^{-r}(f_{s-1})$$

Observe that this is a loop in Γ based at 0 whose $k-s+1$ edge is $(r, r+1)$.

These two operations are inverse to each other, so we have established a bijection between k-loops in Γ based at 0 whose s-th edge is $(r, r+1)$ and k-paths in Γ from $2r$ to 0 whose first edge is $(2r, 2r+1)$ and which first reach $r-1$ after $k-s+1$ steps.

It follows that the left hand side is equal to the number of paths in $\Gamma = \mathbb{N}$ from $2r$ to 0 whose first edge is $(2r, 2r+1)$. By the usual reflection trick, this is the difference of binomials defining $f_{k/2,r}$, and we are done. □

We use the notation $a_k = \sum_{\pi \in \mathcal{P}(k)} (2|\pi| - k)$, which already appeared in section 2.

Theorem 15.19. *For B_n^+ we have:*

$$\det(G_{kn}) = n^{a_k} \prod_{r=1}^{[k/2]} P_r(n-1)^{\sum_{l=1}^{[k/2]} \binom{k}{2l} d_{lr}}$$

Proof. We have $B_n^+ \simeq O_{n-1}^+$, so we can use the same method as in the proof of Theorem 4.2. By using prime exponents for the various O_n^+-related objects, we get:

$$\det(G_{kn}) = n^{a_k} \prod_{l=1}^{[k/2]} \det{}'(G_{2l,n-1})^{\binom{k}{2l}} = n^{a_k} \prod_{l=1}^{[k/2]} \left(\prod_{r=1}^{l} P_r(n-1)^{d_{lr}} \right)^{\binom{k}{2l}}$$

Together with Theorem 5.1, this gives the formula in the statement. □

Let us start with:

Proposition 15.20. *We have a bijection $NC(k) \simeq NC_2(2k)$, constructed as follows:*

(1) *The application $NC(k) \to NC_2(2k)$ is the "fattening" one, obtained by doubling all the legs, and doubling all the strings as well.*
(2) *Its inverse $NC_2(2k) \to NC(k)$ is the "shrinking" application, obtained by collapsing pairs of consecutive neighbors.*

Proof. The fact that the two operations in the statement are indeed inverse to each other is clear, by computing the corresponding two compositions, with the remark that the construction of the fattening operation requires the partitions to be noncrossing. □

We have the following key observation:

Theorem 15.21. *The Gram matrices of $NC_2(2k), NC(k)$ are related as follows,*

$$G_{2k,n}(\pi,\sigma) = n^k(\Delta_{kn}^{-1}G_{k,n^2}\Delta_{kn}^{-1})(\pi',\sigma')$$

where $\pi \to \pi'$ is the shrinking operation, and Δ_{kn} is the diagonal of G_{kn}.

Proof. In the context of Proposition 6.10, it is elementary to see that we have:

$$|\pi \vee \sigma| = k + 2|\pi' \vee \sigma'| - |\pi'| - |\sigma'|$$

We therefore have the following formula, valid for any $n \in \mathbb{N}$:

$$n^{|\pi\vee\sigma|} = n^{k+2|\pi'\vee\sigma'|-|\pi'|-|\sigma'|}$$

Thus, we obtain the formula in the statement. □

Regarding now the quantum group S_N^+, we have here:

Theorem 15.22. *The determinant of the Gram matrix for S_N^+ is given by*

$$\det(G_{kN}) = (\sqrt{N})^{a_k}\prod_{r=1}^{k} P_r(\sqrt{N})^{d_{kr}}$$

where:

$$a_k = \sum_{\pi\in\mathcal{P}(k)} (2|\pi| - k)$$

Proof. We use the shrinking operation $\pi \to \widetilde{\pi}$, obtained by collapsing neighbors. We have the following formula:

$$|\pi \vee \sigma| = k/2 + 2|\widetilde{\pi} \vee \widetilde{\sigma}| - |\widetilde{\pi}| - |\widetilde{\sigma}|$$

In terms of Gram matrices, if we denote by G' the Gram matrix for O_N^+, we have the following formula, with $D_{kN} = diag(N^{|\widetilde{\pi}|/2-k/4})$:

$$G_{kN} = D_{kN}G'_{2k,\sqrt{N}}D_{kN}$$

With this formula in hand, the result follows from Theorem 6.18. □

Finally, we have:

Theorem 15.23. *For H_n^+ we have the formula*

$$\det(G_{kn}) = (\sqrt{n})^{a_k} \prod_{r=1}^{[k/2]} P_r(\sqrt{n})^{2d'_{k/2,r}}$$

with $d'_{sr} = f'_{sr} - f'_{s,r+1}$, where $f'_{sr} = \binom{3s}{s-r} - \binom{3s}{s-r-1}$ for $s \in \mathbb{Z}$, $f'_{sr} = 0$ for $s \notin \mathbb{Z}$.

Proof. According to [14], the diagrams for H_n^+ are the "cablings" of the Fuss-Catalan diagrams, so we can use the same method as in the previous proof. So, by using the above formula we have $G_{kn} = D_{kn} G'_{2k,\sqrt{n}} D_{kn}$, where $D_{kn} = diag(n^{|\widetilde{\pi}|/2-k/4})$, and where G' is the Gram determinant for the Fuss-Catalan algebra. But this latter determinant was computed by Di Francesco, and this gives the result. □

In this section we perform some algebraic manipulations on the formulae found in the previous sections. Consider the quantity $a_k = \sum_{\pi \in \mathcal{P}(k)} (2|\pi| - k)$, which already appeared, several times. Then n^{a_k} is a true "contribution", in the sense of Conjecture 3.3.

We will prove here that a n^{a_k} factor appears naturally, in all the 10 formulae of Gram determinants. This can be regarded as a piece of evidence towards Conjecture 3.3.

In the classical and half-liberated cases there is no need for supplementary work in order to isolate this n^{a_k} factor, and the unified result is as follows.

Theorem 15.24. *In the classical and half-liberated cases, we have*

$$\begin{aligned}
S_n, H_n, H_n^*: \quad \det(G_{kn}) &= n^{a_k} \prod_{\pi \in \mathcal{P}(k)} \frac{n^{k-2|\pi|} n!}{(n-|\pi|)!} \\
O_n: \quad \det(G_{kn}) &= n^{a_k} \prod_{|\lambda| = k/2} f_n(\lambda)^{f^{2\lambda}} \\
B_n: \quad \det(G_{kn}) &= n^{a_k} \prod_{|\lambda| \leq k/2} f'_n(\lambda)^{\binom{k}{2|\lambda|} f^{2\lambda}} \\
O_n^*: \quad \det(G_{kn}) &= n^{a_k} \prod_{|\lambda| = k/2} f''_n(\lambda)^{f^{\lambda 2}}
\end{aligned}$$

where $f_n^\circ(\lambda) = \prod_{(i,j) \in \lambda} (n + j - i + \varphi^\circ)$, with $\varphi = j - 1, \varphi' = j - 2, \varphi'' = 0$.

Proof. This is a reformulation of the results in section 4, by using $a_k = 0$ for O_n, O_n^*. □

In order to process the formulae in section 5, we need the following technical result.

Proposition 15.25. *The Chebycheff polynomials P_r have the following properties:*

(1) *$P_r(n-1) = Q_r(n)$, with $Q_0 = 1, Q_1 = n - 1$ and $Q_{r+1} = (n-1)Q_r - Q_{r-1}$.*
(2) *$P_{2l}(n) = R_{2l}(n^2)$, with $R_0 = 1, R_2 = n - 1$ and $R_{2l+2} = (n-2)R_{2l} - R_{2l-2}$.*

(3) $P_{2l+1}(n) = nR_{2l+1}(n^2)$, *with* $R_1 = 1, R_3 = n-2$ *and* $R_{2l+3} = (n-2)R_{2l+1} - R_{2l-1}$.
(4) $P_{2l}(n) = n^{-l}S_{2l}(n^2)^{1/2}$, *with* $S_0 = 1, S_2 = n(n-1)^2$ *and so on.*
(5) $P_{2l+1}(n) = n^{-l}S_{2l+1}(n^2)^{1/2}$, *with* $S_1 = n, S_3 = n^2(n-2)^2$ *and so on.*

Proof. This is routine. As pointed out in section 7 below, Q_r are the orthogonal polynomials for B_n^+, and R_{2l} are the orthogonal polynomials for S_n^+. As for the polynomials S_r, these are some technical objects, introduced in relation with the H_n^+ computation. □

Theorem 15.26. *In the free cases, we have*

$$O_n^+: \quad \det(G_{kn}) = n^{a_k}\prod_{r=1}^{[k/2]} P_r(n)^{d^1_{k/2,r}}$$

$$B_n^+: \quad \det(G_{kn}) = n^{a_k}\prod_{r=1}^{[k/2]} Q_r(n)^{\sum_{l=1}^{[k/2]}\binom{k}{2l}d^1_{lr}}$$

$$S_n^+: \quad \det(G_{kn}) = n^{a_k}\prod_{r=1}^{k} R_r(n)^{d^1_{kr}}$$

$$H_n^+: \quad \det(G_{kn}) = n^{a_k}\prod_{r=1}^{[k/2]} S_r(n)^{d^2_{k/2,r}}$$

where $d^i_{kr} = f^i_{kr} - f^i_{k,r+1}$, *with* $f^i_{kr} = \binom{(i+1)k}{k-r} - \binom{(i+1)k}{k-r-1}$ *for* $k \in \mathbb{Z}$, *and* $f^i_{kr} = 0$ *for* $k \notin \mathbb{Z}$.

Proof. The O_n^+ formula is the one in Theorem 5.1, with a $n^{a_k} = 1$ factor inserted.

The B_n^+ formula is the one in Theorem 5.2, with $P_r(n-1)$ replaced by $Q_r(n)$.

For the S_n^+ formula, we use Theorem 5.3. By replacing the Chebycheff polynomials P_{2l}, P_{2l+1} by the polynomials R_{2l}, R_{2l+1} from Proposition 6.2, we get:

$$\det(G_{kn}) = (\sqrt{n})^{a_k}\prod_{r=1}^{k} P_r(\sqrt{n})^{d^1_{kr}} = (\sqrt{n})^{a_k}\sqrt{n}^{\sum_{l=1}^{[(k+1)/2]} d^1_{k,2l-1}}\prod_{r=1}^{k} R_r(n)^{d_{kr}}$$

Now recall from Proposition 2.2 that $a_k = \frac{1}{k+1}\binom{2k}{k}$. On the other hand a direct computation gives $\sum_{l=1}^{[(k+1)/2]} d^1_{k,2l-1} = \frac{1}{k+1}\binom{2k}{k}$, so we get the formula in the statement.

For the H_n^+ formula we use a similar method. With $k = 2l$, Theorem 5.4 gives:

$$\det(G_{2l,n}) = (\sqrt{n})^{a_{2l}}\prod_{r=1}^{l} P_r(\sqrt{n})^{2d^2_{lr}} = (\sqrt{n})^{a_{2l}}(\sqrt{n})^{-2\sum_{s=2}^{l}[s/2]d^2_{ls}}\prod_{r=1}^{l} S_r(n)^{d^2_{lr}}$$

Now recall from Proposition 2.2 that $a_{2l} = -2\binom{3l-1}{l-2}$. On the other hand a direct computation gives $\sum_{s=2}^{l}[s/2]d^2_{ls} = \binom{3l-1}{l-2}$, so we get the formula in the statement. □

As a conclusion, the formulae in Theorem 6.1 and Theorem 6.3 are an intermediate step towards a general decomposition result of type $\det(G_{kn}) = \prod_{\pi\in\mathcal{P}(k)} \varphi(\pi)$. We will come back to the question of finding such a general decomposition result in section 8 below.

We present here a speculation in the free case, in relation with orthogonal polynomials. As we will see, this speculation works for S_n^+, O_n^+, B_n^+, but doesn't work for H_n^+.

Definition 15.27. *The orthogonal polynomials for a real probability measure μ are the polynomials $Q_0, Q_1, Q_2, \ldots$ satisfying the following conditions:*

(1) $Q_k(n) = n^k + a_1 n^{k-1} + \ldots + a_{k-1}n + a_k$, *with* $a_i \in \mathbb{R}$.
(2) *For any* $k \neq l$ *we have* $\int Q_k(n)Q_l(n)\, d\mu(n) = 0$.

The orthogonal polynomials can be constructed by using a recursive formula, of type $Q_{k+1} = (n - \alpha_k)Q_k - \beta_k Q_{k-1}$. Here the parameters $\alpha_k, \beta_k \in \mathbb{R}$ are uniquely determined by the linear equations coming from the fact that Q_{k+1} must be orthogonal to n^{k-1}, n^k.

More precisely, by solving these two equations we obtain the following formulae, where the integral sign denotes the integration with respect to μ:

$$\alpha_k = \frac{\int n^{k+1}Q_k}{\int n^k Q_k} - \frac{\int n^k Q_{k-1}}{\int n^{k-1}Q_{k-1}}, \quad \beta_k = \frac{\int n^k Q_k}{\int n^{k-1}Q_{k-1}}$$

The numbers α_k, β_k are called Jacobi parameters of the sequence $\{Q_k\}$. Since $Q_0 = 1$, in order to describe $\{Q_k\}$ we just need to specify Q_1, and the Jacobi parameters.

The orthogonal polynomials for an easy quantum group are by definition those for the asymptotic measure of the main character, given in Theorem 2.6.

