Invitation to finite groups

Teo Banica

Department of Mathematics, University of Cergy-Pontoise, F-95000 Cergy-Pontoise, France. teo.banica@gmail.com

2010 *Mathematics Subject Classification.* 20B05

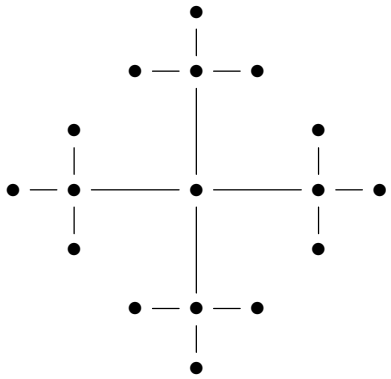
Key words and phrases. Finite group, Reflection group

Abstract. This is an introduction to the finite groups, with focus on the groups of permutations or reflections, and more generally, on the finite groups of unitary matrices. We first discuss the basics of group theory, both results and examples, notably with a study of the reflection groups, the Sylow theorems, and the structure result for the finite abelian groups. Then we go into the study of representation theory, and of other more advanced aspects, notably with results about the subgroups of SU_2, SO_3. We then discuss, using representation theory, a number of advanced analytic aspects, for the most in relation with questions coming from probability. Finally, we provide a brief introduction to the various possible generalizations of the finite groups.

Preface

There is a lot of symmetry in the real world, surrounding us. Minerals, plants, animals, we all have interesting symmetry features, witnessing for some built-in symmetry, in the various laws of mathematics, physics, chemistry and biology, having produced us.

Mathematically speaking, understanding this symmetry is a key problem. Have a look for instance at the snowflake pictured below, isn't this beautiful, by all possible beauty standards in this world, and wouldn't you like to know more about its symmetry:



Actually, understanding why snowflakes are made like this is a quite difficult question, requiring you to know well all basic mathematics, all basic physics, including quantum mechanics, and then a bit of quantum chemistry, and some advanced thermodynamics too. So, perhaps not the easiest example to start with. Maybe, for later.

More modestly, what we can do, as mathematicians, is to have at least a good understanding of abstract, mathematical symmetry. And here, things are quite straightforward. Symmetries are encoded by mathematical objects called groups, and the simplest such groups are those which are finite. So, as a reasonable objective, let us try to understand the finite groups. And for the laws of nature, and snowflakes, these can come later.

This book is an introduction to the finite groups, with focus on the groups of permutations or reflections, and more generally, on the finite groups of unitary matrices. The text is organized quite symmetrically, in 4 parts, each having 4 chapters, each having 4 sections, plus an informal exercise section at the end, as follows:

Part I discusses the basics of group theory, notably with a study of the reflection groups, the Sylow theorems, and the structure result for the finite abelian groups.

Part II goes into representation theory, and other advanced aspects, notably with results about diagrams and easiness, and about the subgroups of SU_2, SO_3.

Part III discusses, using representation theory techniques, a number of advanced analytic aspects, for the most in relation with questions coming from probability.

Part IV provides a brief introduction to the various generalizations of the finite groups, such as the compact groups, the discrete groups, and the finite quantum groups.

And this is pretty much all that I have to say, in this preface, and in the hope that you will like the table of contents, and why not, enjoy reading the whole book too.

Let me also mention that, contrary to what most technical book authors say about their books, as being concieved and written and fine-tuned over an extremely long period of time, this book was written quite quickly. Simply because I just love this stuff.

And thanks here to my cats, for teaching me this, once you are really interested in something, just go for it, with maximum speed, and no questions asked.

Cergy, May 2025
Teo Banica

Contents

Part I

Finite groups

And I miss you
Like the deserts miss the rain
And I miss you
Like the deserts miss the rain

CHAPTER 1

Group theory

1a. Group theory

Symmetries are encoded by groups, and with the groups being something very simple, namely some sets, with a composition operation, which must satisfy what we should expect from a "multiplication". The precise definition of the groups is as follows:

DEFINITION 1.1. *A group is a set G endowed with a multiplication operation*

$$(g,h)\to gh$$

which must satisfy the following conditions:

(1) *Associativity: we have, $(gh)k=g(hk)$, for any $g,h,k\in G$.*
(2) *Unit: there is an element $1\in G$ such that $g1=1g=g$, for any $g\in G$.*
(3) *Inverses: for any $g\in G$ there is $g^{-1}\in G$ such that $gg^{-1}=g^{-1}g=1$.*

The multiplication law is not necessarily commutative. In the case where it is, in the sense that $gh=hg$, for any $g,h\in G$, we call G abelian, en hommage to Abel, and we usually denote its multiplication, unit and inverse operation as follows:

$$(g,h)\to g+h\quad,\quad 0\in G\quad,\quad g\to -g$$

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 groups, with typically the basic systems of numbers that we know being abelian groups, and the basic sets of matrices being non-abelian groups. But again, this is of course not a general rule. Here are some basic illustrations:

PROPOSITION 1.2. *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 the definition of the groups, as follows:

(1) The group axioms are indeed satisfied for $\mathbb{Z}$, with the sum $g+h$ being the usual sum, 0 being the usual 0, and $-g$ being the usual $-g$.

(2) Once again, the axioms are satisfied for $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, with the remark that for $\mathbb{Q}$ we are using here the fact that the sum of two rational numbers is rational, coming from:

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$$

(3) In $\mathbb{N}$ we do not have inverses, so we do not have a group:

$$-1 \notin \mathbb{N}$$

(4) The group axioms are indeed satisfied for $\mathbb{Q}^*$, with the product gh being the usual product, 1 being the usual 1, and g^{-1} being the usual g^{-1}. Observe that we must remove indeed the element $0 \in \mathbb{Q}$, because in a group, any element must be invertible.

(5) Once again, the axioms are satisfied for $\mathbb{R}^*, \mathbb{C}^*$, with the remark that for $\mathbb{C}$ we are using here the fact that the nonzero complex numbers can be inverted, coming from:

$$z\bar{z}=|z|^2$$

(6) Here in $\mathbb{N}^*, \mathbb{Z}^*$ we do not have inverses, so we do not have groups, as claimed. □

There are many interesting groups coming from linear algebra, as follows:

THEOREM 1.3. *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 for $\mathbb{R}^N, \mathbb{C}^N$, with the sum being the usual sum of vectors, $-v$ being the usual $-v$, and the null vector 0 being the unit.

(2) Once again, the axioms are clearly satisfied for $M_N(\mathbb{R}), M_N(\mathbb{C})$, with the sum being the usual sum of matrices, $-M$ being the usual $-M$, and the null matrix 0 being the unit. Observe that what we have here is in fact a particular case of (1), because any $N \times N$ matrix can be regarded as a $N^2 \times 1$ vector, and so at the group level we have:

$$(M_N(\mathbb{R}), +) \simeq (\mathbb{R}^{N^2}, +) \quad , \quad (M_N(\mathbb{C}), +) \simeq (\mathbb{C}^{N^2}, +)$$

(3) Regarding now $GL_N(\mathbb{R}), GL_N(\mathbb{C})$, these are groups because the product of invertible matrices is invertible, according to the following formula:

$$(AB)^{-1} = B^{-1}A^{-1}$$

Observe that at $N = 1$ we obtain the groups $(\mathbb{R}^*, \cdot), (\mathbb{C}^*, \cdot)$. At $N \geq 2$ the groups $GL_N(\mathbb{R}), GL_N(\mathbb{C})$ are not abelian, because we do not have $AB = BA$ in general.

(4) The sets $SL_N(\mathbb{R}), SL_N(\mathbb{C})$ formed by the real and complex matrices of determinant 1 are subgroups of the groups in (3), because of the following formula, which shows that the matrices satisfying $\det A = 1$ are stable under multiplication:

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

(5) Regarding now O_N, U_N, here the group property is clear too from definitions, and is best seen by using the associated linear maps, because the composition of two isometries is an isometry. Equivalently, assuming $U^* = U^{-1}$ and $V^* = V^{-1}$, we have:

$$(UV)^* = V^*U^* = V^{-1}U^{-1} = (UV)^{-1}$$

(6) The sets of matrices SO_N, SU_N in the statement are obtained by intersecting the groups in (4) and (5), and so they are groups indeed:

$$SO_N = O_N \cap SL_N(\mathbb{R})$$

$$SU_N = U_N \cap SL_N(\mathbb{C})$$

Thus, all the sets in the statement are indeed groups, as claimed. □

Summarizing, the notion of group is something extremely wide. Now back to Definition 1.1, because of this, at that level of generality, there is nothing much that can be said. Let us record, however, as our first theorem regarding the arbitrary groups:

THEOREM 1.4. *Given a group $(G, \cdot)$, we have the formula*

$$(g^{-1})^{-1} = g$$

valid for any element $g \in G$.

PROOF. This is clear from the definition of the inverses. Assume indeed that:

$$gg^{-1} = g^{-1}g = 1$$

But this shows that g is the inverse of g^{-1}, as claimed. □

As a comment here, the above result, while being something trivial, has led to a lot of controversy among mathematicians and physicists, in recent times. The point indeed is that, for the needs of quantum mechanics, the notion of group must be replaced with something more general, called "quantum group", and there are two schools here:

(1) Certain people, including that unfriendly mathematics or physics professor whose classes no one understands, believe that God is someone nasty, who created quantum mechanics by using some complicated quantum groups, satisfying $(g^{-1})^{-1} \neq g$.

(2) On the opposite, some other mathematicians and physicists, who are typically more relaxed, and better dressed too, and loving life in general, prefer either to use beautiful quantum groups, satisfying $(g^{-1})^{-1} = g$, or not to use quantum groups at all.

Easy choice you would say, but the problem is that, due to some bizarre reasons, the quantum group theory with $(g^{-1})^{-1} = g$ is quite recent, and relatively obscure. For a brief account of what can be done here, mathematically, have a look at my book [9].

1b. Finite groups

In order to have now some theory going, we obviously have to impose some conditions on the groups that we consider. With this idea in mind, let us work out some examples, in the finite group case. The simplest possible finite group is the cyclic group $\mathbb{Z}_N$:

DEFINITION 1.5. *The cyclic group $\mathbb{Z}_N$ is defined as follows:*

(1) *As the additive group of remainders modulo N.*
(2) *As the multiplicative group of the N-th roots of unity.*

The two definitions are equivalent, because if we set $w = e^{2\pi i/N}$, then any remainder modulo N defines a N-th root of unity, according to the following formula:

$$k \to w^k$$

We obtain in this way all the N-roots of unity, and so our correspondence is bijective. Moreover, our correspondence transforms the sum of remainders modulo N into the multiplication of the N-th roots of unity, due to the following formula:

$$w^k w^l = w^{k+l}$$

Thus, the groups defined in (1,2) above are isomorphic, via $k \to w^k$, and we agree to denote by $\mathbb{Z}_N$ the corresponding group. Observe that this group $\mathbb{Z}_N$ is abelian. We will be back to the finite abelian groups later, on several occasions.

As a second basic example of a finite group, we have the symmetric group S_N. This is again something very familiar, appearing as follows:

DEFINITION 1.6. *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.

There are many possible notations for the permutations, the basic one consisting in writing the numbers $1, \ldots, N$, and below them, their permuted versions:

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

Another method, which is faster, and that I personally prefer, remember that time is money, is by denoting the permutations as diagrams, acting from top to bottom:

$\sigma =$ 

Here are some basic properties of the permutations:

THEOREM 1.7. *The permutations have the following properties:*

(1) *There are $N!$ of them.*
(2) *They from a group.*

PROOF. In order to construct a permutation $\sigma \in S_N$, we have:

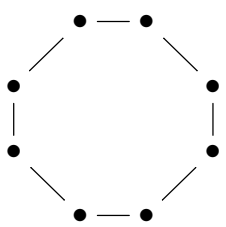
– N choices for the value of $\sigma(N)$.
– $(N-1)$ choices for the value of $\sigma(N-1)$.
– $(N-2)$ choices for the value of $\sigma(N-2)$.
$\vdots$
– and so on, up to 1 choice for the value of $\sigma(1)$.

Thus, we have $N!$ choices, as claimed. As for the second assertion, this is clear. □

The symmetric groups S_N are key objects of group theory, and they have many interesting properties. We will be back to them on many occasions, in what follows, and notably in chapter 2 below, with a systematic study of them.

As a third interesting example now of a finite group, which is something more advanced, we have the dihedral group D_N, which appears as follows:

DEFINITION 1.8. *The dihedral group D_N is the symmetry group of*



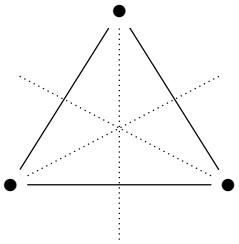
that is, of the regular polygon having N vertices.

In order to understand how this works, here are the basic examples of regular N-gons, at small values of the parameter $N \in \mathbb{N}$, along with their symmetry groups:

$\underline{N = 2}$. Here the N-gon is just a segment, and its symmetries are obviously the identity id, plus the symmetry τ with respect to the middle of the segment:

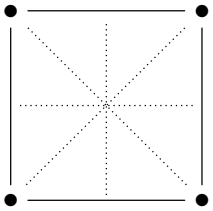
Thus we have $D_2 = \{id, \tau\}$, which in group theory terms means $D_2 = \mathbb{Z}_2$.

$\underline{N = 3}$. Here the N-gon is an equilateral triangle, and we have 6 symmetries, the rotations of angles 0°, 120°, 240°, and the symmetries with respect to the altitudes:



Alternatively, we can say that the symmetries are all the $3! = 6$ possible permutations of the vertices, and so that in group theory terms, we have $D_3 = S_3$.

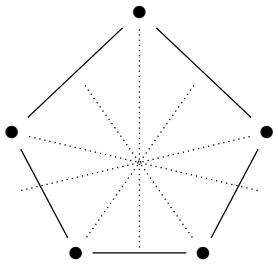
$\underline{N = 4}$. Here the N-gon is a square, and as symmetries we have 4 rotations, of angles $0°, 90°, 180°, 270°$, as well as 4 symmetries, with respect to the 4 symmetry axes, which are the 2 diagonals, and the 2 segments joining the midpoints of opposite sides:



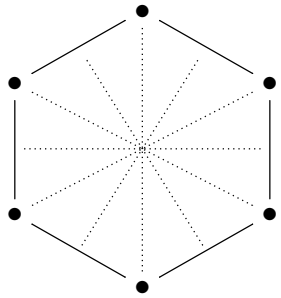
Thus, we obtain as symmetry group some sort of product between $\mathbb{Z}_4$ and $\mathbb{Z}_2$. Observe however that this product is not the usual one, our group being not abelian.

$\underline{N = 5}$. Here the N-gon is a regular pentagon, and as symmetries we have 5 rotations, of angles $0°, 72°, 144°, 216°, 288°$, as well as 5 symmetries, with respect to the 5 symmetry

axes, which join the vertices to the midpoints of the opposite sides:



$\underline{N = 6}$. Here the N-gon is a regular hexagon, and we have 6 rotations, of angles $0°, 60°, 120°, 180°, 240°, 300°$, and 6 symmetries, with respect to the 6 symmetry axes, which are the 3 diagonals, and the 3 segments joining the midpoints of opposite sides:



We can see from the above that the various dihedral groups D_N have many common features, and that there are some differences as well. In general, we have:

PROPOSITION 1.9. *The dihedral group D_N has $2N$ elements, as follows:*

(1) *We have N rotations $R_1, \ldots, R_N$, with R_k being the rotation of angle $2k\pi/N$. When labeling the vertices of the N-gon $1, \ldots, N$, the rotation formula is:*

$$R_k : i \to k + i$$

(2) *We have N symmetries $S_1, \ldots, S_N$, with S_k being the symmetry with respect to the Ox axis rotated by $k\pi/N$. The symmetry formula is:*

$$S_k : i \to k - i$$

PROOF. This is clear, indeed. To be more precise, D_N consists of:

(1) The N rotations, of angles $2k\pi/N$ with $k = 1, \ldots, N$. But these are exactly the rotations $R_1, \ldots, R_N$ from the statement.

(2) 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. But these are exactly the symmetries $S_1, \ldots, S_N$ from the statement. □

With the above description of D_N in hand, we can forget if we want about geometry and the regular N-gon, and talk about D_N abstractly, as follows:

THEOREM 1.10. *The dihedral group D_N is the group having $2N$ elements, $R_1, \ldots, R_N$ and $S_1, \ldots, S_N$, called rotations and symmetries, which multiply as follows,*

$$R_k R_l = R_{k+l}$$

$$R_k S_l = S_{k+l}$$

$$S_k R_l = S_{k-l}$$

$$S_k S_l = R_{k-l}$$

with all the indices being taken modulo N.

PROOF. With notations from Proposition 1.9, the various compositions between rotations and symmetries can be computed as follows:

$$R_k R_l \ : \ i \to l + i \to k + l + i$$

$$R_k S_l \ : \ i \to l - i \to k + l - i$$

$$S_k R_l \ : \ i \to l + i \to k - l - i$$

$$S_k S_l \ : \ i \to l - i \to k - l + i$$

But these are exactly the formulae for $R_{k+l}, S_{k+l}, S_{k-l}, R_{k-l}$, as stated. Now since a group is uniquely determined by its multiplication rules, this gives the result. □

The above result is very nice, and we can even write a nice multiplication table, based on it. We will be back to D_N, on a more systematic basis, in chapter 3 below.

1c. Symmetry groups

As a continuation of the above material, many interesting things can be said about the symmetry groups of the finite graphs, notably with various decomposition results for them. Let us start our study here with something very basic, as follows:

THEOREM 1.11. *Given a finite graph X, with vertices denoted $1, \ldots, N$, the symmetries of X, which are the permutations $\sigma \in S_N$ leaving invariant the edges,*

$$i - j \implies \sigma(i) - \sigma(j)$$

form a subgroup of the symmetric group, as follows, called symmetry group of X:

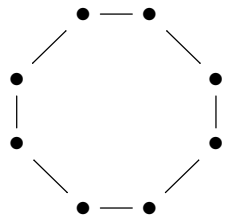
$$G(X) \subset S_N$$

As basic examples, for the empty graph, or for the simplex, we have $G(X) = S_N$.

PROOF. Here the first assertion, regarding the group property of $G(X)$, is clear from definitions, because the symmetries of X are stable under composition. The second assertion, regarding the empty graph and the simplex, is clear as well. □

Let us work out now some more examples. As a first result, dealing with the simplest graph ever, passed the empty graphs and the simplices, we have:

PROPOSITION 1.12. *The symmetry group of the regular N-gon*



is the dihedral group $D_N = \mathbb{Z}_N \rtimes \mathbb{Z}_2$.

PROOF. This is something that we know well from the above, and with the remark, which is something new, that the notation D_N for the group that we get, which is the correct one, is justified by the general group theory discussion before, with N standing for the natural "dimensionality" of this group. To be more precise, geometrically speaking, the regular N-gon is best viewed in $\mathbb{R}^N$, with vertices $1, \ldots, N$ at the standard basis:

$$1 = (1, 0, 0, \ldots, 0, 0)$$

$$2 = (0, 1, 0, \ldots, 0, 0)$$

$$\vdots$$

$$N = (0, 0, 0, \ldots, 0, 1)$$

But, with this interpretation in mind, we are led to an embedding as follows:

$$D_N \subset S_N \subset O_N$$

We conclude from this that N is the correct dimensionality of our group, and so is the correct label to be attached to the dihedral symbol D. Of course, you might find this overly philosophical, or even a bit futile, but listen to this, there are two types of mathematicians in this world, those who use D_N and those who use D_{2N}, and do not ask me why, but it is better to be in the first category, mathematicians using D_N. □

Moving ahead, the problem is now, is Proposition 1.12 good news, or bad news? I don't know about you, but personally I feel quite frustrated by the fact that the computation there leads to $D_N = \mathbb{Z}_N \rtimes \mathbb{Z}_2$, instead to $\mathbb{Z}_N$ itself. I mean, how can a theory be serious, if there is no room there, or even an Emperor's throne, for the cyclic group $\mathbb{Z}_N$.

So, let us fix this. It is obvious that the construction in Theorem 1.11 will work perfectly well for the oriented graphs, or for the colored graphs, so let us formulate:

DEFINITION 1.13. *Given a generalized graph X, with vertices denoted $1,\ldots,N$, the symmetries of X, which are the permutations $\sigma\in S_N$ leaving invariant the edges,*

$$i-j\implies\sigma(i)-\sigma(j)$$

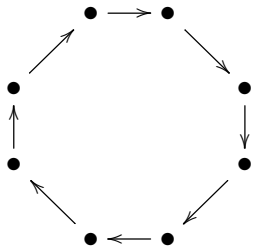
with their orientations and colors, form a subgroup of the symmetric group

$$G(X)\subset S_N$$

called symmetry group of X.

Here, as before with the construction in Theorem 1.11, the fact that we obtain indeed a group is clear from definitions. Now with this convention in hand, we have:

PROPOSITION 1.14. *The symmetry group of the oriented N-gon*



is the cyclic group $\mathbb{Z}_N$.

PROOF. This is clear from definitions, because once we choose a vertex i and denote its image by $\sigma(i)=i+k$, the permutation $\sigma\in S_N$ leaving invariant the edges, with their orientation, must map $\sigma(i+1)=i+k+1$, $\sigma(i+2)=i+k+2$ and so on, and so must be an element of the cyclic group, in remainder modulo N notation $\sigma=k\in\mathbb{Z}_N$. □

With this done, and the authority of $\mathbb{Z}_N$ restored, let us work out some general properties of the construction $X\to G(X)$. For simplicity we will restrict the attention to the usual graphs, as in Theorem 1.11, but pretty much everything will extend to the case of oriented or colored graphs. In fact, our policy in what follows will be that of saying nothing when things extend, and making a comment, when things do not extend.

As a first result, coming as a useful complement to Theorem 1.11, we have:

THEOREM 1.15. *Having a group action on a graph $G\curvearrowright X$ is the same as saying that the action of G leaves invariant the adjacency matrix d, in the sense that:*

$$d_{ij}=d_{g(i)g(j)}\quad,\quad\forall g\in G$$

Equivalently, the action must preserve the spectral projections of d:

$$d=\sum_\lambda\lambda P_\lambda\implies(P_\lambda)_{ij}=(P_\lambda)_{g(i)g(j)}$$

Thus, the symmetry group $G(X)\subset S_N$ is the subgroup preserving the eigenspaces of d.