Proposition 15.28. *The basic orthogonal polynomials are as follows:*

(1) O_n: *here* $Q_1 = n$ *and* $Q_{k+1} = nQ_k - kQ_{k-1}$.
(2) B_n: *here* $Q_1 = n-1$ *and* $Q_{k+1} = (n-1)P_k - kQ_{k-1}$.
(3) O_n^*: *here* $Q_1 = n$ *and* $Q_{k+1} = nQ_k - [(k+1)/2]Q_{k-1}$.
(4) S_n: *here* $Q_1 = n-1$ *and* $Q_{k+1} = (n-k-1)Q_k - kQ_{k-1}$.
(5) O_n^+: *here* $Q_1 = n$ *and* $Q_{k+1} = nQ_k - Q_{k-1}$.
(6) B_n^+: *here* $Q_1 = n-1$ *and* $Q_{k+1} = (n-1)Q_k - Q_{k-1}$.
(7) S_n^+: *here* $Q_1 = n-1$ *and* $Q_{k+1} = (n-2)Q_k - Q_{k-1}$.

Proof. This result is well-known, and easy to deduce from definitions. Note that all the polynomials in the above statement are versions of the polynomials appearing in (1,3,4,5), which are respectively the Hermite, Charlier and Chebycheff polynomials. □

Let us go back now to the considerations in section 6. The polynomials R_{2l} appearing in Proposition 6.2 are the orthogonal polynomials for S_n^+, and it is natural to call $\{R_n | n \in \mathbb{N}\}$ the family of "extended orthogonal polynomials" for S_n^+.

Theorem 15.29. *In the O_n^+, B_n^+, S_n^+ cases we have a formula of type*

$$\det(G_{kn}) = n^{a_k} \prod_{r=1}^{k} Q_r(n)^{d_{kr}}$$

with $d_{kr} \in \mathbb{N}$, where $Q_r(n)$ are the corresponding extended orthogonal polynomials.

Proof. This follows from Theorem 6.3 and Proposition 7.2. □

Regarding now H_n^+, the combinatorics here is that of the Fuss-Catalan algebra. Since μ is symmetric, the orthogonal polynomials are given by $Q_1 = n$ and $Q_{k+1} = nQ_k - \beta_k Q_{k-1}$, where $\beta_k = \gamma_k/\gamma_{k-1}$, with $\gamma_k = \int n^k P_k$. The data is as follows:

	1	2	3	4	5	6	7	8
c_k	1	3	12	55	273	1428	7752	43263
γ_k	1	2	3	11/2	26/3	170/11	17.19/13	19.23/10
β_k	1	2	3/2	11/6	52/33	15.17/11.13	11.19/130	13.23/170

This suggests the following general formula:

$$\beta_k = \begin{cases} \dfrac{3(3k-1)(3k+2)}{4(2k-1)(2k+1)} & (k \text{ even}) \\ \\ \dfrac{3(3k-2)(3k+1)}{4(2k-1)(2k+1)} & (k \text{ odd}) \end{cases}$$

The problem can be probably investigated by using well-known techniques. Our main problem is of course: what is the analogue of Theorem 7.3 for H_n^+?

Let us also mention that the computation of the orthogonal polynomials for H_n, H_n^* looks like a quite difficult problem. Probably the good framework here is that of the quantum groups $H_n^{(s)}$ from [18], because at $s = 2, \infty$ we have H_n, H_n^*.

We have as well the following question: is there a quantum group/planar algebra proof of Theorem 7.3, in the cases B_n^+, S_n^+? For O_n^+ this was done in Theorem 5.1.

We have seen in the previous section that the quantum group H_n^+ is somehow of a more complicated nature than the other quantum groups under consideration.

In this section we restrict attention to O_n^+, B_n^+, S_n^+, and we further rearrange the formulae in Theorem 6.3. The idea comes from the formula of O_n^+. Indeed, the numbers f_{kr} for O_n^+ count the $\mathcal{P}_{o^+}$ diagrams with $2r$ upper points and $2k$ lower points, with the property that each upper point is paired with a lower point. This kind of diagrams, called "epi" in the paper of Jones, Shlyakhtenko and Walker [105], have the following generalization.

Definition 15.30. *Let $\mathcal{P}$ be a category of partitions, and let $0 \leq r \leq k$.*

(1) *We let $\mathcal{P}^r(k)$ be the set of partitions $\sigma \in \mathcal{P}(r, k)$, with $0 \leq r \leq k$, such that each upper point is connected to lower points only, and to at least one of them.*

(2) *The elements of $\mathcal{P}^r(k)$ are called "epi". We let $\mathcal{P}^+(k) = \cup_{r=0}^k \mathcal{P}^r(k)$. For an epi $\sigma \in \mathcal{P}^r(k)$, we denote by $r(\sigma) = r$ the number of its upper legs.*

With these notations, we can now state and prove our main result. This is a global formula for the Gram determinants associated to the quantum groups O_n^+, B_n^+, S_n^+.

Theorem 15.31. *For O_n^+, B_n^+, S_n^+ we have the formula*

$$\det(G_{kn}) = n^{a_k} \prod_{\sigma \in \mathcal{P}^+(k)} \frac{F_{r(\sigma)}}{F_{r(\sigma)-1}}$$

where $F_r = P_{r/2}, Q_{r/2}, R_r$ are the corresponding extended orthogonal polynomials.

Proof. Observe first that the F_r quantities in the statement make indeed sense. This is because the epi for O_n^+, B_n^+ must have an even number of upper legs.

(1) For O_n^+ we have $f_{sr}^1 = \#\mathcal{P}^{2r}(2s)$, so the formula in Theorem 6.3 becomes:

$$\det(G_{kn}) = n^{a_k} \prod_{r=0}^{[k/2]} P_r(n)^{f_{k/2,r} - f_{k/2,r+1}} = n^{a_k} \prod_{r=0}^{[k/2]} P_r(n)^{\#\mathcal{P}^{2r}(k) - \#\mathcal{P}^{2r+2}(k)}$$

Now since we have $\mathcal{P}^+(k) = \cup_{r=0}^{[k/2]} \mathcal{P}^{2r}(k)$, we obtain the formula in the statement:

$$\det(G_{kn}) = n^{a_k} \prod_{r=0}^{[k/2]} \left(\prod_{\sigma \in \mathcal{P}^{2r}(k)} \frac{Q_r(n)}{P_{r-1}(n)} \right) = n^{a_k} \prod_{\sigma \in \mathcal{P}^+(k)} \frac{P_{r(\sigma)/2}(n)}{P_{r(\sigma)/2-1}(n)}$$

(2) For B_n^+ the epi have, according to our definitions, singletons only in the lower row. Thus these epi can be counted as function of those for O_n^+, and we get:

$$\det(G_{kn}) = n^{a_k} \prod_{r=0}^{[k/2]} Q_r(n)^{\sum_{l=1}^{[k/2]} \binom{k}{2l} d_{lr}^1} = n^{a_k} \prod_{r=0}^{[k/2]} Q_r(n)^{\#\mathcal{P}^{2r}(k) - \#\mathcal{P}^{2r+2}(k)}$$

A similar manipulation as in (1) gives now the formula in the statement.

(3) For S_n^+ the epi are in standard bijection (via fatenning/collapsing of neighbors) with the epi for O_n^+. Thus the formula in Theorem 6.3 becomes:

$$\det(G_{kn}) = n^{a_k} \prod_{r=0}^{k} R_r(n)^{d_{kr}^1} = n^{a_k} \prod_{r=0}^{k} R_r(n)^{\#\mathcal{P}^r(k) - \#\mathcal{P}^{2r+1}(k)}$$

Once again, a similar manipulation as in (1) gives the formula in the statement. □

Observe that the quantum group H_n^+ cannot be included into the above general theorem, and this for 2 reasons: first, because the orthogonal polynomial interpretation of the polynomials appearing in Theorem 6.3. fails, cf. the previous section, and second, because the epi interpretation of the exponents appearing in Theorem 6.3 seems to fail as well.

We have seen in this paper that the Gram matrix determinants have a natural interpretation in the easy quantum group framework, developed in [25], [18], [19], [20]. The known computations, that we partly extended, simplified, or rearranged in this paper, provide a complete set of formulae for the main examples of easy quantum groups.

Our conjecture is that these Gram determinants should have general decompositions of type $\det(G_{kn}) = \prod_{\pi\in\mathcal{P}(k)} \varphi(\pi)$. More precisely, the situation here is as follows:

(1) For S_n, H_n, H_n^* the conjecture holds, with $\varphi(\pi) = n!/(n - |\pi|)!$.
(2) For O_n, B_n, O_n^* we have a decomposition result, but over Young diagrams.
(3) For O_n^+, B_n^+, S_n^+ we have a decomposition result, but over the associated epi.

The remaining problem is to find the correct surjective maps for (2,3), i.e. the correct surjections from diagrams/epi to partitions. Of course, this question is not very clearly formulated. The main problem is probably to understand the behavior of the Gram matrix determinants in relation with the liberation operation $G_n \to G_n^+$. Indeed, we expect in this situation the contributions φ to be related by a kind of induction/restriction procedure.

In addition to the concrete computations performed in this paper, let us mention that there are as well some quite heavy, abstract methods, that we haven't really tried yet. First, the inclusion $G_n \subset G_n^+$ gives rise to a planar algebra module in the sense of Jones [104], and our above "liberation conjecture" can be understood as saying that the Gram matrix combinatorics behaves well with respect to this planar module structure. And second, modulo the orthogonal polynomial issues discussed in the previous section, some useful tools should come from the analytic theory of the Bercovici-Pata bijection [30].

16. Weingarten calculus

We discuss here the integration over the closed subgroups $G \subset U_N$, first in the general case, and then in the easy case.

As a main application, we will extend the character results from the previous section to the truncated characters, which are defined as follows:

Definition 16.1. *Given a closed subgroup $G \subset U_N$, the variable*

$$\chi_t(g) = \sum_{i=1}^{[tN]} g_{ii}$$

is called truncation of the main character, with parameter $t \in (0, 1]$.

Obviously we cannot use here the same method as for the characters, which was based on the following formula, which does not apply beyond the $t = 1$ case:

$$\int_G \chi_1^k = \dim(Fix(\pi^{\otimes k}))$$

We will still use, however, the moment method, in order to investigate the truncated characters χ_t.

The first step, which is something trivial, is as follows:

Proposition 16.2. *The moments of the truncated characters are given by*

$$\int_G \chi_1^k = \sum_{i_1=1}^{[tN]} \cdots \sum_{i_k=1}^{[tN]} \int_G g_{i_1 i_1}^{e_1} \ldots g_{i_k i_k}^{e_k} dg$$

where $k = e_1 \ldots e_k$ is our exponent, with $e_i \in \{\circ, \bullet\}$ as usual.

Proof. This is clear from the definition of χ_t, namely:

$$\chi_t(g) = \sum_{i=1}^{[tN]} g_{ii}$$

Indeed, the complex conjugate of χ_t is given by:

$$\bar{\chi}_t(g) = \sum_{i=1}^{[tN]} \bar{g}_{ii}$$

Thus, raising to power k and integrating leads to the formula in the statement. □

Summarizing, in order to advance, we are led to the computation of the arbitrary polynomial integrals over our compact group $G \subset U_N$:

$$\int_G g_{i_1j_1}^{e_1} \ldots g_{i_kj_k}^{e_k} dg = ?$$

Let us first discuss this question in general, for an arbitary closed subgroup $G \subset U_N$.

By using Peter-Weyl theory, we are led to the following result:

Theorem 16.3. *The polynomial integrals over a closed subgroup*

$$G \subset U_N$$

are given by the formula

$$\int_G g_{i_1j_1}^{e_1} \ldots g_{i_kj_k}^{e_k} dg = \sum_{\pi,\sigma \in D_k} \delta_\pi(i)\delta_\sigma(j) W_k(\pi, \sigma)$$

for any colored integer $k = e_1 \ldots e_k$ and any multi-indices i, j, where D_k is a linear basis of $Fix(\pi^{\otimes k})$,

$$\delta_\pi(i) = < \pi, e_{i_1} \otimes \ldots \otimes e_{i_k} >$$

and $W_k = G_k^{-1}$, with:

$$G_k(\pi, \sigma) = < \pi, \sigma >$$

In the case where G_k is not invertible, we must use the quasi-inverse.

Proof. Consider the integrals in the statement, with $k = e_1 \ldots e_k$ being fixed, and with the multi-indices $i = (i_1, \ldots, i_k)$ and $j = (j_1, \ldots, j_k)$ varying:

$$P_{ij}^k = \int_G g_{i_1j_1}^{e_1} \ldots g_{i_kj_k}^{e_k} dg$$

We know from the Peter-Weyl theory from section 13 above that these integrals form altogether the orthogonal projection onto $Fix(\pi^{\otimes k})$. Thus, we have:

$$\begin{aligned} & P^k \\ = \ & Proj(Fix(\pi^{\otimes k})) \\ = \ & Proj(span(D_k)) \end{aligned}$$

Consider now the following linear map, with $D_k = \{\xi_\pi\}$ being as in the statement:

$$E(x) = \sum_{\pi \in D_k} < x, \xi_\pi > \xi_\pi$$

Let us denote as well by W the inverse of E to the following space:

$$span\left(T_\pi \middle| \pi \in D_k\right)$$

By a standard linear algebra computation, it follows that we have:

$$P = WE$$

But the above restriction is the linear map given by G_k, and so W is the linear map given by W_k, and this gives the result. □

In the easy group case, the above formula simplifies, as follows:

Theorem 16.4. *For an easy group $G \subset U_N$, coming from a category of partitions*

$$D = (D(k, l))$$

we have the Weingarten integration formula

$$\int_G u_{i_1 j_1}^{e_1} \ldots u_{i_k j_k}^{e_k} = \sum_{\pi, \sigma \in D(k)} \delta_\pi(i) \delta_\sigma(j) W_{kN}(\pi, \sigma)$$

for any $k = e_1 \ldots e_k$ and any i, j, where $D(k) = D(\emptyset, k)$, δ are usual Kronecker symbols, and $W_{kN} = G_{kN}^{-1}$, with

$$G_{kN}(\pi, \sigma) = N^{|\pi \vee \sigma|}$$

where $|.|$ is the number of blocks.

Proof. With notations from Theorem 16.3, the Kronecker symbols are given by:

$$\begin{aligned} & \delta_{\xi_\pi}(i) \\ = \ & < \xi_\pi, e_{i_1} \otimes \ldots \otimes e_{i_k} > \\ = \ & \delta_\pi(i_1, \ldots, i_k) \end{aligned}$$

The Gram matrix being as well the correct one, we obtain the result. □

With the above formula in hand, we can go back now to the question of computing the laws of truncated characters. First, we have the following formula:

Theorem 16.5. *The moments of truncated characters are given by the formula*

$$\int_G (g_{11} + \ldots + g_{ss})^k = Tr(W_{kN} G_{ks})$$

where G_{kN} and $W_{kN} = G_{kN}^{-1}$ are the associated Gram and Weingarten matrices.

Proof. We have indeed the following computation:

$$\begin{aligned}
&\int_G(g_{11}+\ldots+g_{ss})^k\\
=\ &\sum_{i_1=1}^{s}\ldots\sum_{i_k=1}^{s}\int_G g_{i_1i_1}\ldots g_{i_ki_k}\\
=\ &\sum_{\pi,\sigma\in D(k)}W_{kN}(\pi,\sigma)\sum_{i_1=1}^{s}\ldots\sum_{i_k=1}^{s}\delta_\pi(i)\delta_\sigma(i)\\
=\ &\sum_{\pi,\sigma\in D(k)}W_{kN}(\pi,\sigma)G_{ks}(\sigma,\pi)\\
=\ &Tr(W_{kN}G_{ks})
\end{aligned}$$

Thus, we have obtained the formula in the statement. □

In order to process now the above formula, things are quite technical, and won't work well in general.

We must impose here an uniformity condition, as follows:

Theorem 16.6. *For an easy group $G=(G_N)$, coming from a category of partitions*

$$D\subset P$$

the following conditions are equivalent:

(1) *$G_{N-1}=G_N\cap U_{N-1}$, via the embedding $U_{N-1}\subset U_N$ given by:*

$$u\to diag(u,1)$$

(2) *$G_{N-1}=G_N\cap U_{N-1}$, via the N possible diagonal embeddings:*

$$U_{N-1}\subset U_N$$

(3) *D is stable under the operation which consists in removing blocks.*

If these conditions are satisfied, we say that $G=(G_N)$ is "uniform".

Proof. We use the general easiness theory from section 15 above.

(1) $\iff$ (2) This is something standard, coming from the inclusion:

$$S_N\subset G_N$$

Indeed, this inclusion makes everything S_N-invariant.

The result follows as well from the proof of (1) $\iff$ (3) below, which can be converted into a proof of (2) $\iff$ (3), in the obvious way.

(1) $\iff$ (3) Given a subgroup $K \subset U_{N-1}$, with fundamental corepresentation u, consider the $N \times N$ matrix:

$$v = diag(u, 1)$$

Our claim is that for any $\pi \in P(k)$ we have:

$$\xi_\pi \in Fix(v^{\otimes k}) \iff \xi_{\pi'} \in Fix(v^{\otimes k'}), \forall \pi' \in P(k'), \pi' \subset \pi$$

In order to prove this, we must study the condition on the left. We have:

$$\begin{aligned}
& \xi_\pi \in Fix(v^{\otimes k}) \\
\iff \quad & (v^{\otimes k}\xi_\pi)_{i_1 \ldots i_k} = (\xi_\pi)_{i_1 \ldots i_k}, \forall i \\
\iff \quad & \sum_j (v^{\otimes k})_{i_1 \ldots i_k, j_1 \ldots j_k} (\xi_\pi)_{j_1 \ldots j_k} = (\xi_\pi)_{i_1 \ldots i_k}, \forall i \\
\iff \quad & \sum_j \delta_\pi(j_1, \ldots, j_k) v_{i_1 j_1} \ldots v_{i_k j_k} = \delta_\pi(i_1, \ldots, i_k), \forall i
\end{aligned}$$

Now let us recall that our corepresentation has the special form:

$$v = diag(u, 1)$$

We conclude from this that for any index $a \in \{1, \ldots, k\}$, we must have:

$$i_a = N \implies j_a = N$$

With this observation in hand, if we denote by i', j' the multi-indices obtained from i, j obtained by erasing all the above $i_a = j_a = N$ values, and by $k' \leq k$ the common length of these new multi-indices, our condition becomes:

$$\sum_{j'} \delta_\pi(j_1, \ldots, j_k)(v^{\otimes k'})_{i'j'} = \delta_\pi(i_1, \ldots, i_k), \forall i$$

Here the index j is by definition obtained from j' by filling with N values. In order to finish now, we have two cases, depending on i, as follows:

Case 1. Assume that the index set $\{a | i_a = N\}$ corresponds to a certain subpartition $\pi' \subset \pi$. In this case, the N values will not matter, and our formula becomes:

$$\sum_{j'} \delta_\pi(j'_1, \ldots, j'_{k'})(v^{\otimes k'})_{i'j'} = \delta_\pi(i'_1, \ldots, i'_{k'})$$

Case 2. Assume now the opposite, namely that the set $\{a | i_a = N\}$ does not correspond to a subpartition $\pi' \subset \pi$. In this case the indices mix, and our formula reads:

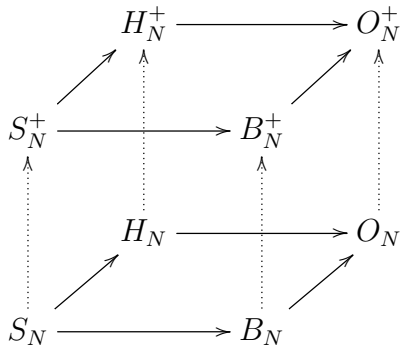
$$0 = 0$$

Thus, we are led to $\xi_{\pi'} \in Fix(v^{\otimes k'})$, for any subpartition $\pi' \subset \pi$, as claimed.

Now with this claim in hand, the result follows from Tannakian duality. $\square$

For classification purposes the uniformity axiom is something very natural and useful, substantially cutting from complexity, and we have the following result, from [25]:

Theorem 16.7. *The classical and free uniform orthogonal easy quantum groups, with inclusions between them, are as follows:*

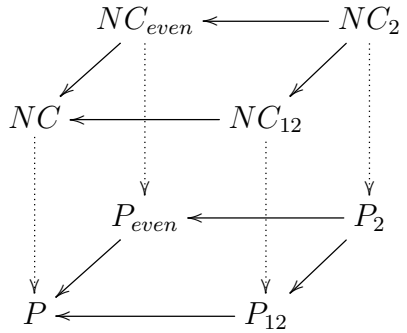


Moreover, this is an intersection/easy generation diagram, in the sense that for any of its square subdiagrams

$$P \subset Q, R \subset S$$

we have $P = Q \cap R$ *and* $\{Q, R\} = S$.

Proof. We know that the quantum groups in the statement are indeed easy and uniform, the corresponding categories of partitions being as follows:



Since this latter diagram is an intersection and generation diagram, we conclude that we have an intersection and easy generation diagram of quantum groups, as stated.

Regarding now the classification, consider an easy quantum group:

$$S_N \subset G_N \subset O_N$$

This most come from a category:

$$P_2 \subset D \subset P$$

By doing some combinatorics, we can see that D is uniquely determined by the subset $L \subset \mathbb{N}$ consisting of the sizes of the blocks of the partitions in D, with the admissible sets being as follows:

(1) $L = \{2\}$, producing O_N.
(2) $L = \{1, 2\}$, producing B_N.
(3) $L = \{2, 4, 6, \ldots\}$, producing H_N.
(4) $L = \{1, 2, 3, \ldots\}$, producing S_N.

In the free case, $S_N^+ \subset G_N \subset O_N^+$, the situation is quite similar, the admissible sets being once again the above ones, producing this time $O_N^+, B_N^+, H_N^+, S_N^+$. See [25]. □

In the unitary case, the result is more complicated.

By getting back now to the truncated characters, we have the following result:

Theorem 16.8. *For a uniform easy group $G = (G_N)$, we have the formula*

$$\lim_{N\to\infty} \int_{G_N} \chi_t^k = \sum_{\pi \in D(k)} t^{|\pi|}$$

with $D \subset P$ being the associated category of partitions.

Proof. We use the general moment formula from Theorem 16.5 above. With $s = [tN]$, this formula becomes:

$$\int_{G_N} \chi_t^k = Tr(W_{kN} G_{k[tN]})$$

The point now is that in the uniform case the Gram and Weingarten matrices are asymptotically diagonal, and this leads to the formula in the statement. □

We can now improve our quantum group results, as follows:

Theorem 16.9. *With $N \to \infty$, the laws of truncated characters are as follows:*

(1) *For O_N we obtain the Gaussian law g_t.*
(2) *For U_N we obtain the complex Gaussian law G_t.*
(3) *For S_N we obtain the Poisson law p_t.*
(4) *For H_N we obtain the Bessel law b_t.*
(5) *For H_N^s we obtain the generalized Bessel law b_t^s.*
(6) *For K_N we obtain the complex Bessel law B_t.*

Also, for B_N, C_N and for Sp_N we obtain modified normal laws.

Proof. We use the formula in Theorem 16.8 above, namely:

$$\lim_{N\to\infty} \int_{G_N} \chi_t^k = \sum_{\pi \in D(k)} t^{|\pi|}$$

By doing now some combinatorics, this gives the results. □

Let $\mathcal{P}_s$ be the category of all partitions. That is, $\mathcal{P}_s(k,l)$ is the set of partitions between an upper row of k points and a lower row of l points, and the categorical operations are the horizontal and vertical concatenation, and the upside-down turning.

A category of partitions $\mathcal{P} \subset \mathcal{P}_s$ is by definition a collection of sets $\mathcal{P}(k,l) \subset \mathcal{P}_s(k,l)$, which is stable under the categorical operations. We have the following examples.

Proposition 16.10. *The following are categories of partitions:*

(1) $\mathcal{P}_o/\mathcal{P}_o^+$*: all pairings/all noncrossing pairings.*
(2) $\mathcal{P}_o^*$*: pairings with each string having an odd leg and an even leg.*
(3) $\mathcal{P}_b/\mathcal{P}_b^+$*: singletons plus pairings/noncrossing pairings.*
(4) $\mathcal{P}_s/\mathcal{P}_s^+$*: all partitions/all noncrossing partitions.*
(5) $\mathcal{P}_h/\mathcal{P}_h^+$*: partitions/noncrossing partitions with blocks of even size.*
(6) $\mathcal{P}_h^*$*: partitions with blocks having the same number of odd and even legs.*

Proof. This is clear from definitions. Note that $\mathcal{P}_g^\times$ corresponds via Tannakian duality [196], [197] to the easy quantum group $G^\times = (G_n^\times)$, with the notations in [18], [25]. □

We use the notation $\mathcal{P}(k) = \mathcal{P}(0,k)$. We denote by $\vee$ and $\wedge$ the set-theoretic sup and inf of partitions, always taken with respect to $\mathcal{P}_s$, and by $|.|$ the number of blocks.

Definition 16.11. *Associated to any category of partitions $\mathcal{P}$ and to any numbers $k, n \geq 0$ are the following matrices, with entries indexed by $\pi, \sigma \in \mathcal{P}(k)$:*

(1) *Gram matrix:* $G_{kn}(\pi,\sigma) = n^{|\pi\vee\sigma|}$.
(2) *Weingarten matrix:* $W_{kn} = G_{kn}^{-1}$.

In order for G_{kn} to be invertible, n must be big enough, and $n \geq k$ is known to be sufficient. The precise bounds depend on the category of partitions, and can be deduced from the various explicit formulae of $\det(G_{kn})$, to be given later on in this paper.

The interest in the above matrices comes from the fact that in the case $\mathcal{P} = \mathcal{P}_g^\times$, they describe the integration over the corresponding easy quantum group $G_n^\times$.

Theorem 16.12. *We have the Weingarten formula*

$$\int_{G_n^\times} u_{i_1j_1} \ldots u_{i_kj_k}\, du = \sum_{\pi,\sigma\in\mathcal{P}_g^\times(k)} \delta_\pi(i)\delta_\sigma(j) W_{kn}(\pi,\sigma)$$

where the δ symbols are 0 or 1, depending on whether the indices fit or not.

Proof. This follows by using a classical argument from [189], [50]. See [18], [25]. □

The exact computation of the Weingarten matrix is a quite subtle problem. A precise result is available only in the finite group case, where the formula is given in terms of the Möbius function μ on $\mathcal{P}$ as follows.