PROOF. As before with Theorem 1.11, a lot of talking in the statement, with everything being trivial, coming from definitions, and with the statement itself being called Theorem instead of Proposition just due to its theoretical importance. □

Observe that Theorem 1.15 naturally leads us into colored graphs, because while the adjacency matrix is symmetric and binary, $d \in M_N(0,1)^{symm}$, the spectral projections P_λ are also symmetric, but no longer binary, $P_\lambda \in M_N(\mathbb{R})^{symm}$. Moreover, these spectral projections P_λ can have 0 on the diagonal, pushing us into allowing self-edges in our colored graph formalism. We are led in this way to the following statement:

THEOREM 1.16. *Having a group action on a colored graph $G \curvearrowright X$ is the same as saying that the action of G leaves invariant the adjacency matrix d:*

$$d_{ij} = d_{g(i)g(j)} \quad , \quad \forall g \in G$$

Equivalently, the action must preserve the spectral projections of d, as follows:

$$d = \sum_\lambda \lambda P_\lambda \implies (P_\lambda)_{ij} = (P_\lambda)_{g(i)g(j)}$$

Moreover, when allowing self-edges, each P_λ will correspond to a colored graph X_λ.

PROOF. This follows indeed from the above discussion, and with some extra discussion regarding the precise colors that we use, as follows:

(1) When using real colors, the result follows from the linear algebra result regarding the diagonalization of real symmetric matrices, which tells us that the spectral projections of any such matrix $d \in M_N(\mathbb{R})^{symm}$ are also real and symmetric, $P_\lambda \in M_N(\mathbb{R})^{symm}$.

(2) When using complex colors, the result follows from the linear algebra result regarding the diagonalization of complex self-adjoint matrices, which tells us that the spectral projections of any such matrix $d \in M_N(\mathbb{C})^{sa}$ are also self-adjoint, $P_\lambda \in M_N(\mathbb{C})^{sa}$. □

The point with the perspective brought by the above results is that, when using permutation group tools for the study of the groups $G \subset S_N$ acting on our graph, $G \curvearrowright X$, what will eventually happen is that these tools, once sufficiently advanced, will become very close to the regular tools for the study of d, namely the same sort of mixture of linear algebra, calculus and probability, so in the end we will have a unified theory.

But probably too much talking, just trust me, we won't be doing groups and algebra here just because we are scared by analysis, and by the true graph problems. Quite the opposite. And we will see illustrations for this harmony and unity later on.

Leaving now the oriented or colored graphs aside, as per our general graph policy explained above, as a second general result about $X \to G(X)$, we have:

THEOREM 1.17. *The construction $X \to G(X)$ has the property*

$$G(X) = G(X^c)$$

where $X \to X^c$ is the complementation operation.

PROOF. This is clear from the construction of $G(X)$ from Theorem 1.11, and follows as well from the interpretation in Theorem 1.18, because the adjacency matrices of X, X^c are related by the following formula, where $\mathbb{I}_N$ is the all-one matrix:

$$d_X + d_{X^c} = \mathbb{I}_N - 1_N$$

Indeed, since on the right we have the adjacency matrix of the simplex, which commutes with everything, commutation with d_X is equivalent to commutation with d_{X^c}, and this gives the result, via the interpretation of $G(X)$ coming from Theorem 1.15. □

In order to reach now to more advanced results, it is convenient to enlarge the attention to the colored graphs. Indeed, for the colored graphs, we can formulate:

THEOREM 1.18. *Having an action on a colored graph $G \curvearrowright X$ is the same as saying that the action leaves invariant the color components of X. Equivalently, with*

$$d = \sum_{c \in C} c d_c$$

being the color decomposition of the adjacency matrix, with color components

$$(d_c)_{ij} = \begin{cases} 1 & \text{if } d_{ij} = c \\ 0 & \text{otherwise} \end{cases}$$

the action must leave invariant all these color components d_c. Thus, the symmetry group $G(X) \subset S_N$ is the subgroup which preserves all these matrices d_c.

PROOF. As before with our other statements here, in the present first chapter of this book, a lot of talking in the statement, with everything there being trivial. □

I have this feeling that you might get to sleep, on the occasion of the present section, which is overly theoretical, this is how things are, we have to have some theory started, right. But, in the case it is so, I have something interesting for you, in relation with the above. Indeed, by combining Theorem 1.16 with Theorem 1.18, both trivialities, we are led to the following enigmatic statement, which all of the sudden wakes us up:

THEOREM 1.19. *Given an adjacency matrix of a graph X, which can be taken in a colored graph sense, $d \in M_N(\mathbb{C})$, or even binary as usual,*

$$d \in M_N(0, 1)$$

a group action $G \curvearrowright X$ must preserve all "spectral-color" components of this matrix, obtained by succesively applying the spectral decomposition, and color decomposition.

PROOF. This is clear indeed by combining Theorem 1.16 and Theorem 1.18, and with the remark that, indeed, even for a usual binary matrix $d \in M_N(0,1)$ this leads to something non-trivial, because the spectral components of this matrix are no longer binary, and so all of the sudden, we are into colors and everything. □

With the above result in hand, which is something quite unexpected, we are led into a quite interesting linear algebra question, which is surely new for you, namely:

QUESTION 1.20. *What are the spectral-color components of a matrix $d \in M_N(\mathbb{C})$, or even of a usual binary matrix $d \in M_N(0,1)$?*

This question is something non-trivial, and we will be back to this on several occasions, and notably at the end of this book, when talking planar algebras in the sense of Jones [60], which provide the good framework for the study of such questions.

1d. Rotation groups

In the continuous case now, that we need to know about too, we will be mainly interested in the unitary group U_N, in its real version, which is the orthogonal group O_N, and in various technical versions of these basic groups O_N, U_N. So, let us start with:

THEOREM 1.21. *We have the following results:*

(1) *The rotations of $\mathbb{R}^N$ form the orthogonal group O_N, which is given by:*

$$O_N = \left\{ U \in M_N(\mathbb{R}) \middle| U^t = U^{-1} \right\}$$

(2) *The rotations of $\mathbb{C}^N$ form the unitary group U_N, which is given by:*

$$U_N = \left\{ U \in M_N(\mathbb{C}) \middle| U^* = U^{-1} \right\}$$

In addition, we can restrict the attention to the rotations of the corresponding spheres.

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

(1) We know from linear algebra that a linear map $T : \mathbb{R}^N \to \mathbb{R}^N$, written as $T(x) = Ux$ with $U \in M_N(\mathbb{R})$, is a rotation, in the sense that it preserves the distances and the angles, precisely when the associated matrix U is orthogonal, in the following sense:

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

Thus, we obtain the result. As for the last assertion, this is clear as well, because an isometry of $\mathbb{R}^N$ is the same as an isometry of the unit sphere $S_{\mathbb{R}}^{N-1} \subset \mathbb{R}^N$.

(2) We know from linear algebra that a linear map $T : \mathbb{C}^N \to \mathbb{C}^N$, written as $T(x) = Ux$ with $U \in M_N(\mathbb{C})$, is a rotation, in the sense that it preserves the distances and the scalar products, precisely when the associated matrix U is unitary, in the following sense:

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

Thus, we obtain the result. As for the last assertion, this is clear as well, because an isometry of $\mathbb{C}^N$ is the same as an isometry of the unit sphere $S_{\mathbb{C}}^{N-1} \subset \mathbb{C}^N$. □

In order to introduce some further continuous groups $G \subset U_N$, we will need:

PROPOSITION 1.22. *We have the following results:*

(1) *For an orthogonal matrix $U \in O_N$ we have $\det U \in \{\pm 1\}$.*
(2) *For a unitary matrix $U \in U_N$ we have $\det U \in \mathbb{T}$.*

PROOF. This is clear from the equations defining O_N, U_N, as follows:

(1) We have indeed the following implications:

$$\begin{aligned} U \in O_N &\implies U^t = U^{-1} \\ &\implies \det U^t = \det U^{-1} \\ &\implies \det U = (\det U)^{-1} \\ &\implies \det U \in \{\pm 1\} \end{aligned}$$

(2) We have indeed the following implications:

$$\begin{aligned} U \in U_N &\implies U^* = U^{-1} \\ &\implies \det U^* = \det U^{-1} \\ &\implies \overline{\det U} = (\det U)^{-1} \\ &\implies \det U \in \mathbb{T} \end{aligned}$$

Here we have used the fact that $\bar{z} = z^{-1}$ means $z\bar{z} = 1$, and so $z \in \mathbb{T}$. □

We can now introduce the subgroups $SO_N \subset O_N$ and $SU_N \subset U_N$, as being the subgroups consisting of the rotations which preserve the orientation, as follows:

THEOREM 1.23. *The following are groups of matrices,*

$$SO_N = \left\{ U \in O_N \middle| \det U = 1 \right\} \quad , \quad SU_N = \left\{ U \in U_N \middle| \det U = 1 \right\}$$

consisting of the rotations which preserve the orientation.

PROOF. The fact that we have indeed groups follows from the properties of the determinant, of from the property of preserving the orientation, which is clear as well. □

Summarizing, we have constructed so far 4 continuous groups of matrices, consisting of various rotations, with inclusions between them, as follows:

$$\begin{array}{ccc} SU_N & \longrightarrow & U_N \\ \uparrow & & \uparrow \\ SO_N & \longrightarrow & O_N \end{array}$$

At $N = 1$ the situation is trivial, and we obtain very simple groups, as follows:

PROPOSITION 1.24. *The basic continuous groups at $N = 1$ are*

$$\begin{array}{ccc} \{1\} & \longrightarrow & \mathbb{T} \\ \uparrow & & \uparrow \\ \{1\} & \longrightarrow & \{\pm 1\} \end{array}$$

or, equivalently, are the following cyclic groups,

$$\begin{array}{ccc} \mathbb{Z}_1 & \longrightarrow & \mathbb{Z}_\infty \\ \uparrow & & \uparrow \\ \mathbb{Z}_1 & \longrightarrow & \mathbb{Z}_2 \end{array}$$

with the convention that $\mathbb{Z}_s$ is the group of s-th roots of unity.

PROOF. This is clear from definitions, because for a 1×1 matrix the unitarity condition reads $\bar{U} = U^{-1}$, and so $U \in \mathbb{T}$, and this gives all the results. □

At $N = 2$ now, let us first discuss the real case. The result here is as follows:

THEOREM 1.25. *We have the following results:*

(1) *SO_2 is the group of usual rotations in the plane, which are given by:*

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

(2) *O_2 consists in addition of the usual symmetries in the plane, given by:*

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

(3) *Abstractly speaking, we have isomorphisms as follows:*

$$SO_2 \simeq \mathbb{T} \quad , \quad O_2 = \mathbb{T} \rtimes \mathbb{Z}_2$$

(4) *When discretizing all this, by replacing the 2-dimensional unit sphere $\mathbb{T}$ by the regular N-gon, the latter isomorphism discretizes as $D_N = \mathbb{Z}_N \rtimes \mathbb{Z}_2$.*

PROOF. This follows from some elementary computations, as follows:

(1) The first assertion is clear, because only the rotations of the plane in the usual sense preserve the orientation. As for the formula of R_t, this is something that we know well from linear algebra, obtained by computing $R_t\binom{1}{0}$ and $R_t\binom{0}{1}$.

(2) The first assertion is clear, because rotations left aside, we are left with the symmetries of the plane, in the usual sense. As for formula of S_t, this is something that we know well too, obtained by computing $S_t\binom{1}{0}$ and $S_t\binom{0}{1}$.

(3) The first assertion is clear, because the angles $t \in \mathbb{R}$, taken as usual modulo 2π, form the group $\mathbb{T}$. As for the second assertion, the proof here is similar to the proof of the crossed product decomposition $D_N = \mathbb{Z}_N \rtimes \mathbb{Z}_2$ for the dihedral groups.

(4) This is something more speculative, the idea here being that the isomorphism $O_2 = \mathbb{T} \rtimes \mathbb{Z}_2$ appears from $D_N = \mathbb{Z}_N \rtimes \mathbb{Z}_2$ by taking the $N \to \infty$ limit. □

Moving forward, let us keep working out what happens at $N = 2$, but this time with a study in the complex case. We first have here the following key result:

THEOREM 1.26. *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 the unit sphere $S^1_{\mathbb{C}} \subset \mathbb{C}^2$.

PROOF. Consider indeed an arbitrary 2×2 matrix, written as follows:

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

Assuming that we have $\det U = 1$, the inverse must be 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, for the matrix entries:

$$d = \bar{a} \quad , \quad c = -\bar{b}$$

Thus our matrix must be of the following special form:

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

Moreover, since the determinant is 1, we must have, as stated:

$$|a|^2 + |b|^2 = 1$$

Thus, we are done with one inclusion. As for the converse, this is clear, the matrices in the statement being unitaries, and of determinant 1, and so being elements of SU_2. Finally, regarding the last assertion, recall that the unit sphere $S^1_{\mathbb{C}} \subset \mathbb{C}^2$ is given by:

$$S^1_{\mathbb{C}} = \left\{(a, b) \;\middle|\; |a|^2 + |b|^2 = 1\right\}$$

Thus, we have an isomorphism of compact spaces, as follows:

$$SU_2 \simeq S^1_{\mathbb{C}} \quad , \quad \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \to (a, b)$$

We have therefore proved our theorem. □

Regarding now the unitary group U_2, the result here is similar, as follows:

THEOREM 1.27. *We have the following formula,*

$$U_2 = \left\{ d \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \;\middle|\; |a|^2 + |b|^2 = 1, |d| = 1 \right\}$$

which makes U_2 be a quotient compact space, as follows,

$$S^1_{\mathbb{C}} \times \mathbb{T} \to U_2$$

but with this parametrization being no longer bijective.

PROOF. In one sense, this is clear from Theorem 1.26, because we have:

$$|d| = 1 \implies dSU_2 \subset U_2$$

In the other sense, let us pick an arbitrary matrix $U \in U_2$. 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, defined up to a sign choice:

$$d = \sqrt{\det U}$$

We know from Proposition 1.22 that we have $|d| = 1$. Thus the rescaled matrix $V = U/d$ is unitary, $V \in U_2$. As for the determinant of this matrix, this is given by:

$$\begin{aligned} \det(V) &= \det(U/d) \\ &= \det(U)/d^2 \\ &= \det(U)/\det(U) \\ &= 1 \end{aligned}$$

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 the matrix $U = dV$ appears as in the statement. Finally, observe that the result that we have just proved provides us with a quotient map as follows:

$$S^1_{\mathbb{C}} \times \mathbb{T} \to U_2 \quad , \quad ((a, b), d) \to d \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$$

However, the parametrization is no longer bijective, because when we globally switch signs, the element $((-a, -b), -d)$ produces the same element of U_2. □

At a more specialized level now, we first have the groups B_N, C_N, consisting of the orthogonal and unitary bistochastic matrices. Let us start with:

DEFINITION 1.28. *A square matrix $M \in M_N(\mathbb{C})$ is called bistochastic if each row and each column sum up to the same number:*

$$\begin{array}{ccccc} M_{11} & \ldots & M_{1N} & \to & \lambda \\ \vdots & & \vdots & & \\ M_{N1} & \ldots & M_{NN} & \to & \lambda \\ \downarrow & & \downarrow & & \\ \lambda & & \lambda & & \end{array}$$

If this happens only for the rows, or only for the columns, the matrix is called row-stochastic, respectively column-stochastic.

In what follows we will be interested in the unitary bistochastic matrices, which are quite interesting objects. As a first result, regarding such matrices, we have:

PROPOSITION 1.29. *For a unitary matrix $U \in U_N$, the following are equivalent:*

(1) *H is bistochastic, with sums λ.*
(2) *H is row stochastic, with sums λ, and $|\lambda| = 1$.*
(3) *H is column stochastic, with sums λ, and $|\lambda| = 1$.*

PROOF. By using a symmetry argument we just need to prove (1) $\iff$ (2), and both the implications are elementary, as follows:

(1) $\implies$ (2) If we denote by $U_1, \ldots, U_N \in \mathbb{C}^N$ the rows of U, we have indeed:

$$\begin{aligned} 1 &= \sum_i < U_1, U_i > \\ &= \sum_j U_{1j} \sum_i \bar{U}_{ij} \\ &= \sum_j U_{1j} \cdot \bar{\lambda} \\ &= |\lambda|^2 \end{aligned}$$

(2) $\implies$ (1) Consider the all-one vector $\xi = (1)_i \in \mathbb{C}^N$. The fact that U is row-stochastic with sums λ reads:

$$\begin{aligned} \sum_j U_{ij} = \lambda, \forall i \quad &\iff \quad \sum_j U_{ij}\xi_j = \lambda\xi_i, \forall i \\ &\iff \quad U\xi = \lambda\xi \end{aligned}$$

Also, the fact that U is column-stochastic with sums λ reads:

$$\begin{aligned} \sum_i U_{ij} = \lambda, \forall j \quad &\iff \quad \sum_j U_{ij}\xi_i = \lambda\xi_j, \forall j \\ &\iff \quad U^t\xi = \lambda\xi \end{aligned}$$

We must prove that the first condition implies the second one, provided that the row sum λ satisfies $|\lambda| = 1$. But this follows from the following computation:

$$\begin{aligned} U\xi = \lambda\xi \quad &\implies \quad U^*U\xi = \lambda U^*\xi \\ &\implies \quad \xi = \lambda U^*\xi \\ &\implies \quad \xi = \bar{\lambda}U^t\xi \\ &\implies \quad U^t\xi = \lambda\xi \end{aligned}$$

Thus, we have proved both the implications, and we are done. □

The unitary bistochastic matrices are stable under a number of operations, and in particular under taking products. Thus, these matrices form a group. We have:

THEOREM 1.30. *The real and complex bistochastic groups, which are the sets*

$$B_N \subset O_N \quad , \quad C_N \subset U_N$$

consisting of matrices which are bistochastic, are isomorphic to O_{N-1}, U_{N-1}.

PROOF. Let us pick a matrix $F \in U_N$ satisfying the following condition, where $e_0, \ldots, e_{N-1}$ is the standard basis of $\mathbb{C}^N$, and where ξ is the all-one vector:

$$Fe_0 = \frac{1}{\sqrt{N}}\xi$$

We have then, by using the above property of F:

$$\begin{aligned} u\xi = \xi &\iff uFe_0 = Fe_0\\ &\iff F^*uFe_0 = e_0\\ &\iff F^*uF = diag(1, w)\end{aligned}$$

Thus we have isomorphisms as in the statement, given by $w_{ij} \to (F^*uF)_{ij}$. □

We will be back to B_N, C_N later. Moving ahead now, as yet another basic example of a continuous group, we have the symplectic group Sp_N. Let us begin with:

DEFINITION 1.31. *The "super-space" $\bar{\mathbb{C}}^N$ is the usual space $\mathbb{C}^N$, with its standard basis $\{e_1, \ldots, e_N\}$, with a chosen sign $\varepsilon = \pm 1$, and a chosen involution on the indices:*

$$i \to \bar{i}$$

The "super-identity" matrix is $J_{ij} = \delta_{i\bar{j}}$ for $i \leq j$ and $J_{ij} = \varepsilon\delta_{i\bar{j}}$ for $i \geq j$.

Up to a permutation of the indices, we have a decomposition $N = 2p + q$, such that the involution is, in standard permutation notation:

$$(12) \ldots (2p-1, 2p)(2p+1) \ldots (q)$$

Thus, up to a base change, the super-identity is as follows, where $N = 2p + q$ and $\varepsilon = \pm 1$, with the 1_q block at right disappearing if $\varepsilon = -1$:

$$J = \begin{pmatrix} 0 & 1 & & & & & & & \\ \varepsilon 1 & 0_{(0)} & & & & & & & \\ & & \ddots & & & & & & \\ & & & 0 & 1 & & & & \\ & & & \varepsilon 1 & 0_{(p)} & & & & \\ & & & & & 1_{(1)} & & & \\ & & & & & & \ddots & & \\ & & & & & & & 1_{(q)} \end{pmatrix}$$

In the case $\varepsilon = 1$, the super-identity is the following matrix:

$$J_+(p,q) = \begin{pmatrix} 0 & 1 & & & & & & & \\ 1 & 0_{(1)} & & & & & & & \\ & & \ddots & & & & & & \\ & & & 0 & 1 & & & & \\ & & & 1 & 0_{(p)} & & & & \\ & & & & & 1_{(1)} & & & \\ & & & & & & \ddots & & \\ & & & & & & & 1_{(q)} \end{pmatrix}$$

In the case $\varepsilon=-1$ now, the diagonal terms vanish, and the super-identity is:

$$J_-(p,0)=\begin{pmatrix}0&1&&&\\-1&0_{(1)}&&&\\&&\ddots&&\\&&&0&1\\&&&-1&0_{(p)}\end{pmatrix}$$

With the above notions in hand, we have the following result:

THEOREM 1.32. *The super-orthogonal group, which is by definition*

$$\bar{O}_N=\left\{U\in U_N\middle|U=J\bar{U}J^{-1}\right\}$$

with J being the super-identity matrix, is as follows:

(1) *At $\varepsilon=1$ we have $\bar{O}_N=O_N$.*
(2) *At $\varepsilon=-1$ we have $\bar{O}_N=Sp_N$.*

PROOF. These results are both elementary, as follows:

(1) At $\varepsilon=-1$ this follows from definitions.

(2) At $\varepsilon=1$ now, consider the root of unity $\rho=e^{\pi i/4}$, and let:

$$\Gamma=\frac{1}{\sqrt{2}}\begin{pmatrix}\rho&\rho^7\\\rho^3&\rho^5\end{pmatrix}$$

Then this matrix Γ is unitary, and we have the following formula:

$$\Gamma\begin{pmatrix}0&1\\1&0\end{pmatrix}\Gamma^t=1$$

Thus the following matrix is unitary as well, and satisfies $CJC^t=1$:

$$C=\begin{pmatrix}\Gamma^{(1)}&&&\\&\ddots&&\\&&\Gamma^{(p)}&\\&&&1_q\end{pmatrix}$$

Thus in terms of $V=CUC^*$ the relations $U=J\bar{U}J^{-1}=$ unitary simply read:

$$V=\bar{V}=\text{unitary}$$

Thus we obtain an isomorphism $\bar{O}_N=O_N$ as in the statement. □

Regarding now Sp_N, we have the following result:

THEOREM 1.33. *The symplectic group $Sp_N \subset U_N$, which is by definition*

$$Sp_N = \left\{ U \in U_N \middle| U = J\bar{U}J^{-1} \right\}$$

consists of the SU_2 patterned matrices,

$$U = \begin{pmatrix} a & b & \ldots \\ -\bar{b} & \bar{a} & \\ \vdots & & \ddots \end{pmatrix}$$

which are unitary, $U \in U_N$. In particular, we have $Sp_2 = SU_2$.