Proposition 16.13. *For S_n, H_n the Weingarten function is given by*

$$W_{kn}(\pi,\sigma)=\sum_{\tau\leq\pi\wedge\sigma}\mu(\tau,\pi)\mu(\tau,\sigma)\frac{(n-|\tau|)!}{n!}$$

and satisfies $W_{kn}(\pi,\sigma)=n^{-|\pi\wedge\sigma|}(\mu(\pi\wedge\sigma,\pi)\mu(\pi\wedge\sigma,\sigma)+O(n^{-1}))$.

Proof. The first assertion follows from the Weingarten formula: in that formula the integrals on the left are known, and this allows the computation of the right term, via the Möbius inversion formula. The second assertion follows from the first one. □

In the general case we have the following result, which is useful for applications.

Proposition 16.14. *For $\pi\leq\sigma$ we have the estimate*

$$W_{kn}(\pi,\sigma)=n^{-|\pi|}(\mu(\pi,\sigma)+O(n^{-1}))$$

and for π,σ arbitrary we have $W_{kn}(\pi,\sigma)=O(n^{|\pi\vee\sigma|-|\pi|-|\sigma|})$.

Proof. Once again this follows by using a classical argument, see [18]. □

In this paper, we will be mainly interested in the computation of $\det(G_{kn})$. Let us being with some simple observations, coming from definitions.

Proposition 16.15. *Let $D_k(n)=\det(G_{kn})$, viewed as element of $\mathbb{Z}[n]$.*

(1) *D_k is monic, of degree $s_k=\sum_{\pi\in\mathcal{P}(k)}|\pi|$.*

(2) *We have $n^{b_k}|D_k$, where $b_k=\#\mathcal{P}(k)$.*

Proof. (1) This follows from $|\pi\vee\sigma|\leq|\pi|$, with equality if and only if $\sigma\leq\pi$. Indeed, from the inequality we get $\deg(D_k)\leq s_k$. Now the coefficient of n^{s_k} is the signed number of permutations $f:\mathcal{P}(k)\to\mathcal{P}(k)$ satisfying $f(\pi)\leq\pi$ for any π, and since there is only one such permutation, namely the identity, we obtain that this coefficient is 1.

(2) This is clear from the definition of D_k, and from $|\pi\vee\sigma|\geq 1$. □

The above result raises the question of computing the numbers $b_k=\#\mathcal{P}(k)$ and $s_k=\sum_{\pi\in\mathcal{P}(k)}|\pi|$. It is convenient here to introduce as well the related numbers $m_k=s_k/b_k$ and $a_k=2s_k-kb_k=(2m_k-k)b_k$, which will appear several times in what follows.

Proposition 16.16. *The numbers b_k,s_k,m_k,a_k are as follows:*

(1) *O_n,O_n^*,O_n^+: $b_{2l}=(2l)!!,l!$, $\frac{1}{l+1}\binom{2l}{l}$, $s_{2l}=lb_{2l}$, $m_{2l}=l$, $a_{2l}=0$.*

(2) *S_n: $b_k=Bell$, $s_k=b_{k+1}-b_k$, $m_k=\frac{b_{k+1}}{b_k}-1$, $a_k=2b_{k+1}-(k+2)b_k$.*

(3) *S_n^+: $b_k=\frac{1}{k+1}\binom{2k}{k}$, $s_k=\frac{1}{2}\binom{2k}{k}$, $m_k=\frac{k+1}{2}$, $a_k=b_k$.*

(4) *H_n^+: $b_{2l}=\frac{1}{2l+1}\binom{3l}{l}$, $s_{2l}=\binom{3l-1}{l-1}$, $m_{2l}=\frac{2l+1}{3}$, $a_{2l}=-2\binom{3l-1}{l-2}$.*

Proof. All these results are well-known. □

For the remaining quantum groups, namely B_n, B_n^+, H_n, H_n^*, the numbers b_k, s_k, m_k, a_k are given by quite complicated formulae. The best approach to their computation is via the trace of the Gram matrix, and its analytic interpretations.

So, let us first reformulate Proposition 2.1, in the following way.

Proposition 16.17. *With $D_k(n) = \det(G_{kn})$ and $T_k(t) = Tr(G_{kt})$, we have:*

(1) $D_k(n) = n^{s_k}(1 + O(n^{-1}))$ *as* $n \to \infty$, *where* $s_k = T_k'(1)$.

(2) $D_k(n) = O(n^{b_k})$ *as* $n \to 0$, *where* $b_k = T_k(1)$.

Proof. This is indeed just a reformulation of Proposition 2.1, using a variable t around 1. Note that in (2) we regard the variable n as a formal parameter, going to 0. □

The trace can be understood in terms of the associated Stirling numbers.

Proposition 16.18. *We have the formula*

$$T_k(t) = \sum_{r=1}^{k} S_{kr} t^r$$

where $S_{kr} = \#\{\pi \in \mathcal{P}(k) : |\pi| = r\}$ are the Stirling numbers.

Proof. This is clear from definitions. □

Another interpretation of the trace, analytic this time, is as follows.

Proposition 16.19. *For any $t \in (0, 1]$ we have the formula*

$$T_k(t) = \lim_{n\to\infty} \int_{G_n^\times} \chi_t^k$$

where $\chi_t = \sum_{i=1}^{[tn]} u_{ii}$ are the truncated characters of the quantum group.

Proof. As explained in [25], [18], this follows from the Weingarten formula. □

In general, the Stirling numbers S_{kr} and the trace $T_k(t)$ are given by quite complicated formulae, unless we are in the situation of one of the quantum groups in Proposition 2.2. Here these invariants are well-known in the O, S cases, and for H^+ we have:

$$T_{2l}(t) = \sum_{r=1}^{l} \frac{1}{r}\binom{l-1}{r-1}\binom{2l}{r-1} t^r$$

See [13]. In general now, the conceptual result concerns the asymptotic measures of truncated characters, i.e. the probability measures μ_t satisfying:

$$T_k(t) = \int x^k d\mu_t(x)$$

We have the following result:

Theorem 16.20. *The asymptotic measures of truncated characters are as follows:*

(1) S_n/S_n^+*: Poisson/free Poisson.*
(2) O_n/O_n^+*: Gaussian/semicircular.*
(3) H_n/H_n^+*: Bessel/free Bessel.*
(4) B_n/B_n^+*: shifted Gaussian/shifted semicircular.*
(5) O_n^*/H_n^**: symmetrized Rayleigh/squeezed ∞-Bessel.*

Proof. The one-parameter measures in the statement are best found via a direct computation, by using classical and free cumulants. See [25], [18], [19]. □

We discuss now the explicit computation of the Gram determinants. The basic formula here is as follows.

Theorem 16.21. *For S_n, H_n, H_n^* we have*

$$\det(G_{kn}) = \prod_{\pi\in\mathcal{P}(k)} \frac{n!}{(n-|\pi|)!}$$

where $|.|$ is the number of blocks.

Proof. We use the fact that the partitions have the property of forming semilattices under $\vee$. The proof uses the upper triangularization procedure together with the explicit knowledge of the Möbius function on $\mathcal{P}(k)$. Consider the following matrix, obtained by making determinant-preserving operations:

$$G'_{kn}(\pi,\sigma) = \sum_{\pi\leq\tau} \mu(\pi,\tau) n^{|\tau\vee\sigma|}$$

It follows from the Möbius inversion formula that we have:

$$G'_{kn}(\pi,\sigma) = \begin{cases} n(n-1)\ldots(n-|\sigma|+1) & \text{if } \pi\leq\sigma \\ 0 & \text{if not} \end{cases}$$

Thus the matrix is upper triangular, and by computing the product on the diagonal we obtain the formula in the statement. □

A first remarkable feature of the above result is that the determinant for S_n, H_n, H_n^* can be computed from the trace: indeed, the Gram trace gives the Stirling numbers, which in turn give the Gram determinant. However, the connecting formula is quite complicated, so let us just record here an improvement of the first estimate in Proposition 2.3.

Proposition 16.22. *With $D_k(n) = \det(G_{kn})$ and $T_k(t) = Tr(G_{kt})$ we have*

$$D_k(n) = n^{s_k}\left(1 - \frac{z_k}{2}\, n^{-1} + O(n^{-2})\right)$$

where $s_k = T_k'(1)$ and $z_k = T_k''(1)$.

Proof. In terms of Stirling numbers, the formula in Theorem 3.1 reads:

$$D_k(n)=\prod_{r=1}^{k}\left(\frac{n!}{(n-r)!}\right)^{S_{kr}}$$

We use now the following basic estimate:

$$\frac{n!}{(n-r)!}=n^r\prod_{s=1}^{r-1}\left(1-\frac{s}{n}\right)=n^r\left(1-\frac{r(r-1)}{2}\,n^{-1}+O(n^{-2})\right)$$

Together with $T_k(t)=\sum_{r=1}^{k}S_{kr}t^r$, this gives the result. □

The above discussion raises the general question on whether the Gram determinant can be computed or not from the Gram trace, or from the measures in Theorem 2.6.

Since the connecting formula for S_n,H_n,H_n^* is already quite complicated, let us formulate for the moment a more modest conjecture, as follows.

Conjecture 16.23. *For any easy quantum group we have a formula of type*

$$\det(G_{kn})=\prod_{\pi\in\mathcal{P}(k)}\varphi(\pi)$$

with the "contributions" being given by an explicit function $\varphi:\mathcal{P}(k)\to\mathbb{Q}(n)$.

This statement is of course quite vague, depending of the meaning of the above word "explicit". As already mentioned, one would expect φ to come from the Gram trace, or from the Stirling numbers, or, even better, from the measures in Theorem 2.6. Such a decomposition could potentially clarify the behavior of the Gram determinants under the "liberation" procedure $G\to G^+$.

This kind of general question appears to be quite difficult. In what follows we will obtain some evidence towards such general decomposition results.

We discuss now the cases O,B,O^*. Here the combinatorics is that of the Young diagrams. We denote by $|.|$ the number of boxes, and we use quantity f^λ, which gives the number of standard Young tableaux of shape λ.

Theorem 16.24. *For O_n we have*

$$\det(G_{kn})=\prod_{|\lambda|=k/2}f_n(\lambda)^{f^{2\lambda}}$$

where $f_n(\lambda)=\prod_{(i,j)\in\lambda}(n+2j-i-1)$.

Proof. This follows from the results of Collins and Matsumoto [46]. Indeed, it is known from there that the Gram matrix is diagonalizable, as follows:

$$G_{kn}=\sum_{|\lambda|=k/2}f_n(\lambda)P_{2\lambda}$$

Here $1 = \Sigma P_{2\lambda}$ is the standard partition of unity associated to the Young diagrams having $k/2$ boxes, and the coefficients $f_n(\lambda)$ are those in the statement. Now since we have $Tr(P_{2\lambda}) = f^{2\lambda}$, this gives the result. □

Theorem 16.25. *For B_n we have*

$$\det(G_{kn}) = n^{a_k} \prod_{|\lambda| \leq k/2} f_n(\lambda)^{\binom{k}{2|\lambda|} f^{2\lambda}}$$

where $a_k = \sum_{\pi \in \mathcal{P}(k)} (2|\pi| - k)$, and $f_n(\lambda) = \prod_{(i,j) \in \lambda} (n + 2j - i - 2)$.

Proof. We recall from [25] that we have an isomorphism $B_n \simeq O_{n-1}$, given by $u = v + 1$, where u, v are the fundamental representations of B_n, O_{n-1}. We get:

$$Fix(u^{\otimes k}) = Fix\left((v+1)^{\otimes k}\right) = Fix\left(\sum_{r=0}^{k} \binom{k}{r} v^{\otimes r}\right)$$

Now if we denote by $\det', f'$ the objects in Theorem 4.1, we obtain:

$$\det(G_{kn}) = n^{a_k} \prod_{r=1}^{k} \det{}'(G_{r,n-1})^{\binom{k}{r}} = n^{a_k} \prod_{r=1}^{k} \left(\prod_{|\lambda| = r/2} f'_{n-1}(\lambda)^{f^{2\lambda}} \right)^{\binom{k}{r}}$$

This gives the formula in the statement. □

The computation of polynomial integrals over the orthogonal group O_n is a key problem in mathematical physics. These integrals are indeed known to appear in a wealth of concrete situations, coming from random matrices, lattice models, combinatorics.

The standard approach to the computation of such integrals is via the Weingarten formula. This formula, originating from Weingarten's paper [189], and worked out by Collins in [45], then by Collins and Śniady in [50], is an identity of the following type:

$$\int_{O_n} u_{i_1 j_1} \ldots u_{i_{2k} j_{2k}} \, du = \sum_{\pi, \sigma} \delta_\pi(i) \delta_\sigma(j) W_{kn}(\pi, \sigma)$$

Here the sum is over all pairings of $\{1, \ldots, 2k\}$, also called Brauer diagrams [39], and the delta symbols, describing the coupling between indices and diagrams, are 0 or 1. As for W_{kn}, this is the key combinatorial ingredient: the Weingarten function.

The exact or asymptotic computation of W_{kn} is a quite subtle problem, and several results have been recently obtained on this subject.

The starting point for the considerations in the present paper is the following elementary reformulation of the Weingarten formula:

$$\int_{O_n}\prod_{i=1}^{n}\prod_{j=1}^{n}u_{ij}^{a_{ij}}\,du=\sum_{\pi,\sigma}\delta_\pi(a_l)\delta_\sigma(a_r)W_{kn}(\pi,\sigma)$$

Here $a\in M_n(\mathbb{N})$ is the matrix of exponents appearing in the original Weingarten formula, and the delta symbols are once again 0 or 1. This formula is of course fully equivalent to the original Weingarten one, but the slight difference in the formulation leads to some potentially interesting consequences, that we will explore in this paper.

We are interested in the computation of arbitary polynomial integrals over the orthogonal group O_n. These are best introduced in a "rectangular way", as follows:

Definition 16.26. *Associated to any matrix $a\in M_{p\times q}(\mathbb{N})$ is the integral*

$$I(a)=\int_{O_n}\prod_{i=1}^{p}\prod_{j=1}^{q}u_{ij}^{a_{ij}}\,du$$

with respect to the Haar measure of O_n, where $n\geq p,q$.

We can of course complete our matrix with 0 values, as to always deal with square matrices, $a\in M_n(\mathbb{N})$. However, the parameters p,q are very useful, because they measure the "complexity" of the problem, as shown for instance by the result below.

Let $x!!=(x-1)(x-3)(x-5)\ldots$, with the product ending at 1 or 2. We have:

Theorem 16.27. *At $p=1$ we have the formula*

$$I\begin{pmatrix}a_1&\ldots&a_q\end{pmatrix}=\varepsilon\cdot\frac{(n-1)!!a_1!!\ldots a_q!!}{(n+\Sigma a_i-1)!!}$$

where $\varepsilon=1$ if all a_i are even, and $\varepsilon=0$ if not.

Proof. This follows from the fact that the first slice of O_n is isomorphic to the real sphere S^{n-1}. Indeed, this gives the following formula:

$$I\begin{pmatrix}a_1&\ldots&a_q\end{pmatrix}=\int_{S^{n-1}}x_1^{a_1}\ldots x_q^{a_q}\,dx$$

This latter integral can be computed by using polar coordinates, and we obtain the formula in the statement. See e.g. [16]. □

Another instructive computation, as well of trigonometric nature, is the one at $n=2$. We have here the following result, which completely solves the problem in this case:

Theorem 16.28. *At $n = 2$ we have the formula*

$$I\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \varepsilon \cdot \frac{(a+d)!!(b+c)!!}{(a+b+c+d+1)!!}$$

where $\varepsilon = 1$ if a, b, c, d are even, $\varepsilon = -1$ is a, b, c, d are odd, and $\varepsilon = 0$ if not.

Proof. When computing the integral over O_2, we can restrict the integration to $SO_2 = S^1$, then further restrict the integration to the first quadrant. We get:

$$I\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \varepsilon \cdot \frac{2}{\pi} \int_0^{\pi/2} (\cos t)^{a+d} (\sin t)^{b+c}\, dt$$

This gives the formula in the statement. □

The above computations might tend to suggest that $I(a)$ always decomposes as a product of factorials. This is far from being true, but in the 2×2 case it is known that $I(a)$ decomposes as a quite reasonable sum of products of factorials.

In this reminder of this paper we discuss the representation theory approach to the computation of $I(a)$. The technology available here is quite advanced, and will lead to a wealth of concrete results about $I(a)$, regarding its vanishing, theoretical poles, and asymptotic behaviour, and notably with a concrete formula for its first order term.

Our main tool is a combinatorial formula for the polynomial integrals over O_n, whose origins go back to Weingarten's paper [189]. The treatment given here follows the papers [45], [50], [46], where this formula was fully formalized, and its true power revealed.

The first remark is that the integrals over O_n of arbitrary polynomial quantities of type $u_{i_1 j_1} \ldots u_{i_s j_s}$ vanish, unless s is even. In what follows, we focus on the $s = 2k$ case.

Let us recall that the pseudo-inverse of a real symmetric matrix G is the unique matrix W satisfying $WGW = W$ and $GWG = G$. If G is invertible, then $W = G^{-1}$.

With this convention, the Weingarten formula is as follows:

Theorem 16.29. *We have the Weingarten formula*

$$\int_{O_n} u_{i_1 j_1} \ldots u_{i_{2k} j_{2k}}\, du = \sum_{\pi,\sigma} \delta_\pi(i) \delta_\sigma(j) W_{kn}(\pi, \sigma)$$

where the various objects on the right are as follows:

(1) *The sum is over all pairings π, σ of the set $\{1, \ldots, 2k\}$.*
(2) *The delta symbols are 0 or 1, depending on whether the indices $i = (i_1, \ldots, i_{2k})$ and $j = (j_1, \ldots, j_{2k})$ fit or not inside the corresponding pairings.*
(3) *W_{kn} is the pseudo-inverse of the matrix $G_{kn}(\pi, \sigma) = n^{loops(\pi,\sigma)}$, where we denote by $loops(\pi, \sigma)$ the number of loops obtained when superposing π, σ.*

Proof. Consider the matrix $P \in M_{n^{2k}}(\mathbb{R})$ formed by all the integrals on the left, with k fixed and i, j varying. It follows from the general theory that P is the orthogonal projection onto the space $Fix(u^{\otimes 2k})$ of fixed vectors of the $2k$-th tensor power of u.

By a well-known result of Brauer [39] the space $Fix(u^{\otimes 2k})$ is spanned by the vectors:

$$\xi_\pi = \Sigma_i \delta_\pi(i) e_{i_1} \otimes \ldots \otimes e_{i_{2k}}$$

Here π ranges over all the pairings of $\{1, \ldots, 2k\}$. Now since the Gram matrix of these vectors is $< \xi_\pi, \xi_\sigma >= G_{kn}(\pi, \sigma)$, when computing P we have to invert this Gram matrix, and we obtain the formula in the statement. □

We refer to [45], [50], [46] for full details regarding the above proof. Let us also mention that the Gram matrix G_{kn} is actually invertible for $n \geq k$. See [50].

Our first task is to convert the above formula, by using our compact notation $I(a)$ for the polynomial integrals over O_n. We restrict attention to the case where Σa_{ij} is even. The result is as follows:

Theorem 16.30. *We have the Weingarten formula*

$$I(a) = \sum_{\pi,\sigma} \delta_\pi(a_l) \delta_\sigma(a_r) W_{kn}(\pi, \sigma)$$

where $k = \Sigma a_{ij}/2$, and where the multi-indices a_l/a_r are defined as follows:

(1) *Start with $a \in M_{p\times q}(\mathbb{N})$, and replace each ij-entry by a_{ij} copies of i/j.*
(2) *Read this matrix in the usual way, as to get the multi-indices a_l/a_r.*

Proof. This is simply a reformulation of Theorem 12.13. Indeed, according to our definitions, the integral in the statement is given by:

$$I(a) = \int_{O_n} \underbrace{u_{11} \ldots u_{11}}_{a_{11}} \underbrace{u_{12} \ldots u_{12}}_{a_{12}} \ldots \underbrace{u_{pq} \ldots u_{pq}}_{a_{pq}} du$$

Thus what we have here is an integral as in Theorem 2.1, the multi-indices being:

$$a_l = (\underbrace{1 \ldots 1}_{a_{11}} \underbrace{1 \ldots 1}_{a_{12}} \ldots \underbrace{p \ldots p}_{a_{pq}})$$

$$a_r = (\underbrace{1 \ldots 1}_{a_{11}} \underbrace{2 \ldots 2}_{a_{12}} \ldots \underbrace{q \ldots q}_{a_{pq}})$$

The result follows now from the Weingarten formula. □

We are now in position of deriving a first general corollary from our study. This extends the vanishing results appearing before:

Proposition 16.31. *We have $I(a) = 0$, unless the matrix a is "admissible", in the sense that all $p + q$ sums on its rows and columns are even numbers.*

Proof. Observe first that the left multi-index associated to a consists of $k_1 = \Sigma a_{1j}$ copies of 1, $k_2 = \Sigma a_{2j}$ copies of 2, and so on, up to $k_p = \Sigma a_{pj}$ copies of p. In the case where one of these numbers is odd we have $\delta_\pi(a) = 0$ for any π, and this gives $I(a) = 0$.

A similar argument with the right multi-index associated to a shows that the sums on the columns of a must be even as well, and we are done. □

A natural question now is whether the converse of Proposition 12.15 holds, and if so, the question of computing the sign of $I(a)$ appears as well. These are both quite subtle questions, and we begin our investigations with a $n \to \infty$ study.

The basic result here, known since [45], [50], states that the Weingarten matrix is asymptotically diagonal, in the sense that we have:

$$W_{kn}(\pi, \sigma) = n^{-k}(\delta_{\pi\sigma} + O(n^{-1/2}))$$

We present below a complete proof for this fact, by following a slightly improved method, which gives a better estimate, along with some concrete bounds:

Theorem 16.32. *The Weingarten matrix is asymptotically diagonal, in the sense that:*

$$W_{kn}(\pi, \sigma) = n^{-k}(\delta_{\pi\sigma} + O(n^{-1}))$$

Moreover, the $O(n^{-1})$ reminder is asymptotically smaller that $(2k/e)^k n^{-1}$.

Proof. It is convenient, for the purposes of this proof, to drop the indices k, n. We know that the Gram matrix is given by $G(\pi, \sigma) = n^{loops(\pi,\sigma)}$, so we have:

$$G(\pi, \sigma) = \begin{cases} n^k & \text{for } \pi = \sigma \\ n, n^2, \ldots, n^{k-1} & \text{for } \pi \neq \sigma \end{cases}$$

Thus the Gram matrix is of the following form, with $||H||_\infty \leq n^{-1}$:

$$G = n^k(I + H)$$

Now recall that for any $K \times K$ matrix X, we have the following lineup of standard inequalities:

$$\begin{aligned} ||X||_\infty &\leq ||X|| \\ &\leq ||X||_2 \\ &\leq K||X||_\infty \end{aligned}$$

In the case of our matrix H, the size is $K = (2k)!!$, so we have:

$$||H|| \leq Kn^{-1}$$

We can use now the following formula:

$$(I + H)^{-1} = I - H + H^2 - H^3 + \ldots$$

We get from this:

$$||I-(I+H)^{-1}||\leq||H||/(1-||H||)$$

Thus we have:

$$\begin{aligned}||I-n^kW||_\infty&=||I-(1+H)^{-1}||_\infty\\&\leq||I-(1+H)^{-1}||\\&\leq||H||/(1-||H||)\\&\leq Kn^{-1}/(1-Kn^{-1})\\&=K/(n-K)\end{aligned}$$

Together with the standard estimate $K\approx(2k/e)^k$, this gives the result. □

We have the following result:

Theorem 16.33. *We have the estimate*

$$I(a)=n^{-k}\left(\prod_{i=1}^{p}\prod_{j=1}^{q}a_{ij}!!+O(n^{-1})\right)$$

when all a_{ij} are even, and $I(a)=O(n^{-k-1})$ otherwise.

Proof. By using the above results, we obtain the following estimate:

$$\begin{aligned}&I(a)\\=&\sum_{\pi,\sigma}\delta_\pi(a_l)\delta_\sigma(a_r)W_{kn}(\pi,\sigma)\\=&n^{-k}\sum_{\pi,\sigma}\delta_\pi(a_l)\delta_\sigma(a_r)(\delta_{\pi\sigma}+O(n^{-1}))\\=&n^{-k}\left(\#\{\pi|\delta_\pi(a_l)=\delta_\pi(a_r)=1\}+O(n^{-1})\right)\end{aligned}$$

In order to count the partitions appearing in the set on the right, let us go back to the multi-indices a_l,a_r described above. It is convenient to view both these multi-indices in a rectangular way, as follows:

$$a_l=\begin{pmatrix}\underbrace{1\ldots1}_{a_{11}}&\cdots&\underbrace{1\ldots1}_{a_{1q}}\\\cdots&\cdots&\cdots\\\underbrace{p\ldots p}_{a_{p1}}&\cdots&\underbrace{p\ldots p}_{a_{pq}}\end{pmatrix}$$

$$a_r = \begin{pmatrix} \underbrace{1\ldots1}_{a_{11}} & \ldots & \underbrace{q\ldots q}_{a_{1q}} \\ \ldots & \ldots & \ldots \\ \underbrace{1\ldots1}_{a_{p1}} & \ldots & \underbrace{p\ldots p}_{a_{pq}} \end{pmatrix}$$

In other words, the multi-indices a_l/a_r are now simply obtained from the matrix a by "dropping" from each entry a_{ij} a sequence of a_{ij} numbers, all equal to i/j.

These two multi-indices, now in matrix form, have total length $2k = \Sigma a_{ij}$. We agree to view as well any pairing of $\{1, \ldots, 2k\}$ in matrix form, by following the same convention.

With this picture, the pairings π which contribute are simply those interconnecting sequences of indices "dropped" from the same a_{ij}, and this gives the following results:

(1) In the case where one of the entries a_{ij} is odd, there is no pairing that can contribute to the leading term under consideration, so we have $I(a) = O(n^{-k-1})$, and we are done.

(2) In the case where all the entries a_{ij} are even, the pairings that contribute to the leading term are those connecting points inside the pq "dropped" sets, i.e. are made out of a pairing of a_{11} points, a pairing of a_{12} points, and so on, up to a pairing of a_{pq} points. Now since an x-point set has $x!!$ pairings, this gives the formula in the statement. □

We have seen how to compute the asymptotic behavior of $I(a)$, by using basic estimates on the Weingarten matrix. However, our results so far are effective only in the "non-degenerate" case, when all the entries of a are even numbers. In the general case, the computation of the asymptotic sign of $I(a)$ requires a finer knowledge of the Weingarten matrix, notably with the exact computation of its leading term in n^{-1}.