PROOF. This follows indeed from definitions, because the condition $U = J\bar{U}J^{-1}$ corresponds precisely to the fact that U must be a SU_2-patterned matrix. □

We will be back later to the symplectic groups, towards the end of the present book, with more results about them. In the meantime, have a look at the mechanics book of Arnold [2], which explains what the symplectic groups and geometry are good for.

1e. Exercises

Exercises:

EXERCISE 1.34.

EXERCISE 1.35.

EXERCISE 1.36.

EXERCISE 1.37.

EXERCISE 1.38.

EXERCISE 1.39.

EXERCISE 1.40.

EXERCISE 1.41.

Bonus exercise.

CHAPTER 2

Permutations

2a. Symmetric groups

Let us go back now to the symmetric groups, which are fundamental objects in group theory, as we will soon discover. These groups are constructed as follows:

DEFINITION 2.1. *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*.*

There are many possible notations for the permutations, the basic one consisting in writing the numbers $1, \ldots, N$, and below them, their permuted versions:

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

Another method, which is faster, and that I personally prefer, remember that time is money, is by denoting the permutations as diagrams, acting from top to bottom:

$\sigma =$ 

Here are some basic properties of the permutations:

THEOREM 2.2. *The permutations have the following properties:*

(1) *There are* $N!$ *of them.*
(2) *They from a group.*

PROOF. In order to construct a permutation $\sigma \in S_N$, 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 $\sigma(1)$.

Thus, we have $N!$ choices, as claimed. As for the second assertion, this is clear. □

At the level of the general theory now, by using the symmetric groups, we have the following fundamental result regarding the finite groups, due to Cayley:

THEOREM 2.3. *Given a finite group G, we have an embedding as follows,*

$$G \subset S_N \quad , \quad g \to (h \to gh)$$

with $N = |G|$. Thus, any finite group is a permutation group.

PROOF. Given a group element $g \in G$, we can associate to it the following map:

$$\sigma_g : G \to G \quad , \quad h \to gh$$

Since $gh = gh'$ implies $h = h'$, this map is bijective, and so is a permutation of G, viewed as a set. Thus, with $N = |G|$, we can view this map as a usual permutation, $\sigma_G \in S_N$. Summarizing, we have constructed so far a map as follows:

$$G \to S_N \quad , \quad g \to \sigma_g$$

Our first claim is that this is a group morphism. Indeed, this follows from:

$$\sigma_g\sigma_h(k) = \sigma_g(hk) = ghk = \sigma_{gh}(k)$$

It remains to prove that this group morphism is injective. But this follows from:

$$\begin{aligned} g \neq h &\implies \sigma_g(1) \neq \sigma_h(1) \\ &\implies \sigma_g \neq \sigma_h \end{aligned}$$

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

Observe that in the above statement the embedding $G \subset S_N$ that we constructed depends on a particular writing $G = \{g_1, \ldots, g_N\}$, which is needed in order to identify the permutations of G with the elements of the symmetric group S_N. This is not very good, in practice, and as an illustration, for the basic examples of groups that we know, the Cayley theorem provides us with embeddings as follows:

$$\mathbb{Z}_N \subset S_N \quad , \quad D_N \subset S_{2N} \quad , \quad S_N \subset S_{N!} \quad , \quad H_N \subset S_{2^N N!}$$

And here the first embedding is the good one, the second one is not the best possible one, but can be useful, and the third and fourth embeddings are useless. Thus, as a conclusion, the Cayley theorem remains something quite theoretical. We will be back to this later on, with a systematic study of the "representation" problem.

Getting back now to our main series of finite groups, $\mathbb{Z}_N \subset D_N \subset S_N \subset H_N$, these are of course permutation groups, according to the above. However, and perhaps even more interestingly, these are as well subgroups of the orthogonal group O_N:

$$\mathbb{Z}_N \subset D_N \subset S_N \subset H_N \subset O_N$$

Indeed, we have $H_N \subset O_N$, because any transformation of the unit cube in $\mathbb{R}^N$ must extend into an isometry of the whole $\mathbb{R}^N$, in the obvious way. Now in view of this, it makes sense to look at the finite subgroups $G \subset O_N$. With two remarks, namely:

(1) Although we do not have examples yet, following our general "complex is better than real" philosophy, it is better to look at the general subgroups $G \subset U_N$.

(2) Also, it is better to upgrade our study to the case where G is compact, and this in order to cover some interesting continuous groups, such as O_N, U_N, SO_N, SU_N.

Long story short, we are led in this way to the study of the closed subgroups $G \subset U_N$. Let us start our discussion here with the following simple fact:

PROPOSITION 2.4. *The closed subgroups $G \subset U_N$ are precisely the closed sets of matrices $G \subset U_N$ satisfying the following conditions:*

(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 from definitions, the only point with this statement being the fact that a subset $G \subset U_N$ can be a group or not, as indicated above. □

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 then with a result stating that, conversely, any smooth compact group appears as a closed subgroup $G \subset U_N$ of some unitary group. However, all this is quite advanced, and we will not need it, in what follows.

As a second result now regarding the closed subgroups $G \subset U_N$, let us prove that any finite group G appears in this way. This is something more or less clear from what we have, but let us make this precise. We first have the following key result:

THEOREM 2.5. *We have a group embedding as follows, obtained by regarding S_N as the permutation group of the N coordinate axes of $\mathbb{R}^N$,*

$$S_N \subset O_N$$

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. Regarding now the explicit formula, 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. □

We can combine the above result with the Cayley theorem, and we obtain the following result, which is something very nice, having theoretical importance:

THEOREM 2.6. *Given a finite group G, we have an embedding as follows,*

$$G \subset O_N \quad , \quad g \to (e_h \to e_{gh})$$

with $N = |G|$. Thus, any finite group is an orthogonal matrix group.

PROOF. The Cayley theorem gives an embedding as follows:

$$G \subset S_N \quad , \quad g \to (h \to gh)$$

On the other hand, Theorem 2.5 provides us with an embedding as follows:

$$S_N \subset O_N \quad , \quad \sigma \to (e_i \to e_{\sigma(i)})$$

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

The same remarks as for the Cayley theorem apply. First, the embedding $G \subset O_N$ that we constructed depends on a particular writing $G = \{g_1, \ldots, g_N\}$. And also, for the basic examples of groups that we know, the embeddings that we obtain are as follows:

$$\mathbb{Z}_N \subset O_N \quad , \quad D_N \subset O_{2N} \quad , \quad S_N \subset O_{N!} \quad , \quad H_N \subset O_{2^N N!}$$

Summarizing, all this is not very good, and in order to advance, it is probably better to forget about the Cayley theorem, and build on Theorem 2.5 instead.

In relation with the basic groups, we have here the following result:

THEOREM 2.7. *We have the following finite groups of matrices:*

(1) $\mathbb{Z}_N \subset O_N$, *the cyclic permutation matrices.*
(2) $D_N \subset O_N$, *the dihedral permutation matrices.*
(3) $S_N \subset O_N$, *the permutation matrices.*
(4) $H_N \subset O_N$, *the signed permutation matrices.*

PROOF. This is something self-explanatory, the idea being that Theorem 2.5 provides us with embeddings as follows, given by the permutation matrices:

$$\mathbb{Z}_N \subset D_N \subset S_N \subset O_N$$

In addition, looking back at the definition of H_N, this group inserts into the embedding on the right, $S_N \subset H_N \subset O_N$. Thus, we are led to the conclusion that all our 4 groups appear as groups of suitable "permutation type matrices". To be more precise:

(1) The cyclic permutation matrices are by definition the matrices as follows, with 0 entries elsewhere, and form a group, which is isomorphic to the cyclic group $\mathbb{Z}_N$:

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

(2) The dihedral matrices are the above cyclic permutation matrices, plus some suitable symmetry permutation matrices, and form a group which is isomorphic to D_N.

(3) The permutation matrices, which by Theorem 2.5 form a group which is isomorphic to S_N, are the $0-1$ matrices having exactly one 1 on each row and column.

(4) Finally, regarding the signed permutation matrices, these are by definition the $(-1)-0-1$ matrices having exactly one nonzero entry on each row and column, and we know that these matrices form a group, which is isomorphic to H_N. □

We will be back to the permutation matrices, later in this chapter.

2b. Cycles, signature

We would like to discuss now some useful decomposition results, for the permutations. For this purpose, we will need some basic abstract results, about the abstract groups, which are good to know. Let us start with the following basic fact:

THEOREM 2.8. *Given a finite group G and a subgroup $H\subset G$, the sets*

$$G/H=\{gH\Big|g\in G\}\quad,\quad H\backslash G=\{Hg\Big|g\in G\}$$

both consist of partitions of G into subsets of size H, and we have the formula

$$|G|=|H|\cdot|G/H|=|H|\cdot|H\backslash G|$$

which shows that the order of the subgroup divides the order of the group:

$$|H|\ \Big|\ |G|$$

When $H\subset G$ is normal, $gH=Hg$ for any $g\in G$, the space $G/H=H\backslash G$ is a group.

PROOF. There are several assertions here, but these are all trivial, when deduced in the precise order indicated in the statement. To be more precise, the partition claim for G/H can be deduced as follows, and the proof for $H\backslash G$ is similar:

$$gH\cap kH\neq\emptyset\iff g^{-1}k\in H\iff gH=kH$$

With this in hand, the cardinality formulae are all clear, and it remains to prove the last assertion. But here, the point is that when $H \subset G$ is normal, we have:

$$gH = kH, sH = tH \implies gsH = gtH = gHt = kHt = ktH$$

Thus $G/H = H\backslash G$ is a indeed group, with multiplication $(gH)(sH) = gsH$. □

As a main consequence of the above result, which is equally famous, we have:

THEOREM 2.9. *Given a finite group G, any $g \in G$ generates a cyclic subgroup*

$$< g >= \{1, g, g^2, \ldots, g^{k-1}\}$$

with $k = ord(g)$ being the smallest number $k \in \mathbb{N}$ satisfying $g^k = 1$. Also, we have

$$ord(g) \ \Big| \ |G|$$

that is, the order of any group element divides the order of the group.

PROOF. As before with Theorem 2.8, we have opted here for a long collection of statements, which are all trivial, when deduced in the above precise order. To be more precise, consider the semigroup $< g >\subset G$ formed by the sequence of powers of g:

$$< g >= \{1, g, g^2, g^3, \ldots\} \subset G$$

Since G was assumed to be finite, the sequence of powers must cycle, $g^n = g^m$ for some $n < m$, and so we have $g^k = 1$, with $k = m - n$. Thus, we have in fact:

$$< g >= \{1, g, g^2, \ldots, g^{k-1}\}$$

Moreover, we can choose $k \in \mathbb{N}$ to be minimal with this property, and with this choice, we have a set without repetitions. Thus $< g >\subset G$ is indeed a group, and more specifically a cyclic group, of order $k = ord(g)$. Finally, $ord(g) \,|\, |G|$ follows from Theorem 2.8. □

With this, we can now talk about the cycle decomposition of permutations. Many interesting things can be said here, of all difficulty levels.

At a more advanced level now, we have the following result, that you surely know from linear algebra, and more specifically, from the theory of the determinant:

THEOREM 2.10. *The permutations have a signature function*

$$\varepsilon : S_N \to \{\pm 1\}$$

which can be defined in the following equivalent ways:

(1) *As $(-1)^c$, where c is the number of inversions.*
(2) *As $(-1)^t$, where t is the number of transpositions.*
(3) *As $(-1)^o$, where o is the number of odd cycles.*
(4) *As $(-1)^x$, where x is the number of crossings.*
(5) *As the sign of the corresponding permuted basis of $\mathbb{R}^N$.*

PROOF. We have explain what the numbers c, t, o, x appearing in (1-4) exactly are, then why they are well-defined modulo 2, then why they are equal to each other, and finally why the constructions (1-4) yield the same sign as (5). Let us begin with the first two steps, namely precise definition of the numbers c, t, o, x, modulo 2:

(1) The idea here is that given any two numbers $i < j$ among $1, \ldots, N$, the permutation can either keep them in the same order, $\sigma(i) < \sigma(j)$, or invert them:

$$\sigma(j) > \sigma(i)$$

Now by making $i < j$ vary over all pairs of numbers in $1, \ldots, N$, we can count the number of inversions, and call it c. This is an integer, $c \in \mathbb{N}$, which is well-defined.

(2) Here the idea, which is something quite intuitive, is that any permutation appears as a product of switches, also called transpositions:

$$i \leftrightarrow j$$

The decomposition as a product of transpositions is not unique, but the number t of the needed transpositions is unique, when considered modulo 2. This follows for instance from the equivalence of (2) with (1,3,4,5), explained below.

(3) Here the point is that any permutation decomposes, in a unique way, as a product of cycles, which are by definition permutations of the following type:

$$i_1 \to i_2 \to i_3 \to \ldots\ldots \to i_k \to i_1$$

Some of these cycles have even length, and some others have odd length. By counting those having odd length, we obtain a well-defined number $o \in \mathbb{N}$.

(4) Here the method is that of drawing the permutation, as we usually do, and by avoiding triple crossings, and then counting the number of crossings. This number x depends on the way we draw the permutations, but modulo 2, we always get the same number. Indeed, this follows from the fact that we can continuously pass from a drawing to each other, and that when doing so, the number of crossings can only jump by ± 2.

Summarizing, we have 4 different definitions for the signature of the permutations, which all make sense, constructed according to (1-4) above. Regarding now the fact that we always obtain the same number, this can be established as follows:

(1)=(2) This is clear, because any transposition inverts once, modulo 2.

(1)=(3) This is clear as well, because the odd cycles invert once, modulo 2.

(1)=(4) This comes from the fact that the crossings correspond to inversions.

(2)=(3) This follows by decomposing the cycles into transpositions.

(2)=(4) This comes from the fact that the crossings correspond to transpositions.

(3)=(4) This follows by drawing a product of cycles, and counting the crossings.

Finally, in what regards the equivalence of all these constructions with (5), here simplest is to use (2). Indeed, we already know that the sign of a system of vectors switches when interchanging two vectors, and so the equivalence between (2,5) is clear. □

As already mentioned, the permutations and their signature are key ingredients in linear algebra, in the theory of the determinant. It is tempting to take a break at this point from group theory, and talk a bit about this, but would this linear algebra intermezzo be really welcome. Not clear, so time to ask the cat. And cat declares:

CAT 2.11. *We cats, both Eastern and Western, know well about the determinant, we need that in our daily work. As for you guys, humans, no idea about it.*

Okay, thanks cat, so not clear what to do, and since we doubt, let's just go for it. The determinant of a matrix is by definition the signed volume of the parallelepiped formed by its column vectors. In other words, we have the following formula, with $v_i \in \mathbb{R}^N$:

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

The point now is that, by playing with Thales and other elementary geometry tools, we are led to some rules for computing the determinants, that you surely know well. And, once we know this, permutations and their signature come into play, as follows:

THEOREM 2.12. *We have the following formula for 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. This follows by recurrence over $N \in \mathbb{N}$, as follows:

(1) When developing the determinant over the first column, we obtain a signed sum of N determinants of size $(N-1) \times (N-1)$. But each of these determinants can be computed by developing over the first column too, and so on, and we are led to the conclusion that we have a formula as in the statement, with $\varepsilon(\sigma) \in \{-1, 1\}$ being certain coefficients.

(2) But these latter coefficients $\varepsilon(\sigma) \in \{-1, 1\}$ can only be the signatures of the corresponding permutations $\sigma \in S_N$, with this being something that can be viewed again by recurrence, with either of the definitions (1-5) in Theorem 2.10 for the signature. □

The above result is something quite tricky, and in order to get familiar with it, there is nothing better than doing some computations. As a first, basic example, in 2 dimensions we recover the usual formula of the determinant, the details being as follows:

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = \varepsilon(|\,|) \cdot ad + \varepsilon(\diagdown) \cdot cb = ad - bc$$

In 3 dimensions now, we recover the well-known 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:

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

In 4 dimensions, the formula of the determinant is as follows:

THEOREM 2.13. *The determinant of the 4×4 matrices is given by*

$$\begin{vmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \\ c_1 & c_2 & c_3 & c_4 \\ d_1 & d_2 & d_3 & d_4 \end{vmatrix}$$

$$\begin{aligned} = \ & a_1b_2c_3d_4 - a_1b_2c_4d_3 - a_1b_3c_2d_4 + a_1b_3c_4d_2 + a_1b_4c_2d_3 - a_1b_4c_3d_2 \\ - \ & a_2b_1c_3d_4 + a_2b_1c_4d_3 + a_2b_3c_1d_4 - a_2b_3c_4d_1 - a_2b_4c_1d_3 + a_2b_4c_3d_1 \\ + \ & a_3b_1c_2d_4 + a_3b_1c_4d_2 - a_3b_2c_1d_4 + a_3b_2c_4d_1 + a_3b_4c_1d_2 - a_3b_4c_2d_1 \\ - \ & a_4b_1c_2d_3 + a_4b_1c_3d_2 - a_4b_2c_1d_3 - a_4b_2c_3d_1 - a_4b_3c_1d_2 + a_4b_3c_2d_1 \end{aligned}$$

with the generic term being of the following form, with $\sigma \in S_4$,

$$\pm a_{\sigma(1)}b_{\sigma(2)}c_{\sigma(3)}d_{\sigma(4)}$$

and with the sign being $\varepsilon(\sigma)$, computable by using Theorem 2.10.

PROOF. We can indeed recover this formula as well as a particular case of Theorem 2.12. To be more precise, the permutations in the statement are listed according to the lexicographic order, and the computation of the corresponding signatures is something elementary, by using the various rules from Theorem 2.10. □

Finally, still talking linear algebra, we have the following key result, which is something that you surely know, but whose proof requires Theorem 2.12, using permutations:

THEOREM 2.14. *We have the formula*

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

valid for any square matrix A.

PROOF. This follows from the formula in Theorem 2.12. Indeed, we have:

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

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

Getting back now to groups, as another illustration for the above, we have:

THEOREM 2.15. *We have the following formula,*

$$A_N = S_N \cap SO_N$$

with the intersection being computed inside O_N.

PROOF. Consider indeed the standard embedding $S_N \subset O_N$, obtained by permuting the coordinate axes of $\mathbb{R}^N$, which in practice is given by the permutation matrices. The determinant of a permutation $\sigma \in S_N$ is then its signature, and this gives the result. □

So long for applications of the symmetric groups. We will be back to this.

2c. Derangements

As a continuation of the above, the permutations having no fixed points at all are called derangements, and the first question which appears, which is a classical question in combinatorics, is that of counting these derangements.

For this purpose, we will need the inclusion-exclusion principle, which is as follows:

THEOREM 2.16. *We have the following formula,*

$$\left|\left(\bigcup_i A_i\right)^c\right| = |A| - \sum_i |A_i| + \sum_{i<j}|A_i\cap A_j| - \sum_{i<j<k}|A_i\cap A_j\cap A_k| + \ldots$$

called inclusion-exclusion principle.

PROOF. This is indeed quite clear, by thinking a bit, as follows:

(1) In order to count $(\cup_i A_i)^c$, we certainly have to start with $|A|$.

(2) Then, we obviously have to remove each $|A_i|$, and so remove $\sum_i |A_i|$.

(3) But then, we have to put back each $|A_i \cap A_j|$, and so put back $\sum_{i<j} |A_i \cap A_j|$.

(4) Then, we must remove each $|A_i \cap A_j \cap A_k|$, so remove $\sum_{i<j<k} |A_i \cap A_j \cap A_k|$.

$\vdots$

(5) And so on, which leads to the formula in the statement. □

Now back to the derangements, we have the following key result:

THEOREM 2.17. *The probability for a random permutation $\sigma \in S_N$ to be a derangement is given by the following formula:*

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

Thus we have the following asymptotic formula, in the $N \to \infty$ limit,

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

where $e = 2.7182\ldots$ is the usual constant from analysis.

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:

$$S_N^{i_1\ldots i_k} = \left\{\sigma \in S_N \middle| \sigma(i_1) = i_1, \ldots, \sigma(i_k) = i_k\right\}$$

The inclusion-exclusion principle tells us that we have:

$$\begin{aligned}
& |X_N| \\
= \ & |S_N| - \sum_i |S_N^i| + \sum_{i<j} |S_N^i \cap S_N^j| - \ldots + (-1)^N \sum_{i_1<\ldots<i_N} |S_N^{i_1} \cup \ldots \cup S_N^{i_N}| \\
= \ & |S_N| - \sum_i |S_N^i| + \sum_{i<j} |S_N^{ij}| - \ldots + (-1)^N \sum_{i_1<\ldots<i_N} |S_N^{i_1\ldots i_N}|
\end{aligned}$$

Thus, the probability that we are interested in is given by:

$$\begin{aligned}
P &= \frac{1}{N!}\left(|S_N| - \sum_i |S_N^i| + \sum_{i<j} |S_N^{ij}| - \ldots + (-1)^N \sum_{i_1<\ldots<i_N} |S_N^{i_1\ldots i_N}|\right) \\
&= \frac{1}{N!}\sum_{k=0}^{N}(-1)^k \sum_{i_1<\ldots<i_k} |S_N^{i_1\ldots i_k}| \\
&= \frac{1}{N!}\sum_{k=0}^{N}(-1)^k \sum_{i_1<\ldots<i_k} (N-k)! \\
&= \frac{1}{N!}\sum_{k=0}^{N}(-1)^k \binom{N}{k}(N-k)! \\
&= \sum_{k=0}^{N}\frac{(-1)^k}{k!} \\
&= 1 - \frac{1}{1!} + \frac{1}{2!} - \ldots + (-1)^{N-1}\frac{1}{(N-1)!} + (-1)^N\frac{1}{N!}
\end{aligned}$$

Since at the end we have the standard expansion of $\frac{1}{e}$, we obtain the result. □

More generally now, we have the following result, improving the above:

THEOREM 2.18. *The probability for a random permutation $\sigma \in S_N$ to have exactly k fixed points, with $k \in \mathbb{N}$, is given by the following formula:*

$$P = \frac{1}{k!}\left(1 - \frac{1}{1!} + \frac{1}{2!} - \ldots + (-1)^{N-1}\frac{1}{(N-1)!} + (-1)^N\frac{1}{N!}\right)$$

Thus we have the following approximation formula,

$$P \simeq \frac{1}{ek!}$$

in the $N \to \infty$ limit.

PROOF. We already know, from Theorem 2.17, that this formula holds at $k = 0$. In the general case now, we have to count the permutations $\sigma \in S_N$ having exactly k points.

Since having such a permutation amounts in choosing k points among $1,\ldots,N$, and then permuting the $N-k$ points left, without fixed points allowed, we have:

$$\begin{aligned}\#\left\{\sigma\in S_N\Big|\chi(\sigma)=k\right\} &= \binom{N}{k}\#\left\{\sigma\in S_{N-k}\Big|\chi(\sigma)=0\right\}\\ &= \frac{N!}{k!(N-k)!}\#\left\{\sigma\in S_{N-k}\Big|\chi(\sigma)=0\right\}\\ &= N!\times\frac{1}{k!}\times\frac{\#\left\{\sigma\in S_{N-k}\Big|\chi(\sigma)=0\right\}}{(N-k)!}\end{aligned}$$

Now by dividing everything by $N!$, we obtain from this the following formula:

$$\frac{\#\left\{\sigma\in S_N\Big|\chi(\sigma)=k\right\}}{N!}=\frac{1}{k!}\times\frac{\#\left\{\sigma\in S_{N-k}\Big|\chi(\sigma)=0\right\}}{(N-k)!}$$

By using now the computation at $k=0$, that we already have, from Theorem 2.17, it follows that with $N\to\infty$ we have the following estimate:

$$\begin{aligned}P(\chi=k) &\simeq \frac{1}{k!}\cdot P(\chi=0)\\ &\simeq \frac{1}{k!}\cdot\frac{1}{e}\end{aligned}$$

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

In order to interpret what we found, let us recall the following key definition:

DEFINITION 2.19. *The Poisson law of parameter* 1 *is the following measure,*

$$p_1=\frac{1}{e}\sum_{k\geq 0}\frac{\delta_k}{k!}$$

and the Poisson law of parameter $t>0$ *is the following measure,*

$$p_t=e^{-t}\sum_{k\geq 0}\frac{t^k}{k!}\,\delta_k$$

with the letter "p" standing for Poisson.

We are using here some simplified notations for these laws. Observe that our laws have indeed mass 1, as they should, due to the following key formula:

$$e^t=\sum_{k\geq 0}\frac{t^k}{k!}$$

These laws appear a bit everywhere, in the discrete context, the reasons for this coming from the Poisson Limit Theorem (PLT). In relation with permutations, we have:

THEOREM 2.20. *The number of fixed points, viewed as random variable,*

$$\chi : S_N \to \mathbb{N}$$

follows the Poisson law p_1, in the $N \to \infty$ limit.

PROOF. This is indeed a fancy reformulation of what we found in Theorem 2.18, by using the probabilistic notions from Definition 2.19. □

As a natural question now, that you might have, can we recover as well the parametric Poisson laws, p_t with $t > 0$, via permutations? In answer, yes, the result being:

THEOREM 2.21. *Given a number $t \in (0, 1]$, the number of fixed points of permutations $\sigma \in S_N$ among $\{1, \ldots, [tN]\}$, viewed as random variable*

$$\chi_t : S_N \to \mathbb{N}$$

follows the Poisson law p_t, in the $N \to \infty$ limit.

PROOF. As before in the proof of Theorem 2.17, we get by inclusion-exclusion:

$$\begin{aligned} P(\chi_t = 0) &= \frac{1}{N!}\sum_{r=0}^{[tN]}(-1)^r \sum_{k_1<\ldots<k_r<[tN]} |S_N^{k_1} \cap \ldots \cap S_N^{k_r}| \\ &= \frac{1}{N!}\sum_{r=0}^{[tN]}(-1)^r \binom{[tN]}{r}(N-r)! \\ &= \sum_{r=0}^{[tN]} \frac{(-1)^r}{r!} \cdot \frac{[tN]!(N-r)!}{N!([tN]-r)!} \end{aligned}$$

Now with $N \to \infty$, we obtain from this the following estimate:

$$P(\chi_t = 0) \simeq \sum_{r=0}^{[tN]} \frac{(-1)^r}{r!} \cdot t^r \simeq e^{-t}$$

More generally, by counting the permutations $\sigma \in S_N$ having exactly r fixed points among $1, \ldots, [tN]$, as in the proof of Theorem 2.18, we obtain:

$$P(\chi_t = r) \simeq \frac{t^r}{r!e^t}$$

Thus, we obtain in the limit a Poisson law of parameter t, as stated. □

Many other things can be said, as a continuation of this. We will be back to this, on several occasions, in what follows, and notably in Part III of the present book.

2d. Finite fields

Ready for some spectacular applications of finite group theory, and more specifically, of the symmetric groups? Let us start with the following key definition:

DEFINITION 2.22. *A field is a set F with a sum operation $+$ and a product operation $\times$, subject to the following conditions:*

(1) *$a+b=b+a$, $a+(b+c)=(a+b)+c$, there exists $0\in F$ such that $a+0=0$, and any $a\in F$ has an inverse $-a\in F$, satisfying $a+(-a)=0$.*
(2) *$ab=ba$, $a(bc)=(ab)c$, there exists $1\in F$ such that $a1=a$, and any $a\neq 0$ has a multiplicative inverse $a^{-1}\in F$, satisfying $aa^{-1}=1$.*
(3) *The sum and product are compatible via $a(b+c)=ab+ac$.*

Normally the simplest field is $\mathbb{Q}$, but, purely mathematically speaking, this is not exactly true, because, by a strange twist of fate, the numbers $0,1$, whose presence in a field is mandatory, $0,1\in F$, can form themselves a field, with addition as follows:

$$1+1=0$$

To be more precise, according to our field axioms, we certainly must have:

$$0+0=0\times 0=0\times 1=1\times 0=0$$

$$0+1=1+0=1\times 1=1$$

Thus, everything regarding the addition and multiplication of $0,1$ is uniquely determined, except for the value of $1+1$. And here, you would say that we should normally set $1+1=2$, with $2\neq 0$ being a new field element, but the point is that $1+1=0$ is something natural too, this being the addition modulo 2:

$$1+1=0(2)$$

And, what we get in this way is a field, denoted as follows:

$$\mathbb{F}_2=\{0,1\}$$

Let us summarize this finding, along with a bit more, obtained by suitably replacing our 2, used for addition, with an arbitrary prime number p, as follows:

THEOREM 2.23. *Given a field F, define its characteristic $p=char(F)$ as being the smallest $p\in\mathbb{N}$ such that the following happens, and as $p=0$, if this never happens:*

$$\underbrace{1+\ldots+1}_{p\ times}=0$$

Then, assuming $p>0$, this characteristic p must be a prime number, we have a field embedding $\mathbb{F}_p\subset F$, and $q=|F|$ must be of the form $q=p^k$, with $k\in\mathbb{N}$.

PROOF. Very crowded statement that we have here, the idea being as follows:

(1) The fact that $p > 0$ must be prime comes by contradiction, by using:

$$(\underbrace{1 + \ldots + 1}_{a \text{ times}}) \times (\underbrace{1 + \ldots + 1}_{b \text{ times}}) = \underbrace{1 + \ldots + 1}_{ab \text{ times}}$$

Indeed, assuming that we have $p = ab$ with $a, b > 1$, the above formula corresponds to an equality of type $AB = 0$ with $A, B \neq 0$ inside F, which is impossible.

(2) Back to the general case, F has a smallest subfield $E \subset F$, called prime field, consisting of the various sums $1 + \ldots + 1$, and their quotients. In the case $p = 0$ we obviously have $E = \mathbb{Q}$. In the case $p > 0$ now, the multiplication formula in (1) shows that the set $S = \{1 + \ldots + 1\}$ is stable under taking quotients, and so $E = S$.

(3) Now with $E = S$ in hand, we obviously have $(E, +) = \mathbb{Z}_p$, and since the multiplication is given by the formula in (1), we conclude that we have $E = \mathbb{F}_p$, as a field. Thus, in the case $p > 0$, we have constructed an embedding $\mathbb{F}_p \subset F$, as claimed.

(4) In the context of the above embedding $\mathbb{F}_p \subset F$, we can say that F is a vector space over $\mathbb{F}_p$, and so we have $|F| = p^k$, with $k \in \mathbb{N}$ being the dimension of this space. □

In order to further advance, in our understanding of the finite fields, let us start with the following key theorem of Fermat, for the usual integers:

THEOREM 2.24. *We have the following congruence, for any prime p,*

$$a^p = a(p)$$

called Fermat's little theorem.

PROOF. The simplest way is to do this by recurrence on $a \in \mathbb{N}$, as follows:

$$\begin{aligned}(a+1)^p &= \sum_{k=0}^{p} \binom{p}{k} a^k \\ &= a^p + 1(p) \\ &= a + 1(p)\end{aligned}$$

Here we have used the fact that all non-trivial binomial coefficients $\binom{p}{k}$ are multiples of p, as shown by a close inspection of these binomial coeffients, given by:

$$\binom{p}{k} = \frac{p(p-1)\ldots(p-k+1)}{k!}$$

Thus, we have the result for any $a \in \mathbb{N}$, and with the case $p = 2$ being trivial, we can assume $p \geq 3$, and here by using $a \to -a$ we get it for any $a \in \mathbb{Z}$, as desired. □

The Fermat theorem is particularly interesting when extended from the integers to the arbitrary field case. In order to discuss this question, let us start with:

PROPOSITION 2.25. *In a field F of characteristic $p > 0$ we have*

$$(a+b)^p = a^p + b^p$$

for any two elements $a, b \in F$.

PROOF. We have indeed the computation, exactly as in the proof of Fermat, by using the fact that the non-trivial binomial coefficients are all multiples of p:

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = a^p + b^p$$

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

Observe that we can iterate the Fermat formula, and we obtain $(a+b)^r = a^r + b^r$ for any power $r = p^s$. In particular we have, with $q = |F|$, the following formula:

$$(a+b)^q = a^q + b^q$$

But this is something quite interesting, showing that the following subset of F, which is closed under multiplication, is closed under addition too, and so is a subfield:

$$E = \left\{ a \in F \middle| a^q = a \right\}$$

So, what is this subfield $E \subset F$? In the lack of examples, or general theory for subfields $E \subset F$, we are a bit in the dark here, but it seems quite reasonable to conjecture that we have $E = F$. Thus, our conjecture would be that we have the following formula, for any $a \in F$, and with this being the field extension of the Fermat theorem itself:

$$a^q = a$$

Now that we have our conjecture, let us think at a potential proof. And here, by looking at the proof of the Fermat theorem, the recurrence method from there, based on $a \to a+1$, cannot work as such, and must be suitably fine-tuned.

Thinking a bit, the recurrence from the proof of Fermat somehow rests on the fact that the additive group $\mathbb{Z}$ is singly generated, by $1 \in \mathbb{Z}$. Thus, we need some sort of field extension of this single generation result, and in the lack of something additive here, the following theorem, which is something multiplicative, comes to the rescue:

THEOREM 2.26. *Given a field F, any finite subgroup of its multiplicative group*

$$G \subset F - \{0\}$$

must be cyclic.

PROOF. This can be done via some standard arithmetics, as follows:

(1) Let us pick an element $g \in G$ of highest order, $n = ord(g)$. Our claim, which will easily prove the result, is that the order $m = ord(h)$ of any $h \in G$ satisfies $m|n$.

(2) In order to prove this claim, let $d = (m, n)$, write $d = am + bn$ with $a, b \in \mathbb{Z}$, and set $k = g^a h^b$. We have then the following computations:

$$k^m = g^{am} h^{bm} = g^{am} = g^{d-bn} = g^d$$

$$k^n = g^{an} h^{bn} = h^{bn} = h^{d-am} = h^d$$

By using either of these formulae, say the first one, we obtain:

$$k^{[m,n]} = k^{mn/d} = (k^m)^{n/d} = (g^d)^{n/d} = g^n = 1$$

Thus $ord(k)|[m, n]$, and our claim is that we have in fact $ord(k) = [m, n]$.

(3) In order to prove this latter claim, assume first that we are in the case $d = 1$. But here the result is clear, because the formulae in (2) read $g = k^m, h = g^n$, and since $n = ord(g), m = ord(g)$ are prime to each other, we conclude that we have $ord(k) = mn$, as desired. As for the general case, where d is arbitrary, this follows from this.

(4) Summarizing, we have proved our claim in (2). Now since the order $n = ord(g)$ was assumed to be maximal, we must have $[m, n]|n$, and so $m|n$. Thus, we have proved our claim in (1), namely that the order $m = ord(h)$ of any $h \in G$ satisfies $m|n$.

(5) But with this claim in hand, the result follows. Indeed, since the polynomial $x^n - 1$ has all the elements $h \in G$ as roots, its degree must satisfy $n \geq |G|$. On the other hand, from $n = ord(g)$ with $g \in G$, we have $n||G|$. We therefore conclude that we have $n = |G|$, which shows that G is indeed cyclic, generated by the element $g \in G$. □

We can now extend the Fermat theorem to the finite fields, as follows:

THEOREM 2.27. *Given a finite field F, with $q = |F|$ we have*

$$a^q = a$$

for any $a \in F$.

PROOF. According to Theorem 2.26 the multiplicative group $F - \{0\}$ is cyclic, of order $q - 1$. Thus, the following formula is satisfied, for any $a \in F - \{0\}$:

$$a^{q-1} = 1$$

Now by multiplying by a, we are led to the conclusion in the statement, with of course the remark that the formula there trivially holds for $a = 0$. □

The Fermat polynomial $X^p - X$ is something very useful, and its field generalization $X^q - X$, with $q = p^k$ prime power, can be used in order to elucidate the structure of finite fields. In order to discuss this question, let us start with a basic fact, as follows:

PROPOSITION 2.28. *Given a finite field F, we have*

$$X^q - X = \prod_{a \in F} (X - a)$$

with $q = |F|$.

PROOF. We know from the Fermat theorem above that we have $a^q = a$, for any $a \in F$. We conclude from this that all the elements $a \in F$ are roots of the polynomial $X^q - X$, and so this polynomial must factorize as in the statement. □

The continuation of the story is more complicated. We first have:

THEOREM 2.29. *Given a field extension $E \subset F$, we can talk about its Galois group G, as the group of automorphisms of F fixing E. The intermediate fields*

$$E \subset K \subset F$$

are then in correspondence with the subgroups $H \subset G$, with such a field K corresponding to the subgroup H consisting of automorphisms $g \in G$ fixing K.

PROOF. This is something self-explanatory, and follows indeed from some algebra, under suitable assumptions, in order for that algebra to properly apply. □

Getting now towards polynomials and their roots, we have here:

THEOREM 2.30. *Given a field F and a polynomial $P \in F[X]$, we can talk about the abstract splitting field of P, where this polynomial decomposes as:*

$$P(X) = c\prod_i (X - a_i)$$

In particular, any field F has a certain algebraic closure $\bar{F}$, where all the polynomials $P \in F[X]$, and in fact all polynomials $P \in \bar{F}[X]$ too, have roots.

PROOF. This is again something self-explanatory, which follows from Theorem 2.29 and from some extra algebra, under suitable assumptions, in order for that extra algebra to properly apply. Regarding the construction at the end, as main example here we have $\bar{\mathbb{R}} = \mathbb{C}$. However, as an interesting fact, $\bar{\mathbb{Q}} \subset \mathbb{C}$ is a proper subfield. □

Good news, with this in hand, we can now elucidate the structure of finite fields:

THEOREM 2.31. *For any prime power $q = p^k$ there is a unique field $\mathbb{F}_q$ having q elements. At $k = 1$ this is the usual $\mathbb{F}_p$. In general, this is the splitting field of:*

$$P = X^q - X$$

Moreover, we can construct an explicit model for $\mathbb{F}_q$, at $q = p^2$ or higher, as

$$\mathbb{F}_q = \mathbb{F}_p[X]/(Q)$$

with $Q \in \mathbb{F}_p[X]$ being a suitable irreducible polynomial, of degree k.

PROOF. There are several assertions here, the idea being as follows:

(1) The first assertion, regarding the existence and uniqueness of $\mathbb{F}_q$, follows from Theorem 2.27 and Theorem 2.30. Indeed, we know from Theorem 2.27 that given a finite field, $|F| = q$ with $k \in \mathbb{N}$, the Fermat polynomial $P = X^q - X$ factorizes as follows:

$$X^q - X = \prod_{a \in F} (X - a)$$

But this shows, via the general theory from Theorem 2.30, that our field F must be the splitting field of P, and so is unique. As for the existence, this follows again from Theorem 2.30, telling us that the splitting field always exists.

(2) In what regards now the modeling of $\mathbb{F}_q$, at $q = p$ there is nothing to do, because we have our usual $\mathbb{F}_p$ here. At $q = p^2$ and higher, by standard commutative algebra we have an isomorphism as follows, whenever $Q \in \mathbb{F}_p[X]$ is taken irreducible:

$$\mathbb{F}_q = \mathbb{F}_p[X]/(Q)$$

(3) Regarding now the best choice of the irreducible polynomial $Q \in \mathbb{F}_p[X]$, providing us with a good model for the finite field $\mathbb{F}_q$, that we can use in practice, this question depends on the value of $q = p^k$, and many things can be said here. All in all, our models are quite similar to $\mathbb{C} = \mathbb{R}[i]$, with i being a formal number satisfying $i^2 = -1$.

(4) To be more precise, at the simplest exponent, $q = 4$, to start with, we can use $Q = X^2 + X + 1$, with this being actually the unique possible choice of a degree 2 irreducible polynomial $Q \in \mathbb{F}_2[X]$, and this leads to a model as follows:

$$\mathbb{F}_4 = \left\{ 0, 1, a, a + 1 \,\middle|\, a^2 = a + 1 \right\}$$

To be more precise here, we assume of course that the characteristic of our model is $p = 2$, which reads $x + x = 0$ for any x, and so determines the addition table. As for the multiplication table, this is uniquely determined by $a^2 = -a - 1 = a + 1$.

(5) Next, at exponents of type $q = p^2$ with $p \geq 3$ prime, we can use $Q = X^2 - r$, with r being a non-square modulo p, and with $(p - 1)/2$ choices here. We are led to:

$$\mathbb{F}_{p^2} = \left\{ a + b\gamma \,\middle|\, \gamma^2 = r \right\}$$

Here, as before with $\mathbb{F}_4$, our formula is something self-explanatory. Observe the analogy with $\mathbb{C} = \mathbb{R}[i]$, with i being a formal number satisfying $i^2 = -1$.

(6) Finally, at $q = p^k$ with $k \geq 3$ things become more complicated, but the main idea remains the same. We have for instance models for $\mathbb{F}_8$, $\mathbb{F}_{27}$ using $Q = X^3 - X - 1$, and a model for $\mathbb{F}_{16}$ using $Q = X^4 + X + 1$. Many other things can be said here. □

As another application of the above, which motivated Galois, we have:

THEOREM 2.32. *Unlike in degree $N \leq 4$, there is no formula for the roots of polynomials of degree $N = 5$ and higher, with the reason for this, coming from Galois theory, being that S_5 is not solvable. The simplest numeric example is $P = X^5 - X - 1$.*

PROOF. This is something quite tricky, the idea being as follows:

(1) The first assertion, for generic polynomials, is due to Abel-Ruffini, but Galois theory helps in better understanding this, and comes with a number of bonus points too, namely the possibility of formulating a finer result, with Abel-Ruffini's original "generic", which was something algebraic, being now replaced by an analytic "generic", and also with the possibility of dealing with concrete polynomials, such as $P = X^5 - X - 1$.

(2) Regarding now the details of the Galois proof of the Abel-Ruffini theorem, assume that the roots of a polynomial $P \in F[X]$ can be computed by using iterated roots, a bit as for the degree 2 equation, or for the degree 3 and 4 equations, via Cardano. Then, algebrically speaking, this gives rise to a tower of fields as folows, with $F_0 = F$, and each F_{i+1} being obtained from F_i by adding a root, $F_{i+1} = F_i(x_i)$, with $x_i^{n_i} \in F_i$:

$$F_0 \subset F_1 \subset \ldots \subset F_k$$

(3) In order for Galois theory to apply well to this situation, we must make all the extensions normal, which amounts in replacing each $F_{i+1} = F_i(x_i)$ by its extension $K_i(x_i)$, with K_i extending F_i by adding a n_i-th root of unity. Thus, with this replacement, we can assume that the tower in (2) in normal, meaning that all Galois groups are cyclic.

(4) Now by Galois theory, at the level of the corresponding Galois groups we obtain a tower of groups as follows as follows, which is a resolution of the last group G_k, the Galois group of P, in the sense of group theory, in the sense that all quotients are cyclic:

$$G_1 \subset G_2 \subset \ldots \subset G_k$$

As a conclusion, Galois theory tells us that if the roots of a polynomial $P \in F[X]$ can be computed by using iterated roots, then its Galois group $G = G_k$ must be solvable.

(5) In the generic case, the conclusion is that Galois theory tells us that, in order for all polynomials of degree 5 to be solvable, via square roots, the group S_5, which appears there as Galois group, must be solvable, in the sense of group theory. But this is wrong, because the alternating subgroup $A_5 \subset S_5$ is simple, and therefore not solvable.

(6) Finally, regarding the polynomial $P = X^5 - X - 1$, some elementary computations here, based on arithmetic over $\mathbb{F}_2, \mathbb{F}_3$, and involving various cycles of length $2, 3, 5$, show that its Galois group is S_5. Thus, we have our counterexample.

(7) To be more precise, our polynomial factorizes over $\mathbb{F}_2$ as follows:

$$X^5 - X - 1 = (X^2 + X + 1)(X^3 + X^2 + 1)$$

We deduce from this the existence of an element $\tau\sigma \in G \subset S_5$, with $\tau \in S_5$ being a transposition, and with $\sigma \in S_5$ being a 3-cycle, disjoint from it. Thus, we have:

$$\tau = (\tau\sigma)^3 \in G$$

(8) On the other hand since $P = X^5 - X - 1$ is irreducible over $\mathbb{F}_5$, we have as well available a certain 5-cycle $\rho \in G$. Now since $< \tau, \rho >= S_5$, we conclude that the Galois group of P is full, $G = S_5$, and by (4) and (5) we have our counterexample.

(9) Finally, as mentioned in (1), all this shows as well that a random polynomial of degree 5 or higher is not solvable by square roots, and with this being an elementary consequence of the main result from (5), via some standard analysis arguments. □

2e. Exercises

Exercises:

Exercise 2.33.

Exercise 2.34.

Exercise 2.35.

Exercise 2.36.

Exercise 2.37.

Exercise 2.38.

Exercise 2.39.

Exercise 2.40.

Bonus exercise.

CHAPTER 3

Reflection groups

3a. Product operations

We discuss in this chapter more complicated symmetry groups. As a starting point here, we have the following result regarding the dihedral group D_N, from chapter 1:

THEOREM 3.1. *The dihedral group D_N is the group having $2N$ elements, $R_1, \ldots, R_N$ and $S_1, \ldots, S_N$, called rotations and symmetries, which multiply as follows,*

$$R_k R_l = R_{k+l}$$
$$R_k S_l = S_{k+l}$$
$$S_k R_l = S_{k-l}$$
$$S_k S_l = R_{k-l}$$

with all the indices being taken modulo N.