In addition, the problem of computing the higher order terms, which are usually required for delicate applications of the Weingarten formula, appears as well.

We investigate these questions in this section and in the next one. We use a method of Collins [45], further processed by Collins-Śniady [50]. Let us begin with a key definition:

Definition 16.34. *The Brauer space D_k is defined as follows:*

(1) *The points are the Brauer diagrams, i.e. the pairings of $\{1, 2, \ldots, 2k\}$.*
(2) *The distance function is given by $d(\pi, \sigma) = k - loops(\pi, \sigma)$.*

It is indeed well-known, and elementary to check, that d satisfies the usual axioms for a distance function. This actually comes from some general categorical properties of the Brauer diagrams, which are valid in much more general situations. See [15], [60].

The Brauer space, which will play an important role in what follows, is by definition a metric space having $(2k)!! = 1.3.5 \ldots (2k-1)$ points. An interesting question is to find a "geometric" realization of this space. This will be discussed later on.

The series expansion of the Weingarten function in terms of paths on the Brauer space was originally found by Collins in [45] in the unitary case, then by Collins and Śniady [50] in the orthogonal case. We present below a slightly modified statement, along with a complete proof, by using a somewhat lighter formalism:

Theorem 16.35. *The Weingarten function W_{kn} has a series expansion in n^{-1} of the form*

$$W_{kn}(\pi,\sigma)=n^{-k-d(\pi,\sigma)}\sum_{g=0}^{\infty}K_g(\pi,\sigma)n^{-g}$$

where the objects on the right are defined as follows:

(1) *A path from π to σ is a sequence $p=[\pi=\tau_0\neq\tau_1\neq\ldots\neq\tau_r=\sigma]$.*
(2) *The signature of such a path is $+$ when r is even, and $-$ when r is odd.*
(3) *The geodesicity defect of such a path is $g(p)=\Sigma_{i=1}^{r}d(\tau_{i-1},\tau_i)-d(\pi,\sigma)$.*
(4) *K_g counts the signed paths from π to σ, with geodesicity defect g.*

Proof. Let us go back to the proof of our main estimate so far. We can write:

$$G_{kn}=n^{-k}(I+H)$$

In terms of the Brauer space distance, the formula of H is simply:

$$H(\pi,\sigma)=\begin{cases}0 & \text{for } \pi=\sigma\\ n^{-d(\pi,\sigma)} & \text{for } \pi\neq\sigma\end{cases}$$

Consider now the set $P_r(\pi,\sigma)$ of r-paths between π and σ. According to the usual rule of matrix multiplication, the powers of H are given by:

$$\begin{aligned}&H^r(\pi,\sigma)\\ =\;&\sum_{p\in P_r(\pi,\sigma)}H(\tau_0,\tau_1)\ldots H(\tau_{r-1},\tau_r)\\ =\;&\sum_{p\in P_r(\pi,\sigma)}n^{-d(\pi,\sigma)-g(p)}\end{aligned}$$

We can use now the formula:

$$(1+H)^{-1}=1-H+H^2-H^3+\ldots$$

By using this formula, we obtain:

$$\begin{aligned}&W_{kn}(\pi,\sigma)\\ =\;&n^{-k}\sum_{r=0}^{\infty}(-1)^rH^r(\pi,\sigma)\\ =\;&n^{-k-d(\pi,\sigma)}\sum_{r=0}^{\infty}\sum_{p\in P_r(\pi,\sigma)}(-1)^rn^{-g(p)}\end{aligned}$$

Now by rearranging the various terms of the double sum according to their geodesicity defect $g = g(p)$, this gives the formula in the statement. □

For the $I(a)$ translation of the above result, it is convenient to use the total length of a path, defined as:

$$d(p) = \sum_{i=1}^{r} d(\tau_{i-1}, \tau_i)$$

Observe that we have:

$$d(p) = d(\pi, \sigma) + g(p)$$

With these conventions, we have:

Theorem 16.36. *The integral $I(a)$ has a series expansion in n^{-1} of the form*

$$I(a) = n^{-k} \sum_{d=0}^{\infty} H_d(a) n^{-d}$$

where the coefficient on the right can be interpreted as follows:

(1) *Starting from $a \in M_{p\times q}(\mathbb{N})$, construct the multi-indices a_l, a_r as usual.*
(2) *Call a path "a-admissible" if its endpoints satisfy $\delta_\pi(a_l) = 1$ and $\delta_\sigma(a_r) = 1$.*
(3) *Then $H_d(a)$ counts all a-admissible signed paths in D_k, of total length d.*

Proof. We combine first the above results:

$$\begin{aligned} & I(a) \\ = & \sum_{\pi,\sigma} \delta_\pi(a_l)\delta_\sigma(a_r) W_{kn}(\pi, \sigma) \\ = & n^{-k} \sum_{\pi,\sigma} \delta_\pi(a_l)\delta_\sigma(a_r) \sum_{g=0}^{\infty} K_g(\pi, \sigma) n^{-d(\pi,\sigma)-g} \end{aligned}$$

Let us denote by $H_d(\pi, \sigma)$ the number of signed paths between π and σ, of total length d. In terms of the new variable $d = d(\pi, \sigma) + g$, the above expression becomes:

$$\begin{aligned} & I(a) \\ = & n^{-k} \sum_{\pi,\sigma} \delta_\pi(a_l)\delta_\sigma(a_r) \sum_{d=0}^{\infty} H_d(\pi, \sigma) n^{-d} \\ = & n^{-k} \sum_{d=0}^{\infty} \left(\sum_{\pi,\sigma} \delta_\pi(a_l)\delta_\sigma(a_r) H_d(\pi, \sigma) \right) n^{-d} \end{aligned}$$

We recognize in the middle the quantity $H_d(a)$, and this gives the result. □

We derive now some concrete consequences from the abstract results in the previous section. First, let us recall the following result, due to Collins and Śniady [50]:

Theorem 16.37. *We have the estimate*

$$W_{kn}(\pi,\sigma)=n^{-k-d(\pi,\sigma)}(\mu(\pi,\sigma)+O(n^{-1}))$$

where μ is the Möbius function.

Proof. We know from the above that we have the following estimate:

$$W_{kn}(\pi,\sigma)=n^{-k-d(\pi,\sigma)}(K_0(\pi,\sigma)+O(n^{-1}))$$

Now since one of the possible definitions of the Möbius function is that this counts the signed geodesic paths, we have $K_0=\mu$, and we are done. □

It is probably interesting to note here that in some more general settings, e.g. when O_n is replaced by its free version O_n^+, the straightforward extension of Theorem 5.1 doesn't seem to hold in full generality. In fact, the computation of the first order term of the generalized Weingarten functions is an open, interesting question. See [15], [60], [17].

Let us go back now to our integrals $I(a)$. The analogue of the above result of Collins and Śniady, fully generalizing Theorem 3.2, is as follows:

Theorem 16.38. *We have the estimate*

$$I(a)=n^{-k-e(a)}(\mu(a)+O(n^{-1}))$$

where the objects on the right are as follows:

(1) $e(a)=\min\{d(\pi,\sigma)|\pi,\sigma\in D_k,\delta_\pi(a_l)=\delta_\sigma(a_r)=1\}$.
(2) $\mu(a)$ *counts all a-admissible signed paths in D_k, of total length $e(a)$.*

Proof. We know from Theorem 4.3 that we have an estimate of the following type:

$$I(a)=n^{-k-e}(H_e(a)+O(n^{-1}))$$

Here, according to the various notations in the previous section, $e\in\mathbb{N}$ is the smallest total length of an a-admissible path, and $H_e(a)$ counts all signed a-admissible paths of total length e. Now since the smallest total length of such a path is of course attained when the path is just a segment, we have $e=e(a)$ and $H_e(a)=\mu(a)$, and we are done. □

Summarizing, we have now a full description of the asymptotic behavior of $I(a)$. To illustrate how Theorem 5.2 applies, let us recover the results in Theorem 3.2:

(1) Assume first that all entries of a are even. In this case there is at least one partition π such that $\delta_\pi(a_l)=\delta_\pi(a_r)=1$, so we have $e(a)=0$, and we recover the leading term n^{-k} from Theorem 3.2. As for the coefficient $\mu(a)$, this counts the partitions π such that $\delta_\pi(a_l)=\delta_\pi(a_r)=1$, so we fully recover Theorem 3.2.

(2) Assume now that a has at least one odd entry. Here there is no π as above, so we have $e(a)\geq 1$, and we recover the quantity $O(n^{-k-1})$ from Theorem 3.2.

Regarding now the higher order terms, the situation is quite complicated. In fact, Theorem 4.3 is quite difficult to use as stated, as it was the case in fact with Theorem 4.2 as well.

We have now a quite satisfactory picture of $\lim_{n\to\infty} I(a)$. However, the computation of $I(a)$ for fixed n remains a quite subtle problem, as shown for instance by Theorem 1.3.

As explained in the previous section, the exact formula coming from the geodesic expansion is quite difficult to handle, in the lack of a better understanding of the Brauer space D_k. However, there have been many attempts for working out the combinatorics of the geodesic expansion. Let us mention here the pioneering work of Collins in the unitary case [45], further processed by Collins and Śniady in the orthogonal case [50].

A remarkable advance on this subject came quite recently, in the preprint of Collins and Matsumoto [46]. In this section we briefly explain their new formula, and we work out the corresponding consequences regarding the integrals $I(a)$.

The formula of Collins and Matsumoto [46] is as follows:

Theorem 16.39. *We have the formula*

$$W_{kn}(\pi,\sigma)=\frac{\sum_{\lambda\vdash k,\, l(\lambda)\leq k}\chi^{2\lambda}(1_k)w^{\lambda}(\pi^{-1}\sigma)}{(2k)!!\prod_{(i,j)\in\lambda}(n+2j-i-1)}$$

where the various objects on the right are as follows:

(1) *The sum is over all partitions of* $\{1,\ldots,2k\}$ *of length* $l(\lambda)\leq k$.
(2) w^{λ} *is the corresponding zonal spherical function of* (S_{2k},H_k).
(3) $\chi^{2\lambda}$ *is the character of* S_{2k} *associated to* $2\lambda=(2\lambda_1,2\lambda_2,\ldots)$.
(4) *The product is over all squares of the Young diagram of* λ.

It is of course possible to deduce from this a new a formula for $I(a)$, just by putting together the formulae in Theorem 2.2 and Theorem 6.1. However, there are probably several non-trivial simplifications that might appear when doing the sum over π,σ, and we do not know how the final statement about $I(a)$ should look like.

Instead, let us just record the following consequence:

Proposition 16.40. *The possible poles of* $I(a)$ *can be at the numbers*

$$-(k-1),-(k-2),\ldots,2k-1,2k$$

where $k\in\mathbb{N}$ *associated to the admissible matrix* $a\in M_{p\times q}(\mathbb{N})$ *is given by* $k=\Sigma a_{ij}/2$.

Proof. We know from Theorem 2.2 that the possible poles of $I(a)$ can only come from those of the Weingarten function. On the other hand, Theorem 6.1 tells us that these latter poles are located at the numbers of the form $-2j+i+1$, with (i,j) ranging over all possible squares of all possible Young diagrams, and this gives the result. □

There are many other applications of the Weingarten formula, and of easiness in general, concerning the compact groups themselves, thier structure and combinatorics, or their actions on various structures, such as sequences or arrays of random variables. There are as well many applications to the random matrices, where standard manipulations can lead into integration questions over various classical compact groups.