PROOF. This is something that we know well from chapter 1, and we refer to the material there for full explanations on this result, and for more about it. □

Observe now that D_N has the same cardinality as $E_N = \mathbb{Z}_N \times \mathbb{Z}_2$. We obviously don't have $D_N \simeq E_N$, because D_N is not abelian, while E_N is. So, our next goal will be that of proving that D_N appears by "twisting" E_N. In order to do this, let us start with:

PROPOSITION 3.2. *The group $E_N = \mathbb{Z}_N \times \mathbb{Z}_2$ is the group having $2N$ elements, $r_1, \ldots, r_N$ and $s_1, \ldots, s_N$, which multiply according to the following rules,*

$$r_k r_l = r_{k+l}$$
$$r_k s_l = s_{k+l}$$
$$s_k r_l = s_{k+l}$$
$$s_k s_l = r_{k+l}$$

with all the indices being taken modulo N.

PROOF. With the notation $\mathbb{Z}_2 = \{1, \tau\}$, the elements of the product group $E_N = \mathbb{Z}_N \times \mathbb{Z}_2$ can be labeled $r_1, \ldots, r_N$ and $s_1, \ldots, s_N$, as follows:

$$r_k = (k, 1) \quad , \quad s_k = (k, \tau)$$

These elements multiply then according to the formulae in the statement. Now since a group is uniquely determined by its multiplication rules, this gives the result. □

Let us compare now Theorem 3.1 and Proposition 3.2. In order to formally obtain D_N from E_N, we must twist some of the multiplication rules of E_N, namely:

$$s_k r_l = s_{k+l} \to s_{k-l}$$

$$s_k s_l = r_{k+l} \to r_{k-l}$$

Informally, this amounts in following the rule "τ switches the sign of what comes afterwards", and we are led in this way to the following definition:

DEFINITION 3.3. *Given two groups A, G, with an action $A \curvearrowright G$, the crossed product*

$$P = G \rtimes A$$

is the set $G \times A$, with multiplication $(g, a)(h, b) = (gh^a, ab)$.

It is routine to check that P is indeed a group. Observe that when the action is trivial, $h^a = h$ for any $a \in A$ and $h \in H$, we obtain the usual product $G \times A$.

Now with this technology in hand, by getting back to the dihedral group D_N, we can improve Theorem 3.1, into a final result on the subject, as follows:

THEOREM 3.4. *We have a crossed product decomposition as follows,*

$$D_N = \mathbb{Z}_N \rtimes \mathbb{Z}_2$$

with $\mathbb{Z}_2 = \{1, \tau\}$ acting on $\mathbb{Z}_N$ via switching signs, $k^\tau = -k$.

PROOF. We have an action $\mathbb{Z}_2 \curvearrowright \mathbb{Z}_N$ given by the formula in the statement, namely $k^\tau = -k$, so we can consider the corresponding crossed product group:

$$P_N = \mathbb{Z}_N \rtimes \mathbb{Z}_2$$

In order to understand the structure of P_N, we follow Proposition 3.2. The elements of P_N can indeed be labeled $\rho_1, \ldots, \rho_N$ and $\sigma_1, \ldots, \sigma_N$, as follows:

$$\rho_k = (k, 1) \quad , \quad \sigma_k = (k, \tau)$$

Now when computing the products of such elements, we basically obtain the formulae in Proposition 3.2, perturbed as in Definition 3.3. To be more precise, we have:

$$\rho_k \rho_l = \rho_{k+l}$$

$$\rho_k \sigma_l = \sigma_{k+l}$$

$$\sigma_k \rho_l = \sigma_{k+l}$$

$$\sigma_k \sigma_l = \rho_{k+l}$$

But these are exactly the multiplication formulae for D_N, from Theorem 3.1. Thus, we have an isomorphism $D_N \simeq P_N$ given by $R_k \to \rho_k$ and $S_k \to \sigma_k$, as desired. □

More generally now, for the transitive graphs, that we are mostly interested in, the point is that at very small values of the order, $N = 2, \ldots, 9$, these always decompose as products, via three main types of graph products, constructed as follows:

DEFINITION 3.5. *Given two finite graphs X, Y, we can construct:*

(1) *The direct product $X \times Y$ has vertex set $X \times Y$, and edges:*

$$(i, \alpha) - (j, \beta) \iff i - j,\ \alpha - \beta$$

(2) *The Cartesian product $X \square Y$ has vertex set $X \times Y$, and edges:*

$$(i, \alpha) - (j, \beta) \iff i = j,\ \alpha - \beta \text{ or } i - j, \alpha = \beta$$

(3) *The lexicographic product $X \circ Y$ has vertex set $X \times Y$, and edges:*

$$(i, \alpha) - (j, \beta) \iff \alpha - \beta \text{ or } \alpha = \beta,\ i - j$$

We call these three products the standard products of graphs.

Several comments can be made here. First, the direct product $X \times Y$ is the usual one in a categorical sense, and we will leave clarifying this observation as an exercise. The Cartesian product $X \square Y$ is quite natural too from a geometric perspective, for instance because a product by a segment gives a prism. As for the lexicographic product $X \circ Y$, this is something interesting too, obtained by putting a copy of X at each vertex of Y.

At the level of symmetry groups, several things can be said, and we first have:

THEOREM 3.6. *We have group embeddings as follows, for any graphs X, Y,*

$$G(X) \times G(Y) \subset G(X \times Y)$$

$$G(X) \times G(Y) \subset G(X \square Y)$$

$$G(X) \wr G(Y) \subset G(X \circ Y)$$

but these embeddings are not always isomorphisms.

PROOF. The fact that we have indeed embeddings as above is clear from definitions. As for the counterexamples, in each case, these are easy to construct as well, provided by our study of small graphs, at $N = 2, \ldots, 11$, and we will leave this as an exercise. □

The problem now is that of deciding when the embeddings in Theorem 3.6 are isomorphisms. In order to discusss this, we first have the following basic fact:

THEOREM 3.7. *Given a subgroup $G \subset S_N$, regarded as matrix group via*

$$G \subset S_N \subset O_N$$

the standard coordinates of the group elements, $u_{ij}(g) = g_{ij}$, are given by:

$$u_{ij} = \chi\left(\sigma \in G \middle| \sigma(j) = i\right)$$

Moreover, these functions $u_{ij} : G \to \mathbb{C}$ generate the algebra $C(G)$.

PROOF. Here the first assertion comes from the fact that the entries of the permutation matrices $\sigma \in S_N \subset O_N$, acting as $\sigma(e_i) = e_{\sigma(i)}$, are given by the following formula:

$$\sigma_{ij} = \begin{cases} 1 & \text{if } \sigma(j) = i \\ 0 & \text{otherwise} \end{cases}$$

As for the second assertion, this comes from the Stone-Weierstrass theorem, because the coordinate functions $u_{ij} : G \to \mathbb{C}$ obviously separate the group elements $\sigma \in G$. □

We are led in this way to the following definition:

DEFINITION 3.8. *The magic matrix associated to a permutation group $G \subset S_N$ is the $N \times N$ matrix of characteristic functions*

$$u_{ij} = \chi\left(\sigma \in G \middle| \sigma(j) = i\right)$$

with the name "magic" coming from the fact that, on each row and each column, these characteristic functions sum up to 1.

The interest in this notion comes from the fact, that we know from Theorem 3.7, that the entries of the magic matrix generate the algebra of functions on our group:

$$C(G) =< u_{ij} >$$

We will talk more in detail later about such matrices, and their correspondence with the subgroups $G \subset S_N$, and what can be done with it, in the general framework of representation theory. However, for making our point, here is the general principle:

PRINCIPLE 3.9. *Everything that you can do with your group $G \subset S_N$ can be expressed in terms of the magic matrix $u = (u_{ij})$, quite often with good results.*

This principle comes from the above Stone-Weierstrass result, $C(G) =< u_{ij} >$. Indeed, when coupled with some basic spectral theory, and more specifically with the Gelfand theorem from operator algebras, this result tells us that our group G appears as the spectrum of the algebra $< u_{ij} >$, therefore leading to the above principle.

As an illustration for all this, in relation with the graphs, we have:

THEOREM 3.10. *Given a subgroup $G \subset S_N$, the transpose of its action map $X \times G \to X$ on the set $X = \{1, \ldots, N\}$, given by $(i, \sigma) \to \sigma(i)$, is given by:*

$$\Phi(e_i) = \sum_j e_j \otimes u_{ji}$$

Also, in the case where we have a graph with N vertices, the action of G on the vertex set X leaves invariant the edges precisely when we have

$$du = ud$$

with d being as usual the adjacency matrix of the graph.

PROOF. There are several things going on here, the idea being as follows:

(1) Given a subgroup $G \subset S_N$, if we set $X = \{1, \ldots, N\}$, we have indeed an action map as follows, and with the reasons of using $X \times G$ instead of the perhaps more familiar $G \times X$ being dictated by some quantum algebra, that we will do later in this book:

$$a : X \times G \to X \quad , \quad a(i, \sigma) = \sigma(i)$$

(2) Now by transposing this map, we obtain a morphism of algebras, as follows:

$$\Phi : C(X) \to C(X) \otimes C(G) \quad , \quad \Phi(f)(i, \sigma) = f(\sigma(i))$$

When evaluated on the Dirac masses, this map Φ is then given by:

$$\Phi(e_i)(j, \sigma) = e_i(\sigma(j)) = \delta_{\sigma(j)i}$$

Thus, in tensor product notation, we have the following formula, as desired:

$$\Phi(e_i)(j, \sigma) = \left(\sum_j e_j \otimes u_{ji} \right)(j, \sigma)$$

(3) Regarding now the second assertion, observe first that we have:

$$(du)_{ij}(\sigma) = \sum_k d_{ik} u_{kj}(\sigma) = \sum_k d_{ik} \delta_{\sigma(j)k} = d_{i\sigma(j)}$$

On the other hand, we have as well the following formula:

$$(ud)_{ij}(\sigma) = \sum_k u_{ik}(\sigma) d_{kj} = \sum_k \delta_{\sigma(k)i} d_{kj} = d_{\sigma^{-1}(i)j}$$

Thus $du = ud$ reformulates as $d_{ij} = d_{\sigma(i)\sigma(j)}$, which gives the result. □

Back to graphs, we want to know when the embeddings in Theorem 3.6 are isomorphisms. In what regards the first two products, we have here the following result:

THEOREM 3.11. *Let X and Y be finite connected regular graphs. If their spectra $\{\lambda\}$ and $\{\mu\}$ do not contain 0 and satisfy*

$$\{\lambda_i / \lambda_j\} \cap \{\mu_k / \mu_l\} = \{1\}$$

then $G(X \times Y) = G(X) \times G(Y)$. Also, if their spectra satisfy

$$\{\lambda_i - \lambda_j\} \cap \{\mu_k - \mu_l\} = \{0\}$$

then $G(X \square Y) = G(X) \times G(Y)$.

PROOF. This is something quite standard, the idea being as follows:

(1) First, we know from Theorem 3.6 that we have embeddings as follows, valid for any two graphs X, Y, and coming from definitions:

$$G(X) \times G(Y) \subset G(X \times Y)$$

$$G(X) \times G(Y) \subset G(X \square Y)$$

(2) Now let λ_1 be the valence of X. Since X is regular we have $\lambda_1 \in Sp(X)$, with 1 as eigenvector, and since X is connected λ_1 has multiplicity 1. Thus if P_1 is the orthogonal projection onto $\mathbb{C}1$, the spectral decomposition of d_X is of the following form:

$$d_X = \lambda_1 P_1 + \sum_{i \neq 1} \lambda_i P_i$$

We have a similar formula for the adjacency matrix d_Y, namely:

$$d_Y = \mu_1 Q_1 + \sum_{j \neq 1} \mu_j Q_j$$

(3) But this gives the following formulae for the graph products:

$$d_{X \times Y} = \sum_{ij} (\lambda_i \mu_j) P_i \otimes Q_j$$

$$d_{X \,\square\, Y} = \sum_{ij} (\lambda_i + \mu_i) P_i \otimes Q_j$$

Here the projections form partitions of unity, and the scalar are distinct, so these are spectral decompositions. The coactions will commute with any of the spectral projections, and so with both $P_1 \otimes 1$, $1 \otimes Q_1$. In both cases the universal coaction v is the tensor product of its restrictions to the images of $P_1 \otimes 1$, $1 \otimes Q_1$, which gives the result. □

Regarding now the lexicographic product, things here are more tricky. Let us first recall that the lexicographic product of two graphs $X \circ Y$ is obtained by putting a copy of X at each vertex of Y, the formula for the edges being as follows:

$$(i, \alpha) - (j, \beta) \iff \alpha - \beta \text{ or } \alpha = \beta,\ i - j$$

In what regards now the computation of the symmetry group, as before we must do here some spectral theory, and we are led in this way to the following result:

THEOREM 3.12. *Let X, Y be regular graphs, with X connected. If their spectra $\{\lambda_i\}$ and $\{\mu_j\}$ satisfy the condition*

$$\big\{\lambda_1 - \lambda_i \big| i \neq 1\big\} \cap \big\{ -n\mu_j \big\} = \emptyset$$

where n and λ_1 are the order and valence of X, then $G(X \circ Y) = G(X) \wr G(Y)$.

PROOF. This is something quite tricky, the idea being as follows:

(1) First, we know from Theorem 3.6 that we have an embedding as follows, valid for any two graphs X, Y, and coming from definitions:

$$G(X) \wr G(Y) \subset G(X \circ Y)$$

(2) We denote by P_i, Q_j the spectral projections corresponding to λ_i, μ_j. Since X is connected we have $P_1 = \mathbb{I}/n$, and we obtain:

$$\begin{aligned} d_{X\circ Y} &= d_X \otimes 1 + \mathbb{I} \otimes d_Y \\ &= \left(\sum_i \lambda_i P_i\right) \otimes \left(\sum_j Q_j\right) + (nP_1) \otimes \left(\sum_i \mu_j Q_j\right) \\ &= \sum_j (\lambda_1 + n\mu_j)(P_1 \otimes Q_j) + \sum_{i\neq 1} \lambda_i (P_i \otimes 1) \end{aligned}$$

In this formula the projections form a partition of unity and the scalars are distinct, so this is the spectral decomposition of $d_{X\circ Y}$.

(3) Now let W be the universal magic matrix for $X \circ Y$. Then W must commute with all spectral projections, and in particular:

$$[W, P_1 \otimes Q_j] = 0$$

Summing over j gives $[W, P_1 \otimes 1] = 0$, so $1 \otimes C(Y)$ is invariant under the coaction. So, consider the restriction of W, which gives a coaction of $G(X \circ Y)$ on $1 \otimes C(Y)$, that we can denote as follows, with y being a certain magic unitary:

$$W(1 \otimes e_a) = \sum_b 1 \otimes e_b \otimes y_{ba}$$

(4) On the other hand, according to our definition of W, we can write:

$$W(e_i \otimes 1) = \sum_{jb} e_j \otimes e_b \otimes x^b_{ji}$$

By multiplying by the previous relation, found in (3), we obtain:

$$\begin{aligned} W(e_i \otimes e_a) &= \sum_{jb} e_j \otimes e_b \otimes y_{ba} x^b_{ji} \\ &= \sum_{jb} e_j \otimes e_b \otimes x^b_{ji} y_{ba} \end{aligned}$$

But this shows that the coefficients of W are of the following form:

$$W_{jb,ia} = y_{ba} x^b_{ji} = x^b_{ji} y_{ba}$$

(5) In order to advance, consider now the following matrix:

$$x^b = (x^b_{ij})$$

Since the map W above is a morphism of algebras, each row of x^b is a partition of unity. Also, by using the antipode map S, which is transpose to $g \to g^{-1}$, we have:

$$\begin{aligned} S\left(\sum_j x_{ji}^b\right) &= S\left(\sum_{ja} x_{ji}^b y_{ba}\right) \\ &= S\left(\sum_{ja} W_{jb,ia}\right) \\ &= \sum_{ja} W_{ia,jb} \\ &= \sum_{ja} x_{ij}^a y_{ab} \\ &= \sum_a y_{ab} \\ &= 1 \end{aligned}$$

(6) We check now that both x^a, y commute with d_X, d_Y. We have:

$$(d_{X\circ Y})_{ia,jb} = (d_X)_{ij}\delta_{ab} + (d_Y)_{ab}$$

Thus the two products between W and $d_{X\circ Y}$ are given by:

$$(Wd_{X\circ Y})_{ia,kc} = \sum_j W_{ia,jc}(d_X)_{jk} + \sum_{jb} W_{ia,jb}(d_Y)_{bc}$$

$$(d_{X\circ Y}W)_{ia,kc} = \sum_j (d_X)_{ij}W_{ja,kc} + \sum_{jb}(d_Y)_{ab}W_{jb,kc}$$

(7) Now since the magic matrix W commutes by definition with $d_{X\circ Y}$, the terms on the right in the above equations are equal, and by summing over c we get:

$$\sum_j x_{ij}^a(d_X)_{jk} + \sum_{cb} y_{ab}(d_Y)_{bc} = \sum_j (d_X)_{ij}x_{jk}^a + \sum_{cb}(d_Y)_{ab}y_{bc}$$

The second sums in both terms are equal to the valence of Y, so we get $[x^a, d_X] = 0$. Now once again from the formula coming from $[W, d_{X\circ Y}] = 0$, we get:

$$[y, d_Y] = 0$$

(8) Summing up, the coefficients of W are of the following form, where x^b are magic unitaries commuting with d_X, and y is a magic unitary commuting with d_Y:

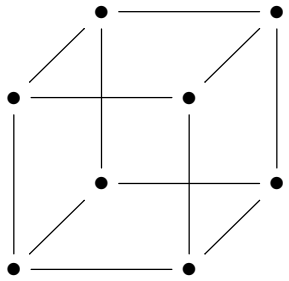
$$W_{jb,ia} = x_{ji}^b y_{ba}$$

But this gives a morphism $C(G(X) \wr G(Y)) \to G(X \circ Y)$ mapping $u_{ji}^{(b)} \to x_{ji}^b$ and $v_{ba} \to y_{ba}$, which is inverse to the morphism in (1), as desired. □

3b. Hyperoctahedral groups

At a more advanced level now, we first have the hyperoctahedral group H_N. This group is something quite tricky, which appears as follows:

DEFINITION 3.13. *The hyperoctahedral group H_N is the group of symmetries of the unit cube in $\mathbb{R}^N$,*



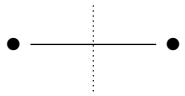
viewed as a graph, or equivalently, as a metric space.

Here the equivalence at the end is clear from definitions, because any symmetry of the cube graph must preserve the lengths of the edges, and so we have:

$$G(\square_{graph}) = G(\square_{metric})$$

The hyperoctahedral group is a quite interesting group, whose definition, as a symmetry group, reminds that of the dihedral group D_N. So, let us start our study in the same way as we did for D_N, with a discussion at small values of $N \in \mathbb{N}$:

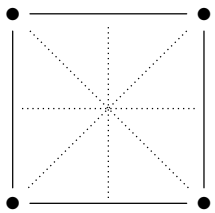
$\underline{N = 1}$. Here the 1-cube is the segment, whose symmetries are the identity id, plus the symmetry τ with respect to the middle of the segment:



Thus, we obtain the group with 2 elements, which is a very familiar object:

$$H_1 = D_2 = S_2 = \mathbb{Z}_2$$

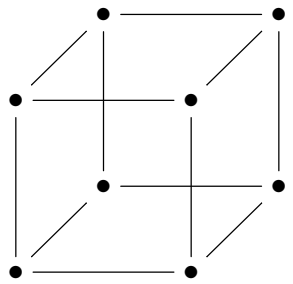
$\underline{N = 2}$. Here the 2-cube is the square, whose symmetries are the 4 rotations, of angles $0°, 90°, 180°, 270°$, and the 4 symmetries with respect to the 4 symmetry axes, which are the 2 diagonals, and the 2 segments joining the midpoints of opposite sides:



Thus, we obtain a group with 8 elements, which again is a very familiar object:

$$H_2 = D_4 = \mathbb{Z}_4 \rtimes \mathbb{Z}_2$$

$\underline{N = 3}$. Here the 3-cube is the usual cube in $\mathbb{R}^3$, pictured as follows:



However, in relation with the symmetries, the situation now is considerably more complicated, because, thinking well, this cube has no less than 48 symmetries. Precisely identifying and counting these symmetries is actually an excellent exercise.

All this looks quite complicated, but fortunately we can count H_N, at $N = 3$, and at higher N as well, by using some tricks, the result being as follows:

THEOREM 3.14. *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. This follows from some geometric thinking, as follows:

(1) 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 $\mathbb{R}^N$.

(2) In order to count now these latter symmetries, a bit as we did for the dihedral group, observe first that we have $N!$ permutations of these N coordinate axes.

(3) But each of these permutations of the coordinate axes $\sigma \in S_N$ can be further "decorated" by a sign vector $e \in \{\pm 1\}^N$, consisting of the possible ± 1 flips which can be applied to each coordinate axis, at the arrival.

(4) And the point is that, obviously, we obtain in this way all the elements of H_N. Thus, we have the following formula, for the cardinality of H_N:

$$|H_N| = |S_N| \cdot |\mathbb{Z}_2^N| = N! \cdot 2^N$$

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 3.15. *We have a wreath product decomposition as follows,*

$$H_N = \mathbb{Z}_2 \wr S_N$$

which means by definition that we have a crossed product decomposition

$$H_N = \mathbb{Z}_2^N \rtimes S_N$$

with the permutations $\sigma \in S_N$ acting on the elements $e \in \mathbb{Z}_2^N$ as follows:

$$\sigma(e_1, \ldots, e_k) = (e_{\sigma(1)}, \ldots, e_{\sigma(k)})$$

In particular we have, as found before, the cardinality formula $|H_N| = 2^N N!$.