References

[1] S. Agaian, Hadamard matrices and their applications, Springer (1985).
[2] G.W. Anderson, A. Guionnet and O. Zeitouni, An introduction to random matrices, Cambridge Univ. Press (2010).
[3] O. Arizmendi, I. Nechita and C. Vargas, On the asymptotic distribution of block-modified random matrices, *J. Math. Phys.* **57** (2016), 1–27.
[4] M.F. Atiyah, The geometry and physics of knots, Cambridge (1990).
[5] M.F. Atiyah and I.G. MacDonald, Introduction to commutative algebra, Addison-Wesley (1969).
[6] G. Aubrun, Partial transposition of random states and non-centered semicircular distributions, *Random Matrices Theory Appl.* **1** (2012), 125–145.
[7] J. Avan, T. Fonseca, L. Frappat, P. Kulish, E. Ragoucy and G. Rollet, Temperley-Lieb R-matrices from generalized Hadamard matrices, *Theor. Math. Phys.* **178** (2014), 223–240.
[8] J. Backelin, Square multiples n give infinitely many cyclic n-roots, preprint 1989.
[9] T. Banica, The free unitary compact quantum group, *Comm. Math. Phys.* **190** (1997), 143–172.
[10] T. Banica, The defect of generalized Fourier matrices, *Linear Algebra Appl.* **438** (2013), 3667–3688.
[11] T. Banica, The glow of Fourier matrices: universality and fluctuations, *Oper. Matrices* **9** (2015), 457–474.
[12] T. Banica, Block-modified Wishart matrices: the easy case, *Indiana Univ. Math. J.* **69** (2020), 1–34.
[13] T. Banica, S.T. Belinschi, M. Capitaine and B. Collins, Free Bessel laws, *Canad. J. Math.* **63** (2011), 3–37.
[14] T. Banica, J. Bichon and B. Collins, The hyperoctahedral quantum group, *J. Ramanujan Math. Soc.* **22** (2007), 345–384.
[15] T. Banica and B. Collins, Integration over compact quantum groups, *Publ. Res. Inst. Math. Sci.* **43** (2007), 277–302.
[16] T. Banica, B. Collins and J.M. Schlenker, On orthogonal matrices maximizing the 1-norm, *Indiana Univ. Math. J.* **59** (2010), 839–856.
[17] T. Banica and S. Curran, Decomposition results for Gram matrix determinants, *J. Math. Phys.* **51** (2010), 1–14.
[18] T. Banica, S. Curran and R. Speicher, Classification results for easy quantum groups, *Pacific J. Math.* **247** (2010), 1–26.
[19] T. Banica, S. Curran and R. Speicher, Stochastic aspects of easy quantum groups, *Probab. Theory Related Fields* **149** (2011), 435–462.
[20] T. Banica, S. Curran and R. Speicher, De Finetti theorems for easy quantum groups, *Ann. Probab.* **40** (2012), 401–435.
[21] T. Banica and I. Nechita, Asymptotic eigenvalue distributions of block-transposed Wishart matrices, *J. Theoret. Probab.* **26** (2013), 855–869.
[22] T. Banica and I. Nechita, Block-modified Wishart matrices and free Poisson laws, *Houston J. Math.* **41** (2015), 113–134.
[23] T. Banica and I. Nechita, Almost Hadamard matrices with complex entries, *Adv. Oper. Theory* **3** (2018), 149–189.
[24] T. Banica, I. Nechita and K. Życzkowski, Almost Hadamard matrices: general theory and examples, *Open Syst. Inf. Dyn.* **19** (2012), 1–26.
[25] T. Banica and R. Speicher, Liberation of orthogonal Lie groups, *Adv. Math.* **222** (2009), 1461–1501.
[26] L.D. Baumert, S.W. Golomb and M. Hall, Discovery of an Hadamard matrix of order 92, *Bull. Amer. Math. Soc.* **68** (1962), 237–238.
[27] R.J. Baxter, Exactly solved models in statistical mechanics, Academic Press (1982).

[28] K. Beauchamp and R. Nicoara, Orthogonal maximal abelian $*$-subalgebras of the 6×6 matrices, *Linear Algebra Appl.* **428** (2008), 1833–1853.
[29] I. Bengtsson, W. Bruzda, Å. Ericsson, J.-Å. Larsson, W. Tadej and K. Życzkowski, Mutually unbiased bases and Hadamard matrices of order six, *J. Math. Phys.* **48** (2007), 1–33.
[30] H. Bercovici and V. Pata, Stable laws and domains of attraction in free probability theory, *Ann. of Math.* **149** (1999), 1023–1060.
[31] J. Bhowmick, F. D'Andrea and L. Dabrowski, Quantum isometries of the finite noncommutative geometry of the standard model, *Comm. Math. Phys.* **307** (2011), 101–131.
[32] P. Biane, Some properties of crossings and partitions, *Discrete Math.* **175** (1997), 41–53.
[33] P. Biran, M. Entov and L. Polterovich, Calabi quasimorphisms for the symplectic ball, *Commun. Contemp. Math.* **6** (2004), 793–802.
[34] D. Bisch and V.F.R. Jones, Algebras associated to intermediate subfactors, *Invent. Math.* **128** (1997), 89–157.
[35] G. Björck, Functions of modulus 1 on Z_n whose Fourier transforms have constant modulus, and cyclic n-roots, *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.* **315** (1990), 131–140.
[36] N. Bourbaki, Eléments de mathématique, Hermann (1970).
[37] M. Brannan and B. Collins, Dual bases in Temperley-Lieb algebras, quantum groups, and a question of Jones, *Quantum Topology* **9** (2018), 715–748.
[38] M. Brannan, B. Collins, H.H. Lee and S. Youn, Temperley-Lieb quantum channels, *Comm. Math. Phys.* **376** (2020), 795–839.
[39] R. Brauer, On algebras which are connected with the semisimple continuous groups, *Ann. of Math.* **38** (1937), 857–872.
[40] A.T. Butson, Generalized Hadamard matrices, *Proc. Amer. Math. Soc.* **13** (1962), 894–898.
[41] A.H. Chamseddine and A. Connes, The spectral action principle, *Comm. Math. Phys.* **186** (1997), 731–750.
[42] A.H. Chamseddine and A. Connes, Why the standard model, *J. Geom. Phys.* **58** (2008), 38–47.
[43] Q. Chen and J. Przytycki, The Gram matrix of a Temperley-Lieb algebra is similar to the matrix of chromatic joins, *Commun. Contemp. Math.* **10** (2008), 849–855.
[44] C.-H. Cho, Holomorphic discs, spin structures, and Floer cohomology of the Clifford torus, *Int. Math. Res. Not.* **35** (2004), 1803–1843.
[45] B. Collins, Moments and cumulants of polynomial random variables on unitary groups, the Itzykson-Zuber integral, and free probability, *Int. Math. Res. Not.* **17** (2003), 953–982.
[46] B. Collins and S. Matsumoto, On some properties of orthogonal Weingarten functions, *J. Math. Phys.* **50** (2009), 1–18.
[47] B. Collins and I. Nechita, Random quantum channels I: graphical calculus and the Bell state phenomenon, *Comm. Math. Phys.* **297** (2010), 345–370.
[48] B. Collins and I. Nechita, Random quantum channels II: entanglement of random subspaces, Rényi entropy estimates and additivity problems, *Adv. Math.* **226** (2011), 1181–1201.
[49] B. Collins and I. Nechita, Gaussianization and eigenvalue statistics for random quantum channels (III), *Ann. Appl. Probab.* **21** (2011), 1136–1179.
[50] B. Collins and P. Śniady, Integration with respect to the Haar measure on unitary, orthogonal and symplectic groups, *Comm. Math. Phys.* **264** (2006), 773–795.
[51] A. Copeland, F. Schmidt and R. Simion, Note on two determinants with interesting factorizations, *Discrete Math.* **256** (2002), 449–458.
[52] A. Connes, Une classification des facteurs de type III, *Ann. Sci. Ec. Norm. Sup.* **6** (1973), 133–252.
[53] A. Connes, Classification of injective factors. Cases II_1, II_∞, III_λ, $\lambda \neq 1$, *Ann. of Math.* **104** (1976), 73–115.

[54] A. Connes, Noncommutative geometry, Academic Press (1994).
[55] A. Connes, A unitary invariant in Riemannian geometry, *Int. J. Geom. Methods Mod. Phys.* **5** (2008), 1215–1242.
[56] A. Connes, On the spectral characterization of manifolds, *J. Noncommut. Geom.* **7** (2013), 1–82.
[57] A. Connes and D. Kreimer, Hopf algebras, renormalization and noncommutative geometry, in "Quantum field theory: perspective and prospective", Springer (1999), 59–109.
[58] A. Connes and J. Lott, Particle models and noncommutative geometry, *Nucl. Phys. B* **18** (1991), 29–47.
[59] R. Craigen and H. Kharaghani, On the nonexistence of Hermitian circulant complex Hadamard matrices, *Australas. J. Combin.* **7** (1993), 225–227.
[60] S. Curran, Quantum exchangeable sequences of algebras, *Indiana Univ. Math. J.* **58** (2009), 1097–1126.
[61] S. Curran, Quantum rotatability, *Trans. Amer. Math. Soc.* **362** (2010), 4831–4851.
[62] S. Curran, A characterization of freeness by invariance under quantum spreading, *J. Reine Angew. Math.* **659** (2011), 43–65.
[63] S. Curran and R. Speicher, Quantum invariant families of matrices in free probability, *J. Funct. Anal.* **261** (2011), 897–933.
[64] W. de Launey, On the non-existence of generalized weighing matrices, *Ars Combin.* **17** (1984), 117–132.
[65] W. de Launey and J.E. Dawson, An asymptotic result on the existence of generalised Hadamard matrices, *J. Combin. Theory Ser. A* **65** (1994), 158–163.
[66] W. de Launey, D.L. Flannery and K.J. Horadam, Cocyclic Hadamard matrices and difference sets, *Discrete Appl. Math.* **102** (2000), 47–61.
[67] W. de Launey and D.A. Levin, A Fourier-analytic approach to counting partial Hadamard matrices, *Cryptogr. Commun.* **2** (2010), 307–334.
[68] P. Deligne, Catégories tannakiennes, in "Grothendieck Festchrift", Birkhauser (1990), 111–195.
[69] P. Di Francesco, Meander determinants, *Comm. Math. Phys.* **191** (1998), 543–583.
[70] P. Di Francesco, Folding and coloring problems in mathematics and physics, *Bull. Amer. Math. Soc.* **37** (2000), 251–307.
[71] P. Di Francesco, O. Golinelli and E. Guitter, Meanders and the Temperley-Lieb algebra, *Comm. Math. Phys.* **186** (1997), 1–59.
[72] P. Di Francesco, O. Golinelli and E. Guitter, Meanders: exact asymptotics, *Nucl. Phys. B* **570** (2000) 699–712.
[73] P. Diaconis and D. Freedman, A dozen de Finetti-style results in search of a theory, *Ann. Inst. Henri Poincaré Probab. Stat.* **23** (1987), 397–423.
[74] P. Diaconis and M. Shahshahani, On the eigenvalues of random matrices, *J. Applied Probab.* **31** (1994), 49–62.
[75] J. Dieudonné and A. Grothendieck, Eléments de géométrie algébrique, I-IV, IHES (1967).
[76] P. Diţă, Some results on the parametrization of complex Hadamard matrices, *J. Phys. A* **37** (2004), 5355–5374.
[77] J. Dixmier, C*-algebras, North-Holland (1977).
[78] J. Dixmier, Von Neumann algebras, Elsevier (1981).
[79] S. Doplicher and J. Roberts, A new duality theory for compact groups, *Invent. Math.* **98** (1989), 157–218.
[80] V.G. Drinfeld, Quantum groups, Proc. ICM Berkeley (1986), 798–820.
[81] L. Faddeev, Instructive history of the quantum inverse scattering method, *Acta Appl. Math.* **39** (1995), 69–84.

[82] L. Faddeev, N. Reshetikhin and L. Takhtadzhyan, Quantization of Lie groups and Lie algebras, *Leningrad Math. J.* **1** (1990), 193–225.
[83] J.-C. Faugère, Finding all the solutions of Cyclic 9 using Gröbner basis techniques, *Lecture Notes Ser. Comput.* **9** (2001), 1–12.
[84] P.C. Fishburn and N.J.A. Sloane, The solution to Berlekamp's switching game, *Discrete Math.* **74** (1989), 263–290.
[85] M. Fukuda and P. Śniady, Partial transpose of random quantum states: exact formulas and meanders, *J. Math. Phys.* **54** (2013), 1–31.
[86] I.M. Gelfand, Normierte Ringe, *Mat. Sb.* **9** (1941), 3–24.
[87] I.M. Gelfand and M.A. Naimark, On the imbedding of normed rings into the ring of operators on a Hilbert space, *Mat. Sb.* **12** (1943), 197–217.
[88] D. Goswami, Quantum group of isometries in classical and noncommutative geometry, *Comm. Math. Phys.* **285** (2009), 141–160.
[89] P. Graczyk, G. Letac and H. Massam, The complex Wishart distribution and the symmetric group, *Ann. Statist.* **31** (2003), 287–309.
[90] A. Guionnet, V.F.R. Jones and D. Shlyakhtenko, Random matrices, free probability, planar algebras and subfactors, *Quanta of maths* **11** (2010), 201–239.
[91] U. Haagerup, Orthogonal maximal abelian $*$-subalgebras of the $n \times n$ matrices and cyclic n-roots, in "Operator algebras and quantum field theory", International Press (1997), 296–323.
[92] U. Haagerup, Cyclic p-roots of prime lengths p and related complex Hadamard matrices, preprint 2008.
[93] J. Hadamard, Résolution d'une question relative aux déterminants, *Bull. Sci. Math.* **2** (1893), 240–246.
[94] M. Hall, Integral matrices A for which $AA^T = mI$, in "Number Theory and Algebra", Academic Press (1977), 119–134.
[95] R. Hartshorne, Algebraic geometry, Springer (1977).
[96] F. Hiai and D. Petz, The semicircle law, free random variables and entropy, AMS (2000).
[97] K.J. Horadam, Hadamard matrices and their applications, Princeton Univ. Press (2007).
[98] L. Hörmander, The analysis of linear partial differential operators, I-IV, Springer (1964).
[99] M. Idel and M.M. Wolf, Sinkhorn normal form for unitary matrices, *Linear Algebra Appl.* **471** (2015), 76–84.
[100] N. Ito, Hadamard Graphs I, *Graphs Combin.* **1** (1985), 57–64.
[101] D. Jackson, The lattice of noncrossing partitions and the Birkhoff-Lewis equations, *European J. Combin.* **15** (1994), 245–250.
[102] M. Jimbo, A q-difference analog of $U(\mathfrak{g})$ and the Yang-Baxter equation, *Lett. Math. Phys.* **10** (1985), 63–69.
[103] V.F.R. Jones, Index for subfactors, *Invent. Math.* **72** (1983), 1–25.
[104] V.F.R. Jones, On knot invariants related to some statistical mechanical models, *Pacific J. Math.* **137** (1989), 311–334.
[105] V.F.R. Jones, Subfactors and knots, CBMS Lecture Notes (1991).
[106] V.F.R. Jones, The Potts model and the symmetric group, in "Subfactors, Kyuzeso 1993" (1994), 259–267.
[107] V.F.R. Jones, Planar algebras I, preprint 1999.
[108] V.F.R. Jones, The planar algebra of a bipartite graph, in "Knots in Hellas '98" (2000), 94–117.
[109] V.F.R. Jones, The annular structure of subfactors, *Monogr. Enseign. Math.* **38** (2001), 401–463.
[110] V.F.R. Jones, S. Morrison and N. Snyder, The classification of subfactors of index at most 5, *Bull. Amer. Math. Soc.* **51** (2014), 277–327.