PROOF. As explained in the proof of Theorem 3.14, the elements of H_N can be identified with the pairs $g = (e, \sigma)$ consisting of a permutation $\sigma \in S_N$, and a sign vector $e \in \mathbb{Z}_2^N$, so that at the level of the cardinalities, we have the following formula:

$$|H_N| = |\mathbb{Z}_2^N \times S_N|$$

To be more precise, given an element $g \in H_N$, the element $\sigma \in S_N$ is the corresponding permutation of the N coordinate axes, regarded as unoriented lines in $\mathbb{R}^N$, and $e \in \mathbb{Z}_2^N$ is the vector collecting the possible flips of these coordinate axes, at the arrival. Now observe that the product formula for two such pairs $g = (e, \sigma)$ is as follows, with the permutations $\sigma \in S_N$ acting on the elements $f \in \mathbb{Z}_2^N$ as in the statement:

$$(e, \sigma)(f, \tau) = (ef^\sigma, \sigma\tau)$$

Thus, we are precisely in the framework of the crossed products, as constructed in chapter 1, and we conclude that we have a crossed product decomposition, as follows:

$$H_N = \mathbb{Z}_2^N \rtimes S_N$$

Thus, we are led to the conclusion in the statement, with the formula $H_N = \mathbb{Z}_2 \wr S_N$ being just a shorthand for the decomposition $H_N = \mathbb{Z}_2^N \rtimes S_N$ that we found. □

We will be back to the hyperoctahedral groups later on, on several occasions, with further results about them, both of algebraic and of analytic type.

3c. Complex reflections

The groups that we studied so far are all groups of orthogonal matrices. When looking into general unitary matrices, we led to the following interesting class of groups:

DEFINITION 3.16. *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 $s = \infty$.

This construction is something quite tricky, that will keep as busy, for the remainder of this section. As a first observation, at $s = 1, 2$ we obtain the following groups:

$$H_N^1 = S_N \quad , \quad H_N^2 = H_N$$

Another important particular case of the above construction is $s = \infty$, where we obtain a group which is actually not finite, but is still compact, denoted as follows:

$$K_N \subset U_N$$

This latter group K_N is called full complex reflection group, and will appear many times, in what follows. Let us summarize now these observations, as follows:

PROPOSITION 3.17. *The complex reflection groups $H_N^s \subset U_N$ are as follows:*

(1) *At $s = 1$ we have $H_N^1 = S_N$, having cardinality $|S_N| = N!$.*
(2) *At $s = 2$ we have $H_N^2 = H_N$, having cardinality $|H_N| = 2^N N!$.*
(3) *At $s = \infty$ we have $H_N^\infty = K_N$, having cardinality $|K_N| = \infty$.*

PROOF. This is clear indeed from the above discussion, and with the cardinality results at $s = 1$ and $s = 2$ being something that we know well. □

Let us record as well the following result, which is elementary too:

PROPOSITION 3.18. *We have inclusions as follows, for any r, s:*

$$r|s \implies H_r \subset H_s$$

In particular, we have inclusions $S_N \subset H_N^s \subset K_N$, for any s.

PROOF. With the cyclic group $\mathbb{Z}_s$ being viewed as group of the s-th roots of unity, in the complex plane, as in Definition 3.16, we have inclusions as follows:

$$r|s \implies \mathbb{Z}_r \subset \mathbb{Z}_s$$

Thu, with the group H_N^s constructed as in Definition 3.16, for $r|s$ we have:

$$\begin{aligned} H_N^r &= M_N(\mathbb{Z}_r \cup \{0\}) \cap U_N \\ &\subset M_N(\mathbb{Z}_s \cup \{0\}) \cap U_N \\ &= H_N^s \end{aligned}$$

Finally, the last assertion is clear, and comes as well from this, since for any s:

$$1|s|\infty$$

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

In general, in analogy with what we know about S_N, H_N, we first have:

PROPOSITION 3.19. *The number of elements of H_N^s with $s \in \mathbb{N}$ is:*

$$|H_N^s| = s^N N!$$

At $s = \infty$, the group $K_N = H_N^\infty$ that we obtain is infinite.

PROOF. This is indeed clear from our definition of H_N^s, as a matrix group as above, because there are $N!$ choices for a permutation-type matrix, and then s^N choices for the corresponding s-roots of unity, which must decorate the N nonzero entries. □

Once again in analogy with what we know at $s = 1, 2$, we have as well:

THEOREM 3.20. *We have a wreath product decomposition*

$$H_N^s = \mathbb{Z}_s^N \rtimes S_N = \mathbb{Z}_s \wr S_N$$

with the permutations $\sigma \in S_N$ acting on the elements $e \in \mathbb{Z}_s^N$ as follows:

$$\sigma(e_1, \ldots, e_k) = (e_{\sigma(1)}, \ldots, e_{\sigma(k)})$$

In particular we have, as found before, the cardinality formula $|H_N^s| = s^N N!$.

PROOF. As explained in the proof of Proposition 3.19, the elements of H_N^s can be identified with the pairs $g = (e, \sigma)$ consisting of a permutation $\sigma \in S_N$, and a decorating vector $e \in \mathbb{Z}_s^N$, so that at the level of the cardinalities, we have:

$$|H_N| = |\mathbb{Z}_s^N \times S_N|$$

Now observe that the product formula for two such pairs $g = (e, \sigma)$ is as follows, with the permutations $\sigma \in S_N$ acting on the elements $f \in \mathbb{Z}_s^N$ as in the statement:

$$(e, \sigma)(f, \tau) = (ef^\sigma, \sigma\tau)$$

Thus, we are in the framework of the crossed products, and we obtain $H_N^s = \mathbb{Z}_s^N \rtimes S_N$. But this can be written, by definition, as $H_N^s = \mathbb{Z}_s \wr S_N$, and we are done. □

Finally, in relation with graph symmetries, the above groups appear as follows:

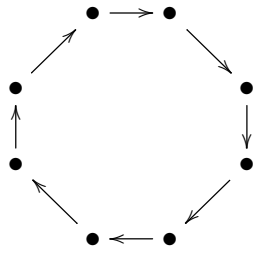
THEOREM 3.21. *The complex reflection group H_N^s appears as symmetry group,*

$$H_N^s = G(NC_s)$$

with NC_s consisting of N disjoint copies of the oriented cycle C_s.

PROOF. This is something elementary, the idea being as follows:

(1) Consider first the oriented cycle C_s, which looks as follows:



It is then clear that the symmetry group of this graph is the cyclic group $\mathbb{Z}_s$.

(2) In the general case now, where we have $N \in \mathbb{N}$ disjoint copies of the above cycle C_s, we must suitably combine the corresponding N copies of the cyclic group $\mathbb{Z}_s$. But this leads to the wreath product group $H_N^s = \mathbb{Z}_s \wr S_N$, as stated. □

3d. Reflection groups

Back to the rotation groups, in the real case, we have the following result:

PROPOSITION 3.22. *We have a decomposition as follows, with SO_N^{-1} consisting by definition of the orthogonal matrices having determinant -1:*

$$O_N = SO_N \cup SO_N^{-1}$$

Moreover, when N is odd the set SO_N^{-1} is simply given by $SO_N^{-1} = -SO_N$.

PROOF. The first assertion is clear from definitions, because the determinant of an orthogonal matrix must be ± 1. The second assertion is clear too. Finally, when N is even the situation is a bit more complicated, and requires complex numbers. □

In the complex case now, the result is simpler, as follows:

PROPOSITION 3.23. *We have a decomposition as follows, with SU_N^d consisting by definition of the unitary matrices having determinant $d \in \mathbb{T}$:*

$$O_N = \bigcup_{d \in \mathbb{T}} SU_N^d$$

Moreover, the components are $SU_N^d = f \cdot SU_N$, where $f \in \mathbb{T}$ is such that $f^N = d$.

PROOF. This is clear from definitions, and from the fact that the determinant of a unitary matrix belongs to $\mathbb{T}$, by extracting a suitable square root of the determinant. □

It is possible to use the decomposition in Proposition 3.23 in order to say more about what happens in the real case, in the context of Proposition 3.22, but we will not get into this. We will basically stop here with our study of O_N, U_N, and of their versions SO_N, SU_N. As a last result on the subject, however, let us record:

THEOREM 3.24. *We have subgroups of O_N, U_N constructed via the condition*

$$(\det U)^d = 1$$

with $d \in \mathbb{N} \cup \{\infty\}$, which generalize both O_N, U_N and SO_N, SU_N.

PROOF. This is indeed from definitions, and from the multiplicativity property of the determinant. We will be back to these groups, which are quite specialized, later on. □

With this discussed, let us go back now to the complex reflection groups from the previous section, and make a link with the material there. We first have:

THEOREM 3.25. *The full complex reflection group $K_N \subset U_N$, given by*

$$K_N = M_N(\mathbb{T} \cup \{0\}) \cap U_N$$

has a wreath product decomposition as follows,

$$K_N = \mathbb{T} \wr S_N$$

with S_N acting on $\mathbb{T}^N$ in the standard way, by permuting the factors.

PROOF. This is something that we know from before, appearing as the $s = \infty$ particular case of the results established there for the complex reflection groups H_N^s. □

By using the above full complex reflection group K_N, we can talk in fact about the reflection subgroup of any compact group $G \subset U_N$, as follows:

DEFINITION 3.26. *Given $G \subset U_N$, we define its reflection subgroup to be*

$$K = G \cap K_N$$

with the intersection taken inside U_N.

This notion is something quite interesting, leading us into the question of understanding what the subgroups of K_N are. We have here the following construction:

THEOREM 3.27. *We have subgroups of the basic complex reflection groups,*

$$H_N^{sd} \subset H_N^s$$

constructed via the following condition, with $d \in \mathbb{N} \cup \{\infty\}$,

$$(\det U)^d = 1$$

which generalize all the complex reflection groups that we have so far.

PROOF. Here the first assertion is clear from definitions, and from the multiplicativity of the determinant. As for the second assertion, this is rather a remark, coming from the fact that the alternating group A_N, which is the only finite group so far not fitting into the series $\{H_N^s\}$, is indeed of this type, obtained from $H_N^1 = S_N$ by using $d = 1$. □

The point now is that, by a well-known and deep result in group theory, the complex reflection groups consist of the series $\{H_N^{sd}\}$ constructed above, and of a number of exceptional groups, which can be fully classified. To be more precise, we have:

THEOREM 3.28. *The irreducible complex reflection groups are*

$$H_N^{sd} = \left\{ U \in H_N^s \middle| (\det U)^d = 1 \right\}$$

along with 34 exceptional examples.

PROOF. This is something quite advanced, and we refer here to the paper of Shephard and Todd [87], and to the subsequent literature on the subject. □

3e. Exercises

Exercises:

EXERCISE 3.29.

EXERCISE 3.30.

EXERCISE 3.31.

EXERCISE 3.32.

EXERCISE 3.33.

EXERCISE 3.34.

EXERCISE 3.35.

EXERCISE 3.36.

Bonus exercise.

CHAPTER 4

Abelian groups

4a. Group duals

We have seen so far that the basic examples of groups, even taken finite, lead us into linear algebra, and more specifically, into the study of groups of unitary matrices:

$$G \subset U_N$$

This is indeed a good idea, and we will systematically do this in this book, starting from the next chapter. Before getting into this, however, let us go back to the definition of the abstract groups, from the beginning of chapter 1, and make a last attempt of developing some useful general theory there, without relation to linear algebra.

Basic common sense suggests looking into the case of the finite abelian groups, which can only be far less complicated than the arbitrary finite groups. However, as somewhat a surprise, this leads us again into linear algebra, due to the following fact:

THEOREM 4.1. *Let us call representation of a finite group G any morphism*

$$u : G \to U_N$$

to a unitary group. Then the 1*-dimensional representations are the morphisms*

$$\chi : G \to \mathbb{T}$$

called characters of G, and these characters form a finite abelian group $\widehat{G}$.

PROOF. Regarding the first assertion, this is just some philosophy, making the link with matrices and linear algebra, and coming from $U_1 = \mathbb{T}$. So, let us prove now the second assertion, stating that the set of characters $\widehat{G} = \{\chi : G \to \mathbb{T}\}$ is a finite abelian group. There are several things to be proved here, the idea being as follows:

(1) Our first claim is that $\widehat{G}$ is a group, with the pointwise multiplication, namely:

$$(\chi\rho)(g) = \chi(g)\rho(g)$$

Indeed, if χ, ρ are characters, so is $\chi\rho$, and so the multiplication is well-defined on $\widehat{G}$. Regarding the unit, this is the trivial character, constructed as follows:

$$1 : G \to \mathbb{T} \quad , \quad g \to 1$$

Finally, we have inverses, with the inverse of $\chi : G \to \mathbb{T}$ being its conjugate:

$$\bar{\chi} : G \to \mathbb{T} \quad , \quad g \to \overline{\chi(g)}$$

(2) Our next claim is that $\widehat{G}$ is finite. Indeed, given a group element $g \in G$, we can talk about its order, which is smallest integer $k \in \mathbb{N}$ such that $g^k = 1$. Now assuming that we have a character $\chi : G \to \mathbb{T}$, we have the following formula:

$$\chi(g)^k = 1$$

Thus $\chi(g)$ must be one of the k-th roots of unity, and in particular there are finitely many choices for $\chi(g)$. Thus, there are finitely many choices for χ, as desired.

(3) Finally, the fact that $\widehat{G}$ is abelian follows from definitions, because the pointwise multiplication of functions, and in particular of characters, is commutative. □

The above construction is quite interesting, especially in the case where the starting finite group G is abelian itself, and as an illustration here, we have:

THEOREM 4.2. *The character group operation $G \to \widehat{G}$ for the finite abelian groups, called Pontrjagin duality, has the following properties:*

(1) *The dual of a cyclic group is the group itself, $\widehat{\mathbb{Z}}_N = \mathbb{Z}_N$.*
(2) *The dual of a product is the product of duals, $\widehat{G \times H} = \widehat{G} \times \widehat{H}$.*
(3) *Any product of cyclic groups $G = \mathbb{Z}_{N_1} \times \ldots \times \mathbb{Z}_{N_k}$ is self-dual, $G = \widehat{G}$.*

PROOF. We have several things to be proved, the idea being as follows:

(1) A character $\chi : \mathbb{Z}_N \to \mathbb{T}$ is uniquely determined by its value $z = \chi(g)$ on the standard generator $g \in \mathbb{Z}_N$. But this value must satisfy:

$$z^N = 1$$

Thus we must have $z \in \mathbb{Z}_N$, with the cyclic group $\mathbb{Z}_N$ being regarded this time as being the group of N-th roots of unity. Now conversely, any N-th root of unity $z \in \mathbb{Z}_N$ defines a character $\chi : \mathbb{Z}_N \to \mathbb{T}$, by setting, for any $r \in \mathbb{N}$:

$$\chi(g^r) = z^r$$

Thus we have an identification $\widehat{\mathbb{Z}}_N = \mathbb{Z}_N$, as claimed.

(2) A character of a product of groups $\chi : G \times H \to \mathbb{T}$ must satisfy:

$$\chi(g, h) = \chi\left[(g, 1)(1, h)\right] = \chi(g, 1)\chi(1, h)$$

Thus χ must appear as the product of its restrictions $\chi_{|G}, \chi_{|H}$, which must be both characters, and this gives the identification in the statement.

(3) This follows from (1) and (2). Alternatively, any character $\chi : G \to \mathbb{T}$ is uniquely determined by its values $\chi(g_1), \ldots, \chi(g_k)$ on the standard generators of $\mathbb{Z}_{N_1}, \ldots, \mathbb{Z}_{N_k}$, which must belong to $\mathbb{Z}_{N_1}, \ldots, \mathbb{Z}_{N_k} \subset \mathbb{T}$, and this gives $\widehat{G} = G$, as claimed. □

4b. Some analysis

We can get some further insight into group duality by using some standard spectral theory methods. Let us begin with the following basic fact from analysis:

THEOREM 4.3. *Given a Hilbert space H, consider the linear operators $T : H \to H$, and for each such operator define its norm by the following formula:*

$$||T|| = \sup_{||x||=1} ||Tx||$$

The operators which are bounded, $||T|| < \infty$, form then a complex algebra $B(H)$, which is complete with respect to $||.||$. When H comes with a basis $\{e_i\}_{i\in I}$, we have

$$B(H) \subset \mathcal{L}(H) \subset M_I(\mathbb{C})$$

where $\mathcal{L}(H)$ is the algebra of all linear operators $T : H \to H$, and $\mathcal{L}(H) \subset M_I(\mathbb{C})$ is the correspondence $T \to M$ obtained via the usual linear algebra formulae, namely:

$$T(x) = Mx \quad , \quad M_{ij} =< Te_j, e_i >$$

In infinite dimensions, none of the above two inclusions is an equality.

PROOF. This is something straightforward, the idea being as follows:

(1) The fact that we have indeed an algebra, satisfying the product condition in the statement, follows from the following estimates, which are all elementary:

$$||S + T|| \leq ||S|| + ||T|| \quad , \quad ||\lambda T|| = |\lambda| \cdot ||T|| \quad , \quad ||ST|| \leq ||S|| \cdot ||T||$$

(2) Regarding now the completness 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 $T(\lambda x) = \lambda T(x)$, and we conclude that $T \in \mathcal{L}(H)$.

(3) With this done, it remains to prove now that we have $T \in B(H)$, and that $T_n \to T$ in norm. For this purpose, observe that we have:

$$\begin{aligned} ||T_n - T_m|| \leq \varepsilon \ , \ \forall n, m \geq N &\implies ||T_n x - T_m x|| \leq \varepsilon \ , \ \forall ||x|| = 1 \ , \ \forall n, m \geq N \\ &\implies ||T_n x - Tx|| \leq \varepsilon \ , \ \forall ||x|| = 1 \ , \ \forall n \geq N \\ &\implies ||T_N x - Tx|| \leq \varepsilon \ , \ \forall ||x|| = 1 \\ &\implies ||T_N - T|| \leq \varepsilon \end{aligned}$$

But this gives both $T \in B(H)$, and $T_N \to T$ in norm, and we are done.

(4) Regarding the embeddings, the correspondence $T \to M$ in the statement is indeed linear, and its kernel is $\{0\}$, so we have indeed an embedding as follows, as claimed:

$$\mathcal{L}(H) \subset M_I(\mathbb{C})$$

In finite dimensions we have an isomorphism, because any $M \in M_N(\mathbb{C})$ determines an operator $T : \mathbb{C}^N \to \mathbb{C}^N$, given by $< Te_j, e_i >= M_{ij}$. However, in infinite dimensions, we have matrices not producing operators, as for instance the all-one matrix.

(5) As for the examples of linear operators which are not bounded, these are more complicated, coming from logic, and we will not really need them in what follows. □

Summarizing, the correct infinite analogue of the algebra $M_N(\mathbb{C})$ is not the infinite matrix algebra $M_I(\mathbb{C})$, which is actually not even an algebra, when $|I| = \infty$, but rather the algebra $B(H)$ of bounded linear operators $T : H \to H$ on a Hilbert space H.

Moving on, everything advanced that you know about $M_N(\mathbb{C})$, be that projections, rotations, other special matrices, or spectral theorems, uses adjoint matrices. So, let us talk now about adjoint operators, in our framework. The result here is as follows:

THEOREM 4.4. *Any bounded operator $T \in B(H)$ has an adjoint $T^* \in B(H)$, given by the following formula, valid for any two vectors $x, y \in H$:*

$$< Tx, y >=< x, T^* y >$$

The operation $T \to T^*$ is then an isometric involution of $B(H)$, and we have:

$$||TT^*|| = ||T||^2$$

When H comes with an orthonormal basis $\{e_i\}_{i \in I}$, we have $(T^*)_{ij} = \overline{T}_{ji}$.

PROOF. As before, all this is standard material. Given an operator $T \in B(H)$, let us pick a vector $y \in H$, and consider the following linear form:

$$x \to < Tx, y >$$

This linear form must then come from a scalar product with a vector T^*y, as in the statement, and we obtain in this way a definition for T^*, namely $y \to T^*y$. It is then routine to check that we have indeed $T^* \in B(H)$, with this coming from:

$$||T^*|| = ||T||$$

The fact that $T \to T^*$ is then an involution of $B(H)$ is routine too. Regarding now the formula $||TT^*|| = ||T||^2$, in one sense we have the following estimate:

$$||TT^*|| \leq ||T|| \cdot ||T^*|| = ||T||^2$$

In the other sense, we have the following estimate:

$$\begin{aligned} ||T||^2 &= \sup_{||x||=1} |< Tx, Tx >| \\ &= \sup_{||x||=1} |< x, T^*Tx >| \\ &\leq ||T^*T|| \end{aligned}$$

Now by replacing in this formula $T \to T^*$ we obtain $||T||^2 \leq ||TT^*||$, as desired. Finally, $(T^*)_{ij} = \overline{T}_{ji}$ is clear from the formula $T_{ij} =< Te_j, e_i >$, applied to T, T^*. □

Getting now back to algebra, in view of the above, let us formulate:

DEFINITION 4.5. *An abstract operator algebra, or C^*-algebra, is a complex algebra A having a norm $||.||$ and an involution $*$, subject to the following conditions:*

(1) *A is closed with respect to the norm.*
(2) *We have $||aa^*|| = ||a||^2$, for any $a \in A$.*

As a basic example, the algebra $M_N(\mathbb{C})$ of the complex $N \times N$ matrices is a C^*-algebra, with the usual matrix norm and involution of matrices, namely:

$$||M|| = \sup_{||x||=1} ||Mx|| \quad , \quad (M^*)_{ij} = \bar{M}_{ji}$$

More generally, we know from Theorem 4.3 and Theorem 4.4 that the algebra $B(H)$ of the bounded linear operators $T : H \to H$ on a complex Hilbert space H is a C^*-algebra, with the usual norm and involution of the linear operators, namely:

$$||T|| = \sup_{||x||=1} ||Tx|| \quad , \quad (T^*)_{ij} = \bar{T}_{ji}$$

But, let us stay for the moment with the usual matrices. Any $*$-subalgebra $A \subset M_N(\mathbb{C})$ is automatically closed, so is a C^*-algebra. In fact, we have the following result:

THEOREM 4.6. *The finite dimensional C^*-algebras are exactly the algebras*

$$A = M_{n_1}(\mathbb{C}) \oplus \ldots \oplus M_{n_k}(\mathbb{C})$$

with norm $||(a_1, \ldots, a_k)|| = \sup_i ||a_i||$, and involution $(a_1, \ldots, a_k)^* = (a_1^*, \ldots, a_k^*)$.

PROOF. This is something very standard. Consider indeed an arbitrary $*$-algebra of the $N \times N$ matrices, $A \subset M_N(\mathbb{C})$. Let us first look at the center of this algebra, $Z(A) = A \cap A'$. This center, viewed as an algebra, is then of the following form:

$$Z(A) \simeq \mathbb{C}^k$$

Consider now the standard basis $e_1, \ldots, e_k \in \mathbb{C}^k$, and let $p_1, \ldots, p_k \in Z(A)$ be the images of these vectors via the above identification. In other words, these elements $p_1, \ldots, p_k \in A$ are central minimal projections, summing up to 1:

$$p_1 + \ldots + p_k = 1$$

The idea is then that this partition of the unity will eventually lead to the block decomposition of A, as in the statement. We prove this in 4 steps, as follows:

Step 1. We first construct the matrix blocks, our claim here being that each of the following linear subspaces of A are non-unital $*$-subalgebras of A:

$$A_i = p_i A p_i$$

But this is clear, with the fact that each A_i is closed under the various non-unital $*$-subalgebra operations coming from the projection equations $p_i^2 = p_i^* = p_i$.

Step 2. We prove now that the above algebras $A_i \subset A$ are in a direct sum position, in the sense that we have a non-unital $*$-algebra sum decomposition, as follows:

$$A = A_1 \oplus \ldots \oplus A_k$$

As with any direct sum question, we have two things to be proved here. First, by using the formula $p_1 + \ldots + p_k = 1$ and the projection equations $p_i^2 = p_i^* = p_i$, we conclude that we have the needed generation property, namely:

$$A_1 + \ldots + A_k = A$$

As for the fact that the sum is indeed direct, this follows as well from the formula $p_1 + \ldots + p_k = 1$, and from the projection equations $p_i^2 = p_i^* = p_i$.

Step 3. Our claim now, which will finish the proof, is that each of the $*$-subalgebras $A_i = p_i A p_i$ constructed above is in fact a full matrix algebra. To be more precise, with $n_i = rank(p_i)$, our claim is that we have isomorphisms, as follows:

$$A_i \simeq M_{n_i}(\mathbb{C})$$

In order to prove this claim, recall that the projections $p_i \in A$ were chosen central and minimal. Thus, the center of each of the algebras A_i reduces to the scalars:

$$Z(A_i) = \mathbb{C}$$

But this shows, either via a direct computation, or via the bicommutant theorem, that the each of the algebras A_i is a full matrix algebra, as claimed.

Step 4. We can now obtain the result, by putting together what we have. Indeed, by using the results from Step 2 and Step 3, we obtain an isomorphism as follows:

$$A \simeq M_{n_1}(\mathbb{C}) \oplus \ldots \oplus M_{n_k}(\mathbb{C})$$

In addition to this, a careful look at the isomorphisms established in Step 3 shows that at the global level, of the algebra A itself, the above isomorphism simply comes by twisting the following standard multimatrix embedding, discussed in the beginning of the proof, (1) above, by a certain unitary matrix $U \in U_N$:

$$M_{n_1}(\mathbb{C}) \oplus \ldots \oplus M_{n_k}(\mathbb{C}) \subset M_N(\mathbb{C})$$

Now by putting everything together, we obtain the result. □

Let us develop now the theory of the arbitrary C^*-algebras. We first have:

THEOREM 4.7. *Given an element $a \in A$ of a C^*-algebra, define its spectrum as:*

$$\sigma(a) = \left\{\lambda \in \mathbb{C}\middle| a - \lambda \notin A^{-1}\right\}$$

The following spectral theory results hold, exactly as in the $A = B(H)$ case:

(1) *We have $\sigma(ab) \cup \{0\} = \sigma(ba) \cup \{0\}$.*
(2) *We have $\sigma(f(a)) = f(\sigma(a))$, for any $f \in \mathbb{C}(X)$ having poles outside $\sigma(a)$.*
(3) *The spectrum $\sigma(a)$ is compact, non-empty, and contained in $D_0(||a||)$.*
(4) *The spectra of unitaries ($u^* = u^{-1}$) and self-adjoints ($a = a^*$) are on $\mathbb{T}, \mathbb{R}$.*
(5) *The spectral radius of normal elements ($aa^* = a^*a$) is given by $\rho(a) = ||a||$.*

In addition, assuming $a \in A \subset B$, the spectra of a with respect to A and to B coincide.

PROOF. Here the assertions (1-5), which are formulated a bit informally, are well-known for the full operator algebra $A = B(H)$, and the proof in general is similar:

(1) Assuming that $1 - ab$ is invertible, with inverse c, we have $abc = cab = c - 1$, and it follows that $1 - ba$ is invertible too, with inverse $1 + bca$. Thus $\sigma(ab), \sigma(ba)$ agree on $1 \in \mathbb{C}$, and by linearity, it follows that $\sigma(ab), \sigma(ba)$ agree on any point $\lambda \in \mathbb{C}^*$.

(2) The formula $\sigma(f(a)) = f(\sigma(a))$ is clear for polynomials, $f \in \mathbb{C}[X]$, by factorizing $f - \lambda$, with $\lambda \in \mathbb{C}$. Then, the extension to the rational functions is straightforward, because $P(a)/Q(a) - \lambda$ is invertible precisely when $P(a) - \lambda Q(a)$ is.

(3) By using $1/(1-b) = 1 + b + b^2 + \ldots$ for $||b|| < 1$ we obtain that $a - \lambda$ is invertible for $|\lambda| > ||a||$, and so $\sigma(a) \subset D_0(||a||)$. It is also clear that $\sigma(a)$ is closed, so what we have is a compact set. Finally, assuming $\sigma(a) = \emptyset$ the function $f(\lambda) = \varphi((a - \lambda)^{-1})$ is well-defined, for any $\varphi \in A^*$, and by Liouville we get $f = 0$, contradiction.

(4) Assuming $u^* = u^{-1}$ we have $||u|| = 1$, and so $\sigma(u) \subset D_0(1)$. But with $f(z) = z^{-1}$ we obtain via (2) that we have as well $\sigma(u) \subset f(D_0(1))$, and this gives $\sigma(u) \subset \mathbb{T}$. As for the result regarding the self-adjoints, this can be obtained from the result for the unitaries, by using (2) with functions of type $f(z) = (z + it)/(z - it)$, with $t \in \mathbb{R}$.

(5) It is routine to check, by integrating quantities of type $z^n/(z-a)$ over circles centered at the origin, and estimating, that the spectral radius is given by $\rho(a) = \lim ||a^n||^{1/n}$. But in the self-adjoint case, $a = a^*$, this gives $\rho(a) = ||a||$, by using exponents of type $n = 2^k$, and then the extension to the general normal case is straightforward.

(6) Regarding now the last assertion, the inclusion $\sigma_B(a) \subset \sigma_A(a)$ is clear. For the converse, assume $a - \lambda \in B^{-1}$, and set $b = (a-\lambda)^*(a-\lambda)$. We have then:

$$\sigma_A(b) - \sigma_B(b) = \left\{\mu \in \mathbb{C} - \sigma_B(b) \middle| (b-\mu)^{-1} \in B - A\right\}$$

Thus this difference in an open subset of $\mathbb{C}$. On the other hand b being self-adjoint, its two spectra are both real, and so is their difference. Thus the two spectra of b are equal, and in particular b is invertible in A, and so $a - \lambda \in A^{-1}$, as desired. □

With these ingredients, we can now a prove a key result, as follows:

THEOREM 4.8 (Gelfand). *If X is a compact space, the algebra $C(X)$ of continuous functions on it $f : X \to \mathbb{C}$ is a C^*-algebra, with usual norm and involution, namely:*

$$||f|| = \sup_{x \in X} |f(x)| \quad , \quad f^*(x) = \overline{f(x)}$$

Conversely, any commutative C^*-algebra is of this form, $A = C(X)$, with

$$X = \left\{\chi : A \to \mathbb{C} \ , \ \text{normed algebra character}\right\}$$

with topology making continuous the evaluation maps $ev_a : \chi \to \chi(a)$.

PROOF. There are several things going on here, the idea being as follows:

(1) The first assertion is clear from definitions. Observe that we have indeed:

$$||ff^*|| = \sup_{x \in X} |f(x)|^2 = ||f||^2$$

Observe also that the algebra $C(X)$ is commutative, because $fg = gf$.

(2) Conversely, given a commutative C^*-algebra A, let us define X as in the statement. Then X is compact, and $a \to ev_a$ is a morphism of algebras, as follows:

$$ev : A \to C(X)$$

(3) We first prove that ev is involutive. We use the following formula, which is similar to the $z = Re(z) + iIm(z)$ decomposition formula for usual complex numbers:

$$a = \frac{a + a^*}{2} + i \cdot \frac{a - a^*}{2i}$$

Thus it is enough to prove $ev_{a^*} = ev_a^*$ for the self-adjoint elements a. But this is the same as proving that $a = a^*$ implies that ev_a is a real function, which is in turn true, by Theorem 4.7, because $ev_a(\chi) = \chi(a)$ is an element of $\sigma(a)$, contained in $\mathbb{R}$.

(4) Since A is commutative, each element is normal, so ev is isometric:

$$||ev_a|| = \rho(a) = ||a||$$

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. □

Now back to groups and duality, we are led in this way to the following result:

THEOREM 4.9. *Given a finite abelian group G, we have an isomorphism of commutative C^*-algebras as follows, obtained by linearizing/delinearizing the characters:*

$$\mathbb{C}[G] \simeq C(\widehat{G})$$

Also, the Pontrjagin duality is indeed a duality, in the sense that we have $G = \widehat{\widehat{G}}$.

PROOF. We have several assertions here, the idea being as follows:

(1) Given a finite abelian group G, consider indeed the group algebra $\mathbb{C}[G]$, having as elements the formal combinations of elements of G, and with involution given by:

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

This $*$-algebra is then a C^*-algebra, with norm coming by acting $\mathbb{C}[G]$ on itself, and so by the Gelfand theorem we obtain an isomorphism as follows:

$$\mathbb{C}[G] = C(X)$$

To be more precise, X is the space of the $*$-algebra characters as follows:

$$\chi : \mathbb{C}[G] \to \mathbb{C}$$

The point now is that by delinearizing, such a $*$-algebra character must come from a usual group character of G, obtained by restricting to G, as follows:

$$\chi : G \to \mathbb{T}$$

Thus we have $X = \widehat{G}$, and we are led to the isomorphism in the statement, namely:

$$\mathbb{C}[G] \simeq C(\widehat{G})$$

(2) In order to prove now the second assertion, consider the following group morphism, which is available for any finite group G, not necessarily abelian:

$$G \to \widehat{\widehat{G}} \quad , \quad g \to (\chi \to \chi(g))$$

Our claim is that in the case where G is abelian, this is an isomorphism. As a first observation, we only need to prove that this morphism is injective or surjective, because the cardinalities match, according to the following formula, coming from (1):

$$|G| = \dim \mathbb{C}[G] = \dim C(\widehat{G}) = |\widehat{G}|$$

(3) We will prove that the above morphism is injective. For this purpose, let us compute its kernel. We know that $g \in G$ is in the kernel when the following happens:

$$\chi(g) = 1 \quad , \quad \forall \chi \in \widehat{G}$$

But this means precisely that $g \in \mathbb{C}[G]$ is mapped, via the isomorphism $\mathbb{C}[G] \simeq C(\widehat{G})$ constructed in (1), to the constant function $1 \in C(\widehat{G})$, and now by getting back to $\mathbb{C}[G]$ via our isomorphism, this shows that we have indeed $g = 1$, which ends the proof. □

4c. Sylow theorems

Sylow theorems.

4d. Abelian groups

With the above ingredients in hand, we can go back to the finite abelian groups. We have the following result, which is something remarkable, refining all the above:

THEOREM 4.10. *The finite abelian groups are the following groups,*

$$G = \mathbb{Z}_{N_1} \times \ldots \times \mathbb{Z}_{N_k}$$

and these groups are all self-dual, $G = \widehat{G}$.

PROOF. This is something quite tricky, the idea being as follows:

(1) In order to prove our result, assume that G is finite and abelian. For any prime number $p \in \mathbb{N}$, let us define $G_p \subset G$ to be the subset of elements having as order a power of p. Equivalently, this subset $G_p \subset G$ can be defined as follows:

$$G_p = \left\{ g \in G \middle| \exists k \in \mathbb{N}, g^{p^k} = 1 \right\}$$

(2) It is then routine to check, based on definitions, that each G_p is a subgroup. Our claim now is that we have a direct product decomposition as follows:

$$G = \prod_p G_p$$

(3) Indeed, by using the fact that our group G is abelian, we have a morphism as follows, with the order of the factors when computing $\prod_p g_p$ being irrelevant:

$$\prod_p G_p \to G \quad , \quad (g_p) \to \prod_p g_p$$

Moreover, it is routine to check that this morphism is both injective and surjective, via some simple manipulations, so we have our group decomposition, as in (2).

(4) Thus, we are left with proving that each component G_p decomposes as a product of cyclic groups, having as orders powers of p, as follows:

$$G_p = \mathbb{Z}_{p^{r_1}} \times \ldots \times \mathbb{Z}_{p^{r_s}}$$

But this is something that can be checked by recurrence on $|G_p|$, via some routine computations, and so we are led to the conclusion in the statement.

(5) Finally, the fact that the finite abelian groups are self-dual, $G = \widehat{G}$, follows from the structure result that we just proved, and from Theorem 4.2 (3). □

So long for finite abelian groups. All the above was of course a bit quick, and for further details on all this, and especially on Theorem 4.10, which is something non-trivial, and for some generalizations as well, to the case of suitable non-finite abelian groups, we refer to the algebra book of Lang [64], where all this material is carefully explained.

We can feel that all this is related to Fourier analysis, and we have:

FACT 4.11. *The following happen, regarding the locally compact abelian groups:*

(1) *What we did in the finite case, namely group characters, and construction and basic properties of the dual, can be extended to them.*
(2) *As basic examples of this, besides what we have in the finite case, and notably $\widehat{\mathbb{Z}}_N = \mathbb{Z}_N$, we have $\widehat{\mathbb{Z}} = \mathbb{T}$, $\widehat{\mathbb{T}} = \mathbb{Z}$, and also $\widehat{\mathbb{R}} = \mathbb{R}$.*
(3) *With some care for analytic aspects, $C^*(G) \simeq C(\widehat{G})$ remains true in this setting, and in the case $G = \mathbb{R}$, this isomorphism is the Fourier transform.*

Obviously, all this is a bit heavy, but you get the point, we have 3 types of Fourier analysis in life, namely the "standard" one that we previously learned in this chapter, corresponding to $G = \mathbb{R}$, then another one that we skipped, and that we encourage you to learn, called the "Fourier series" one, corresponding to $G = \mathbb{Z}, \mathbb{T}$, and finally the "discrete" one that we started to learn, over $G = \mathbb{Z}_N$ and other finite abelian groups.

In practice, all this is a bit complicated, and back now to the finite abelian groups, let us work out a softer version of all the above, which is what is really needed, in practice, when doing discrete Fourier analysis. For $G = \mathbb{Z}_N$, what we need is:

DEFINITION 4.12. *The Fourier matrix F_N is the following matrix, with $w = e^{2\pi i/N}$:*

$$F_N = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & w & w^2 & \ldots & w^{N-1} \\ 1 & w^2 & w^4 & \ldots & w^{2(N-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & w^{N-1} & w^{2(N-1)} & \ldots & w^{(N-1)^2} \end{pmatrix}$$

That is, $F_N = (w^{ij})_{ij}$, with indices $i, j \in \{0, 1, \ldots, N-1\}$, taken modulo N.

Observe that this matrix is Hadamard, in the sense that its entries are on the unit circle, and the rows are pairwise orthogonal, the result here being as follows:

THEOREM 4.13. *The Fourier matrix, constructed as above,*

$$F_N = (w^{ij}) \quad , \quad w = e^{2\pi i/N}$$

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. □

More generally now, we have the following result:

THEOREM 4.14. *Given a finite abelian group G, with dual group $\widehat{G} = \{\chi : G \to \mathbb{T}\}$, consider the corresponding Fourier coupling, namely:*

$$\mathcal{F}_G : G \times \widehat{G} \to \mathbb{T} \quad , \quad (i, \chi) \to \chi(i)$$

(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 by using the above finite abelian 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:

$$< R_i, R_j >= \sum_\chi \chi(i)\overline{\chi(j)} = \sum_\chi \chi(i-j) = |G| \cdot \delta_{ij}$$

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 as follows, with $w = e^{2\pi i/N}$:

$$(i, j) \to w^{ij}$$

(3) We use here the following formula that we know, 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 nice application of discrete Fourier analysis, we have:

THEOREM 4.15. *For a matrix $M\in M_N(\mathbb{C})$, the following are equivalent:*

(1) *M is circulant, $M_{ij}=\xi_{j-i}$, for a certain vector $\xi\in\mathbb{C}^N$.*

(2) *M is Fourier-diagonal, $M=F_NQF_N^*$, for a certain diagonal matrix Q.*

Moreover, if these conditions hold, then $\xi=F_N^*q$, where $q=(Q_{11},\ldots,Q_{NN})$.

PROOF. This follows from some computations with roots of unity, as follows:

(1) $\implies$ (2) Assuming $M_{ij}=\xi_{j-i}$, the matrix $Q=F_N^*MF_N$ is indeed diagonal, as shown by the following computation:

$$\begin{aligned}Q_{ij}&=\sum_{kl}w^{jl-ik}\xi_{l-k}\\&=\sum_{kr}w^{j(k+r)-ik}\xi_r\\&=N\delta_{ij}\sum_r w^{jr}\xi_r\end{aligned}$$

(2) $\implies$ (1) Assuming $Q=diag(q_1,\ldots,q_N)$, the matrix $M=F_NQF_N^*$ is indeed circulant, as shown by the following computation:

$$M_{ij}=\sum_k w^{ik}Q_{kk}w^{-jk}=\sum_k w^{(i-j)k}q_k$$

Indeed, since the last term depends only on $j-i$, we have $M_{ij}=\xi_{j-i}$, with $\xi_i=\sum_k w^{-ik}q_k=(F_N^*q)_i$. Thus, we are led to the conclusions in the statement. □

As an illustration for the above result, the all-one matrix diagonalizes as follows:

THEOREM 4.16. *The flat matrix $\mathbb{I}_N$ diagonalizes as follows,*

$$\begin{pmatrix}1&\ldots&\ldots&1\\\vdots&&&\vdots\\\vdots&&&\vdots\\1&\ldots&\ldots&1\end{pmatrix}=\frac{1}{N}F_N\begin{pmatrix}N&&&\\&0&&\\&&\ddots&\\&&&0\end{pmatrix}F_N^*$$

with $F_N=(w^{ij})_{ij}$ being the Fourier matrix.

PROOF. This follows from Theorem 4.15, but let us see as well how the direct proof goes. We must find the 0-eigenvectors of $\mathbb{I}_N$, which amounts in solving:

$$x_0 + \ldots + x_{N-1} = 0$$

For this purpose, we use the root of unity $w = e^{2\pi i/N}$, and more specifically, the following standard formula, coming by computing a barycenter, in the obvious way:

$$\sum_{i=0}^{N-1} w^{ij} = N\delta_{j0}$$

This formula shows that for $j = 1, \ldots, N-1$, the vector $v_j = (w^{ij})_i$ is a 0-eigenvector. Moreover, these vectors are pairwise orthogonal, because we have:

$$< v_j, v_k >= \sum_i w^{ij-ik} = N\delta_{jk}$$

Thus, we have our basis $\{v_1, \ldots, v_{N-1}\}$ of 0-eigenvectors, and since the N-eigenvector is $\xi = v_0$, the passage matrix P that we are looking is given by:

$$P = \begin{bmatrix} v_0 & v_1 & \ldots & v_{N-1} \end{bmatrix}$$

But this is precisely the Fourier matrix, $P = F_N$. In order to finish now, observe that the above computation of $< v_i, v_j >$ shows that $F_N/\sqrt{N}$ is unitary, and so:

$$F_N^{-1} = \frac{1}{N} F_N^*$$

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

There are many other interesting illustrations of Theorem 4.15, the general idea being that, in everything regarding the circulant matrices, we must use Fourier.

Next, we have the following result, which is standard in discrete Fourier analysis, extending what we previously knew from the above, in the circulant case:

THEOREM 4.17. *For a matrix $A \in M_N(\mathbb{C})$, the following are equivalent,*

(1) *A is G-invariant, $A_{ij} = \xi_{j-i}$, for a certain vector $\xi \in \mathbb{C}^N$,*
(2) *A is Fourier-diagonal, $A = F_G Q F_G^*$, for a certain diagonal matrix Q,*

and if so, $\xi = F_G^* q$, where $q \in \mathbb{C}^N$ is the vector formed by the diagonal entries of Q.

PROOF. This is something that we know from the above in the cyclic case, $G = \mathbb{Z}_N$, and the proof in general is similar, by using matrix indices as follows:

$$i, j \in G$$

To be more precise, in order to get started, with our generalization, let us decompose our finite abelian group G as a product of cyclic groups, as follows:

$$G = \mathbb{Z}_{N_1} \times \ldots \times \mathbb{Z}_{N_s}$$

The corresponding Fourier matrix decomposes then as well, as follows:

$$F_G = F_{N_1} \otimes \ldots \otimes F_{N_s}$$

Now if we set $w_i = e^{2\pi i/N_i}$, this means that we have the following formula:

$$(F_G)_{ij} = w_1^{i_1 j_1} \ldots w_s^{i_s j_s}$$

We can now prove the equivalence in the statement, as follows:

(1) $\implies$ (2) Assuming $A_{ij} = \xi_{j-i}$, the matrix $Q = F_G^* A F_G$ is diagonal, as shown by the following computation, with all indices being group elements:

$$\begin{aligned}
Q_{ij} &= \sum_{kl} \overline{(F_G)}_{ki} A_{kl} (F_G)_{lj} \\
&= \sum_{kl} w_1^{-k_1 i_1} \ldots w_s^{-k_s i_s} \cdot \xi_{l-k} \cdot w_1^{l_1 j_1} \ldots w_s^{l_s j_s} \\
&= \sum_{kl} w_1^{l_1 j_1 - k_1 i_1} \ldots w_s^{l_s j_s - k_s i_s} \xi_{l-k} \\
&= \sum_{kr} w_1^{(k_1+r_1) j_1 - k_1 i_1} \ldots w_s^{(k_s+r_s) j_s - k_s i_s} \xi_r \\
&= \sum_{r} w_1^{r_1 j_1} \ldots w_s^{r_s j_s} \xi_r \sum_{k} w_1^{k_1(j_1-i_1)} \ldots w_s^{k_s(j_s-i_s)} \\
&= \sum_{r} w_1^{r_1 j_1} \ldots w_s^{r_s j_s} \xi_r \cdot N_1 \delta_{i_1 j_1} \ldots N_s \delta_{i_s j_s} \\
&= N \delta_{ij} \sum_{r} (F_G)_{jr} \xi_r
\end{aligned}$$

(2) $\implies$ (1) Assuming $Q = diag(q_1, \ldots, q_N)$, the matrix $A = F_G Q F_G^*$ is G-invariant, as shown by the following computation, again with all indices being group elements:

$$\begin{aligned}
A_{ij} &= \sum_{kl} (F_G)_{ik} Q_{kk} \overline{(F_G)}_{kj} \\
&= \sum_{k} w_1^{i_1 k_1} \ldots w_s^{i_s k_s} \cdot q_k \cdot w_1^{-j_1 k_1} \ldots w_s^{-j_s k_s} \\
&= \sum_{k} w_1^{(i_1-j_1) k_1} \ldots w_s^{(i_s-j_s) k_s} q_k
\end{aligned}$$

To be more precise, in this formula the last term depends only on $j-i$, and so shows that we have $A_{ij}=\xi_{j-i}$, with ξ being the following vector:

$$\begin{aligned}\xi_i &= \sum_k w_1^{-i_1k_1}\ldots w_s^{-i_sk_s}q_k\\ &= \sum_k (F_G^*)_{ik}q_k\\ &= (F_G^*q)_i\end{aligned}$$

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

Many other things can be said, as a continuation of the above.