[111] V.F.R. Jones, D. Shlyakhtenko and K. Walker, An orthogonal approach to the subfactor of a planar algebra, *Pacific J. Math.* **246** (2010), 187–197.
[112] V.F.R. Jones and V.S. Sunder, Introduction to subfactors, Cambridge Univ. Press (1997).
[113] O. Kallenberg, Probabilistic symmetries and invariance principles, Springer (2005).
[114] A. Karabegov, The reconstruction of a unitary matrix from the moduli of its elements and symbols on a finite phase space, preprint 1989.
[115] H. Kesten, Symmetric random walks on groups, *Trans. Amer. Math. Soc.* **92** (1959), 336–354.
[116] H. Kharaghani and J. Seberry, The excess of complex Hadamard matrices, *Graphs Combin.* **9** (1993), 47–56.
[117] H. Kharaghani and B. Tayfeh-Rezaie, A Hadamard matrix of order 428, *J. Combin. Des.* **13** (2005), 435–440.
[118] F. Klein, Vergleichende Betrachtungen über neuere geometrische Forschungen, *Math. Ann.* **43** (1893), 63–100.
[119] V. Kodiyalam and V.S. Sunder, Temperley-Lieb and non-crossing partition planar algebras, *Contemp. Math.* **456** (2008), 61–72.
[120] C. Köstler, R. Speicher, A noncommutative de Finetti theorem: invariance under quantum permutations is equivalent to freeness with amalgamation, *Comm. Math. Phys.* **291** (2009), 473–490.
[121] C. Koukouvinos, M. Mitrouli and J. Seberry, An algorithm to find formulae and values of minors for Hadamard matrices, *Linear Algebra Appl.* **330** (2001), 129–147.
[122] M.G. Krein, A principle of duality for a bicompact group and a square block algebra, *Dokl. Akad. Nauk. SSSR* **69** (1949), 725–728.
[123] T.Y. Lam and K.H. Leung, On vanishing sums of roots of unity, *J. Algebra* **224** (2000), 91–109.
[124] S. Lang, Algebra, Addison-Wesley (1993).
[125] B. Lindstöm, Determinants on semilattices, *Proc. Amer. Math. Soc.* **20** (1969), 207–208.
[126] W. Liu, General de Finetti type theorems in noncommutative probability, *Comm. Math. Phys.* **369** (2019), 837–866.
[127] M. Lupini, L. Mančinska and D.E. Roberson, Nonlocal games and quantum permutation groups, *J. Funct. Anal.* **279** (2020), 1–39.
[128] S. Malacarne, Woronowicz's Tannaka-Krein duality and free orthogonal quantum groups, *Math. Scand.* **122** (2018), 151–160.
[129] A. Mang and M. Weber, Categories of two-colored pair partitions, part I: Categories indexed by cyclic groups, preprint 2019.
[130] A. Mang and M. Weber, Categories of two-colored pair partitions, part II: Categories indexed by semigroups, preprint 2019.
[131] V.A. Marchenko and L.A. Pastur, Distribution of eigenvalues in certain sets of random matrices, *Mat. Sb.* **72** (1967), 507–536.
[132] P. Martin, Potts models and related problems in statistical mechanics, World Scientific (1991).
[133] M. Matolcsi, J. Réffy and F. Szöllősi, Constructions of complex Hadamard matrices via tiling abelian groups, *Open Syst. Inf. Dyn.* **14** (2007), 247–263.
[134] D. McNulty and S. Weigert, Isolated Hadamard matrices from mutually unbiased product bases, *J. Math. Phys.* **53** (2012), 1–21.
[135] M.L. Mehta, Random matrices, Elsevier (2004).
[136] J.A. Mingo and M. Popa, Freeness and the transposes of unitarily invariant random matrices, *J. Funct. Anal.* **271** (2016), 883–921.
[137] J.A. Mingo and M. Popa, Freeness and the partial transposes of Wishart random matrices, *Canad. J. Math.* **71** (2019), 659–681.
[138] J.A. Mingo and R. Speicher, Free probability and random matrices, Springer (2017).

[139] M.T. Mohan, On some p-almost Hadamard matrices, *Oper. Matrices* **13** (2019), 253–281.
[140] F.J. Murray and J. von Neumann, On rings of operators. IV, *Ann. of Math.* **44** (1943), 716–808.
[141] B. Musto, D.J. Reutter and D. Verdon, A compositional approach to quantum functions, *J. Math. Phys.* **59** (2018), 1–57.
[142] J. Nash, The imbedding problem for Riemannian manifolds, *Ann. of Math.* **63** (1956), 20–63.
[143] A. Nica and R. Speicher, Lectures on the combinatorics of free probability, Cambridge University Press (2006).
[144] R. Nicoara, A finiteness result for commuting squares of matrix algebras, *J. Operator Theory* **55** (2006), 295–310.
[145] R. Nicoara and J. White, Analytic deformations of group commuting squares and complex Hadamard matrices, *J. Funct. Anal.* **272** (2017), 3486–3505.
[146] R. Paley, On orthogonal matrices, *J. Math. Phys.* **12** (1933), 311–320.
[147] K.H. Park and H.Y. Song, Quasi-Hadamard matrices, *Proc. ISIT 2010*, Austin, TX (2010).
[148] M. Petrescu, Existence of continuous families of complex Hadamard matrices of certain prime dimensions and related results, Ph.D. Thesis, UCLA (1997).
[149] G. Pólya, Über eine Aufgabe der Wahrscheinlichkeitsrechnung betreffend die Irrfahrt im Strassennetz, *Math. Ann.* **84** (1921), 149–160.
[150] S. Popa, Orthogonal pairs of $*$-subalgebras in finite von Neumann algebras, *J. Operator Theory* **9** (1983), 253–268.
[151] S. Popa, Classification of amenable subfactors of type II, *Acta Math.* **172** (1994), 163–255.
[152] S. Popa and D. Shlyakhtenko, Universal properties of $L(F_\infty)$ in subfactor theory, *Acta Math.* **191** (2004), 225–257.
[153] S. Raum and M. Weber, The full classification of orthogonal easy quantum groups, *Comm. Math. Phys.* **341** (2016), 751–779.
[154] L.B. Richmond and J. Shallit, Counting abelian squares, *Electron. J. Combin.* **16** (2009), 1–9.
[155] R. Roth and K. Viswanathan, On the hardness of decoding the Gale-Berlekamp code, *IEEE Trans. Inform. Theory* **54** (2008), 1050–1060.
[156] W. Rudin, Principles of mathematical analysis, McGraw-Hill (1964).
[157] W. Rudin, Real and complex analysis, McGraw-Hill (1966).
[158] W. Rudin, Functional analysis, McGraw-Hill (1973).
[159] H.J. Ryser, Combinatorial mathematics, Wiley (1963).
[160] J. Seberry and M. Yamada, Hadamard matrices, sequences, and block designs, Wiley (1992).
[161] J.P. Serre, Linear representations of finite groups, Springer (1977).
[162] G.C. Shephard and J.A. Todd, Finite unitary reflection groups, *Canad. J. Math.* **6** (1954), 274–304.
[163] I.R. Shafarevich, Basic algebraic geometry, Springer (1974).
[164] R. Speicher, Multiplicative functions on the lattice of noncrossing partitions and free convolution, *Math. Ann.* **298** (1994), 611–628.
[165] R. Speicher, Combinatorial theory of the free product with amalgamation and operator-valued free probability theory, *Mem. Amer. Math. Soc.* **132** (1998).
[166] J.J. Sylvester, Thoughts on inverse orthogonal matrices, simultaneous sign-successions, and tesselated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers, *Phil. Mag.* **34** (1867), 461–475.
[167] F. Szöllősi, Parametrizing complex Hadamard matrices, *European J. Combin.* **29** (2008), 1219–1234.
[168] F. Szöllősi, Exotic complex Hadamard matrices and their equivalence, *Cryptogr. Commun.* **2** (2010), 187–198.
[169] W. Tadej and K. Życzkowski, A concise guide to complex Hadamard matrices, *Open Syst. Inf. Dyn.* **13** (2006), 133–177.

[170] W. Tadej and K. Życzkowski, Defect of a unitary matrix, *Linear Algebra Appl.* **429** (2008), 447–481.
[171] T. Tannaka, Über den Dualitätssatz der nichtkommutativen topologischen Gruppen, *Tôhoku Math. J.* **45** (1939), 1–12.
[172] T. Tao, Fuglede's conjecture is false in 5 and higher dimensions, *Math. Res. Lett.* **11** (2004), 251–258.
[173] T. Tao and V. Vu, On random ±1 matrices: singularity and determinant, *Random Structures Algorithms* **28** (2006), 1–23.
[174] P. Tarrago and J. Wahl, Free wreath product quantum groups and standard invariants of subfactors, *Adv. Math.* **331** (2018), 1–57.
[175] P. Tarrago and M. Weber, Unitary easy quantum groups: the free case and the group case, *Int. Math. Res. Not.* **18** (2017), 5710–5750.
[176] N.H. Temperley and E.H. Lieb, Relations between the "percolation" and "colouring" problem and other graph-theoretical problems associated with regular planar lattices: some exact results for the "percolation" problem, *Proc. Roy. Soc. London* **322** (1971), 251–280.
[177] R.J. Turyn, Character sums and difference sets, *Pacific J. Math.* **15** (1965), 319–346.
[178] W.T. Tutte, The matrix of chromatic joins, *J. Combin. Theory Ser. B* **57** (1993), 269–288.
[179] E. Verheiden, Integral and rational completions of combinatorial matrices, *J. Combin. Theory Ser. A* **25** (1978) 267–276.
[180] D.V. Voiculescu, Symmetries of some reduced free product C*-algebras, in "Operator algebras and their connections with topology and ergodic theory", Springer (1985), 556–588.
[181] D. Voiculescu, Addition of certain noncommuting random variables, *J. Funct. Anal.* **66** (1986), 323–346.
[182] D.V. Voiculescu, Multiplication of certain noncommuting random variables, *J. Operator Theory* **18** (1987), 223–235.
[183] D. Voiculescu, Limit laws for random matrices and free products, *Invent. Math.* **104** (1991), 201–220.
[184] D.V. Voiculescu, K.J. Dykema and A. Nica, Free random variables, AMS (1992).
[185] J. von Neumann, On rings of operators. Reduction theory, *Ann. of Math.* **50** (1949), 401–485.
[186] S. Wang, Free products of compact quantum groups, *Comm. Math. Phys.* **167** (1995), 671–692.
[187] S. Wang, Quantum symmetry groups of finite spaces, *Comm. Math. Phys.* **195** (1998), 195–211.
[188] A. Wassermann, Coactions and Yang-Baxter equations for ergodic actions and subfactors, *London Math. Soc. Lect. Notes* **136** (1988), 203–236.
[189] D. Weingarten, Asymptotic behavior of group integrals in the limit of infinite rank, *J. Math. Phys.* **19** (1978), 999–1001.
[190] H. Wenzl, C* tensor categories from quantum groups, *J. Amer. Math. Soc.* **11** (1998), 261–282.
[191] H. Weyl, The classical groups: their invariants and representations, Princeton (1939).
[192] E. Wigner, Characteristic vectors of bordered matrices with infinite dimensions, *Ann. of Math.* **62** (1955), 548–564.
[193] J. Williamson, Hadamard's determinant theorem and the sum of four squares, *Duke Math. J.* **11** (1944), 65–81.
[194] A. Winterhof, On the non-existence of generalized Hadamard matrices, *J. Statist. Plann. Inference* **84** (2000), 337–342.
[195] E. Witten, Quantum field theory and the Jones polynomial, *Comm. Math. Phys.* **121** (1989), 351–399.
[196] S.L. Woronowicz, Twisted SU(2) group. An example of a non-commutative differential calculus, *Publ. Res. Inst. Math. Sci.* **23** (1987), 117–181.
[197] S.L. Woronowicz, Compact matrix pseudogroups, *Comm. Math. Phys.* **111** (1987), 613–665.

[198] S.L. Woronowicz, Tannaka-Krein duality for compact matrix pseudogroups. Twisted SU(N) groups, *Invent. Math.* **93** (1988), 35–76.
[199] S.L. Woronowicz, Compact quantum groups, in "Symétries quantiques" (Les Houches, 1995), North-Holland, Amsterdam (1998), 845–884.
[200] P. Zinn-Justin, Jucys-Murphy elements and Weingarten matrices, *Lett. Math. Phys.* **91** (2010), 119–127.

T.B.: Department of Mathematics, University of Cergy-Pontoise, F-95000 Cergy-Pontoise, France. teo.banica@gmail.com