4e. Exercises

Exercises:

Exercise 4.18.

Exercise 4.19.

Exercise 4.20.

Exercise 4.21.

Exercise 4.22.

Exercise 4.23.

Exercise 4.24.

Exercise 4.25.

Bonus exercise.

Part II

Representations

Red, red wine
Goes to my head
Make me forget that I
Still need her so

CHAPTER 5

Representations

5a. Representations

We have seen in the previous chapter that the 1-dimensional unitary representations $\chi : G \to \mathbb{T}$ of a finite group G, also called characters, led to some interesting insight into the structure of G, notably with some remarkable results, in the abelian case.

In this chapter, and in fact in this whole Part II of the present book, we discuss what can be done with the unitary representations $u : G \to U_N$, in the general case, $N \in \mathbb{N}$. We will see that there is some non-trivial theory here, called Peter-Weyl theory for finite groups, extending, in a subtle way, what we know about the finite abelian groups.

Let us start with something very basic, and intuitive too, that we already met in the previous chapter, in the one-dimensional case $N = 1$, namely:

DEFINITION 5.1. *A representation of a finite group G is a morphism as follows:*

$$u : G \to U_N$$

The character of such a representation is the function $\chi : G \to \mathbb{C}$ given by

$$g \to Tr(u_g)$$

where Tr is the usual trace of the $N \times N$ matrices, $Tr(M) = \sum_i M_{ii}$.

As a first comment here, as mentioned above, we have already met such things in chapter 4, in the case $N = 1$. To be more precise, in the case $N = 1$ we have $U_1 = \mathbb{T}$, and so both the representation, and its character, are a group morphism as follows:

$$u = \chi : G \to \mathbb{T}$$

As a basic example here, for any finite group we always have available the trivial 1-dimensional representation, or character, which is by definition as follows:

$$u : G \to U_1 \quad , \quad g \to (1)$$

As another example, when our finite group G appears as a group of unitary matrices, $G \subset U_N$, the embedding $G \subset U_N$ itself is a representation, called fundamental one:

$$u : G \subset U_N \quad , \quad g \to g$$

In this situation, there are many other representations of G, which are equally interesting. For instance, we can define the representation conjugate to u, as being:

$$\bar{u} : G \subset U_N \quad , \quad g \to \bar{g}$$

In order to clarify all this, and see which representations are available, let us first discuss the various operations on the representations.

The result here, which is something very standard, is as follows:

PROPOSITION 5.2. *The representations of a finite group G are subject to:*

(1) *Making sums. Given representations u, v, having dimensions N, M, their sum is the $N + M$-dimensional representation $u + v = diag(u, v)$.*
(2) *Making products. Given representations u, v, having dimensions N, M, their tensor product is the NM-dimensional representation $(u \otimes v)_{ia,jb} = u_{ij}v_{ab}$.*
(3) *Taking conjugates. Given a representation u, having dimension N, its complex conjugate is the N-dimensional representation $(\bar{u})_{ij} = \bar{u}_{ij}$.*
(4) *Spinning by unitaries. Given a representation u, having dimension N, and a unitary $V \in U_N$, we can spin u by this unitary, $u \to VuV^*$.*

PROOF. The fact that the operations in the statement are indeed well-defined, among maps from G to unitary groups, can be checked as follows:

(1) This follows from the trivial fact that if $g \in U_N$ and $h \in U_M$ are two unitaries, then their diagonal sum is a unitary too, as follows:

$$\begin{pmatrix} g & 0 \\ 0 & h \end{pmatrix} \in U_{N+M}$$

(2) This follows from the fact that if $g \in U_N$ and $h \in U_M$ are two unitaries, then $g \otimes h \in U_{NM}$ is a unitary too. Given unitaries g, h, let us set indeed:

$$(g \otimes h)_{ia,jb} = g_{ij}h_{ab}$$

This matrix is then a unitary too, as shown by the following computation:

$$\begin{aligned}
[(g \otimes h)(g \otimes h)^*]_{ia,jb} &= \sum_{kc} (g \otimes h)_{ia,kc}((g \otimes h)^*)_{kc,jb} \\
&= \sum_{kc} (g \otimes h)_{ia,kc}\overline{(g \otimes h)_{jb,kc}} \\
&= \sum_{kc} g_{ik}h_{ac}\bar{g}_{jk}\bar{h}_{bc} \\
&= \sum_{k} g_{ik}\bar{g}_{jk} \sum_{c} h_{ac}\bar{h}_{bc} \\
&= \delta_{ij}\delta_{ab}
\end{aligned}$$

(3) This simply follows from the fact that if $g \in U_N$ is unitary, then so is its complex conjugate, $\bar{g} \in U_N$, and this due to the following formula, obtained by conjugating:

$$g^* = g^{-1} \implies g^t = \bar{g}^{-1}$$

(4) This is clear as well, because if $g \in U_N$ is unitary, and $V \in U_N$ is another unitary, then we can spin g by this unitary, and we obtain a unitary as follows:

$$VgV^* \in U_N$$

Thus, our operations are well-defined, and this leads to the above conclusions. □

In relation now with characters, we have the following result:

PROPOSITION 5.3. *We have the following formulae, regarding characters*

$$\chi_{u+v} = \chi_u + \chi_v \quad , \quad \chi_{u\otimes v} = \chi_u\chi_v$$

$$\chi_{\bar{u}} = \bar{\chi}_u \quad , \quad \chi_{VuV^*} = \chi_u$$

in relation with the basic operations for the representations.

PROOF. All these assertions are elementary, by using the following well-known trace formulae, valid for any two square matrices g, h, and any unitary V:

$$Tr(diag(g,h)) = Tr(g) + Tr(h) \quad , \quad Tr(g \otimes h) = Tr(g)Tr(h)$$

$$Tr(\bar{g}) = \overline{Tr(g)} \quad , \quad Tr(VgV^*) = Tr(g)$$

To be more precise, the first formula is clear from definitions. Regarding now the second formula, the computation here is immediate too, as follows:

$$\begin{aligned} Tr(g \otimes h) &= \sum_{ia} (g \otimes h)_{ia,ia} \\ &= \sum_{ia} g_{ii}h_{aa} \\ &= Tr(g)Tr(h) \end{aligned}$$

Regarding now the third formula, this is clear from definitions, by conjugating. Finally, regarding the fourth formula, this can be established as follows:

$$Tr(VgV^*) = Tr(gV^*V) = Tr(g)$$

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

Assume now that we are given a finite group $G \subset U_N$. By using the above operations, we can construct a whole family of representations of G, as follows:

DEFINITION 5.4. *Given a finite group $G \subset U_N$, its Peter-Weyl representations are the tensor products between the fundamental representation and its conjugate:*

$$u : G \subset U_N \quad , \quad \bar{u} : G \subset U_N$$

We denote these tensor products $u^{\otimes k}$, with $k = \circ \bullet \bullet \circ \ldots$ being a colored integer, with the colored tensor powers being defined according to the rules

$$u^{\otimes \circ} = u \quad , \quad u^{\otimes \bullet} = \bar{u} \quad , \quad u^{\otimes kl} = u^{\otimes k} \otimes u^{\otimes l}$$

and with the convention that $u^{\otimes \emptyset}$ is the trivial representation $1 : G \to U_1$.

Here are a few examples of such Peter-Weyl representations, namely those coming from the colored integers of length 2, to be often used in what follows:

$$u^{\otimes \circ\circ} = u \otimes u \quad , \quad u^{\otimes \circ\bullet} = u \otimes \bar{u}$$

$$u^{\otimes \bullet\circ} = \bar{u} \otimes u \quad , \quad u^{\otimes \bullet\bullet} = \bar{u} \otimes \bar{u}$$

In relation now with characters, we have the following result:

PROPOSITION 5.5. *The characters of Peter-Weyl representations are given by*

$$\chi_{u^{\otimes k}} = (\chi_u)^k$$

with the colored powers of a variable χ being by definition given by

$$\chi^\circ = \chi \quad , \quad \chi^\bullet = \bar{\chi} \quad , \quad \chi^{kl} = \chi^k \chi^l$$

and with the convention that $\chi^\emptyset$ equals by definition 1.

PROOF. This follows indeed from the additivity, multiplicativity and conjugation formulae established in Proposition 5.3, via the conventions in Definition 5.4. □

Given a closed subgroup $G \subset U_N$, we would like to understand its Peter-Weyl representations, and compute the expectations of the characters of these representations. In order to do so, let us formulate the following key definition:

DEFINITION 5.6. *Given a finite group G, and two of its representations,*

$$u : G \to U_N \quad , \quad v : G \to U_M$$

we define the linear space of intertwiners between these representations as being

$$Hom(u, v) = \left\{ T \in M_{M \times N}(\mathbb{C}) \middle| Tu_g = v_g T, \forall g \in G \right\}$$

and we use the following conventions:

(1) *We use the notations $Fix(u) = Hom(1, u)$, and $End(u) = Hom(u, u)$.*
(2) *We write $u \sim v$ when $Hom(u, v)$ contains an invertible element.*
(3) *We say that u is irreducible, and write $u \in Irr(G)$, when $End(u) = \mathbb{C}1$.*

In the above the terminology is very standard, with Hom and End standing respectively for "homomorphisms" and "endomorphisms", and with Fix standing for "fixed points". In practice, it is useful to think of the representations of G as being the objects of some kind of abstract combinatorial structure associated to G, and of the intertwiners between these representations as being the "arrows" between these objects.

We have in fact the following result, which clarifies all this:

THEOREM 5.7. *The following happen:*

(1) *The intertwiners are stable under composition:*

$$T \in Hom(u, v) \ , \ S \in Hom(v, w) \implies ST \in Hom(u, w)$$

(2) *The intertwiners are stable under taking tensor products:*

$$S \in Hom(u, v) \ , \ T \in Hom(w, t) \implies S \otimes T \in Hom(u \otimes w, v \otimes t)$$

(3) *The intertwiners are stable under taking adjoints:*

$$T \in Hom(u, v) \implies T^* \in Hom(v, u)$$

(4) *Thus, the Hom spaces form a tensor $*$-category.*

PROOF. All this is clear from definitions, the verifications being as follows:

(1) This follows indeed from the following computation, valid for any $g \in G$:

$$STu_g = Sv_gT = w_gST$$

(2) Again, this is clear, because we have the following computation:

$$\begin{aligned}(S \otimes T)(u_g \otimes w_g) &= Su_g \otimes Tw_g \\ &= v_gS \otimes t_gT \\ &= (v_g \otimes t_g)(S \otimes T)\end{aligned}$$

(3) This follows from the following computation, valid for any $g \in G$:

$$\begin{aligned}Tu_g = v_gT &\implies u_g^*T^* = T^*v_g^* \\ &\implies T^*v_g = u_gT^*\end{aligned}$$

(4) This is just an abstract conclusion of (1,2,3), with a tensor $*$-category being by definition an abstract beast satisfying these conditions (1,2,3). We will be back to tensor categories later on in this book, with more details on all this. □

5b. Peter-Weyl

Our claim now is that Theorem 5.7 gives us everything that we need, in order to have some advanced representation theory started, for our finite groups G. Indeed, as a main consequence of Theorem 5.7, we have the following key result:

THEOREM 5.8. *Given a representation $u : G \to U_N$, the linear space*

$$End(u) \subset M_N(\mathbb{C})$$

is a $*$-algebra, with respect to the usual involution of the matrices.

PROOF. We know from Theorem 5.7 (1) that $End(u)$ is a subalgebra of $M_N(\mathbb{C})$, and we know as well from Theorem 5.7 (3) that this subalgebra is stable under the involution $*$. Thus, what we have here is a $*$-subalgebra of $M_N(\mathbb{C})$, as claimed. □

The point now is that we can combine the above result with the following standard fact, from advanced linear algebra, that we know well from chapter 4:

THEOREM 5.9. *Let $A \subset M_N(\mathbb{C})$ be a $*$-algebra.*

(1) *We can write $1 = p_1 + \ldots + p_k$, with $p_i \in A$ being central minimal projections.*
(2) *The linear spaces $A_i = p_i A p_i$ are non-unital $*$-subalgebras 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 $A_i \simeq M_{n_i}(\mathbb{C})$, with $n_i = rank(p_i)$.*
(5) *Thus, we have a $*$-algebra isomorphism $A \simeq M_{n_1}(\mathbb{C}) \oplus \ldots \oplus M_{n_k}(\mathbb{C})$.*

PROOF. This is indeed something very standard, that we know well from chapter 4, and we refer to the material there for the proof, and for various comments. □

Good news, we can now formulate our first Peter-Weyl theorem, as follows:

THEOREM 5.10 (PW1). *Let $u : G \to U_N$ be a representation, consider the algebra $A = End(u)$, and write its unit as above, with p_i being central minimal projections:*

$$1 = p_1 + \ldots + p_k$$

The representation u decomposes then as a direct sum, as follows,

$$u = u_1 + \ldots + u_k$$

with each u_i being an irreducible representation, obtained by restricting u to $Im(p_i)$.

PROOF. This basically follows from Theorem 5.8 and Theorem 5.9, as follows:

(1) As a first observation, by replacing G with its image $u(G) \subset U_N$, we can assume if we want that our representation u is faithful, $G \subset_u U_N$. However, this replacement will not be really needed, and we will keep using $u : G \to U_N$, as above.

(2) In order to prove the result, we will need some preliminaries. We first associate to our representation $u : G \to U_N$ 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 $v \subset u$. This is clear indeed from definitions, and with the remark that the unitaries, being isometries, restrict indeed into unitaries.

(3) Consider now a projection $p \in End(u)$. From $pu = up$ we obtain that the linear space $V = Im(p)$ is invariant under u, and so this space must come from a subrepresentation $v \subset u$. It is routine to check that the operation $p \to v$ maps subprojections to subrepresentations, and minimal projections to irreducible representations.

(4) To be more precise here, the condition $p \in End(u)$ reformulates as follows:

$$pu_g = u_g p \quad , \quad \forall g \in G$$

As for the condition that $V = Im(p)$ is invariant, this reformulates as follows:

$$pu_g p = u_g p \quad , \quad \forall g \in G$$

Thus, we are in need of a technical linear algebra result, stating that for a projection $P \in M_N(\mathbb{C})$ and a unitary $U \in U_N$, the following happens:

$$PUP = UP \implies PU = UP$$

(5) But this can be established with some C^*-algebra know-how, as follows:

$$\begin{aligned} tr[(PU - UP)(PU - UP)^*] &= tr[(PU - UP)(U^*P - PU^*)] \\ &= tr[P - PUPU^* - UPU^*P + UPU^*] \\ &= tr[P - UPU^* - UPU^* + UPU^*] \\ &= tr[P - UPU^*] \\ &= 0 \end{aligned}$$

Indeed, by positivity this gives $PU - UP = 0$, as desired.

(6) With these preliminaries in hand, let us decompose the algebra $End(u)$ as in Theorem 5.9, by using the decomposition $1 = p_1 + \ldots + p_k$ into minimal projections. If we denote by $u_i \subset u$ the subrepresentation coming from the vector space $V_i = Im(p_i)$, then we obtain in this way a decomposition $u = u_1 + \ldots + u_k$, as in the statement. □

In order to formulate our second Peter-Weyl theorem, let us formulate:

Definition 5.11. *Given a finite subgroup $G \subset U_N$, and a unitary representation $v : G \to U_M$, the space of coefficients of this representation is:*

$$C_v = \left\{ f \circ v \middle| f \in M_M(\mathbb{C})^* \right\}$$

In other words, by delinearizing, $C_\nu \subset C(G)$ is the following linear space,

$$C_v = span\left[g \to (v_g)_{ij} \right]$$

with $g \to (v_g)_{ij}$ being the standard matrix coefficients of $v : G \to U_M$.

As a basic example of coefficient we have, besides the matrix coefficients $g \to (v_g)_{ij}$, the character, which appears as the diagonal sum of these coefficients:

$$\chi_v(g) = \sum_i (v_g)_{ii}$$

Here is now our second Peter-Weyl theorem, complementing Theorem 5.10:

THEOREM 5.12 (PW2). *Given a subgroup $G \subset_u U_N$, any irreducible representation*

$$v : G \to U_M$$

appears inside a tensor product of the fundamental representation u and its adjoint $\bar{u}$.

PROOF. In order to prove the result, we will use the following three elementary facts, regarding the spaces of coefficients introduced above:

(1) The construction $v \to C_v$ is functorial, in the sense that it maps subrepresentations into linear subspaces. This is indeed something which is routine to check.

(2) By the Stone-Weierstrass theorem, which tells us that we have $< g_{ij} >= C(G)$, we conclude that have an inclusion of linear spaces as follows:

$$C_v \subset < g_{ij} >$$

(3) By definition of the Peter-Weyl representations, as arbitrary tensor products between the fundamental representation u and its conjugate $\bar{u}$, we have:

$$< g_{ij} >= \sum_k C_{u^{\otimes k}}$$

(4) Now by putting together the observations (2,3) we conclude that we must have an inclusion as follows, for certain exponents $k_1, \ldots, k_p$:

$$C_v \subset C_{u^{\otimes k_1} \oplus \ldots \oplus \pi^{\otimes k_p}}$$

By using now the functoriality result from (1), we deduce from this that we have an inclusion of representations, as follows:

$$v \subset u^{\otimes k_1} \oplus \ldots \oplus u^{\otimes k_p}$$

Together with Theorem 5.10, this leads to the conclusion in the statement. □

As a conclusion to what we have so far, the problem to be solved is that of splitting the Peter-Weyl representations into sums of irreducible representations.

5c. More Peter-Weyl

In order to further advance, and complete the Peter-Weyl theory, we need to talk about integration over G. In the present finite group case the situation is trivial, as follows:

PROPOSITION 5.13. *Any finite group G has a unique probability measure which is invariant under left and right translations,*

$$\mu(E) = \mu(gE) = \mu(Eg)$$

and this is the normalized counting measure on G, given by $\mu(E) = |E|/|G|$.

PROOF. The uniformity condition in the statement gives, with $E = \{h\}$:

$$\mu\{h\} = \mu\{gh\} = \mu\{hg\}$$

Thus μ must be the usual counting measure, normalized as to have mass 1. □

However, for our purposes here, we need to know more about averaging over G. It is convenient 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 5.14. *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 $f = (\tau \otimes id)v$ we have

$$\int_\varphi f = \tau(P)$$

where P is the orthogonal projection onto the 1-eigenspace of $(id \otimes \varphi)v$.

PROOF. By linearity it is enough to prove the first assertion for functions of the following type, where v is a Peter-Weyl representation, and τ is a linear form:

$$f = (\tau \otimes id)v$$

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 $f = (\tau \otimes id)v$:

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \varphi^{*k}(f) = \tau(P)$$

In order to prove this latter formula, observe that we have:

$$\varphi^{*k}(f) = (\tau \otimes \varphi^{*k})v = \tau((id \otimes \varphi^{*k})v)$$

Let us set $M = (id \otimes \varphi)v$. In terms of this matrix, we have:

$$((id \otimes \varphi^{*k})v)_{i_0 i_{k+1}} = \sum_{i_1 \ldots i_k} M_{i_0 i_1} \ldots M_{i_k i_{k+1}} = (M^k)_{i_0 i_{k+1}}$$

Thus we have the following formula, for any $k \in \mathbb{N}$:

$$(id \otimes \varphi^{*k})v = M^k$$

It follows that our Cesàro limit is given by the following formula:

$$\begin{aligned}\lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{n}\varphi^{*k}(f) &= \lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{n}\tau(M^k)\\ &= \tau\left(\lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{n}M^k\right)\end{aligned}$$

Now since v is unitary we have $||v|| = 1$, and so $||M|| \leq 1$. Thus the last Cesàro limit 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. □

The point now is that when the linear form $\varphi \in C(G)^*$ from the above result is chosen to be faithful, we obtain the following finer result:

PROPOSITION 5.15. *Given a faithful unital linear form $\varphi \in C(G)^*$, the limit*

$$\int_\varphi f = \lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{n}\varphi^{*k}(f)$$

exists, and is independent of φ, given on coefficients of representations by

$$\left(id \otimes \int_\varphi\right)v = P$$

where P is the orthogonal projection onto the space $Fix(v) = \left\{\xi \in \mathbb{C}^n \middle| v\xi = \xi\right\}$.

PROOF. In view of Proposition 5.14, it remains to prove that when φ is faithful, the 1-eigenspace of the matrix $M = (id \otimes \varphi)v$ equals the space $Fix(v)$.

"$\supset$" This is clear, and for any φ, because we have the following implication:

$$v\xi = \xi \implies M\xi = \xi$$

"$\subset$" 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 function:

$$f = \sum_i\left(\sum_j v_{ij}\xi_j - \xi_i\right)\left(\sum_k v_{ik}\xi_k - \xi_i\right)^*$$

We must prove that we have $f = 0$. Since v is unitary, we have:

$$\begin{aligned} f &= \sum_{ijk} v_{ij} v_{ik}^* \xi_j \bar{\xi}_k - \frac{1}{N} v_{ij} \xi_j \bar{\xi}_i - \frac{1}{N} v_{ik}^* \xi_i \bar{\xi}_k + \frac{1}{N^2} \xi_i \bar{\xi}_i \\ &= \sum_j |\xi_j|^2 - \sum_{ij} v_{ij} \xi_j \bar{\xi}_i - \sum_{ik} v_{ik}^* \xi_i \bar{\xi}_k + \sum_i |\xi_i|^2 \\ &= ||\xi||^2 - < v\xi, \xi > - \overline{< v\xi, \xi >} + ||\xi||^2 \\ &= 2(||\xi||^2 - Re(< v\xi, \xi >)) \end{aligned}$$

By using now our assumption $M\xi = \xi$, we obtain from this:

$$\begin{aligned} \varphi(f) &= 2\varphi(||\xi||^2 - Re(< v\xi, \xi >)) \\ &= 2(||\xi||^2 - Re(< M\xi, \xi >)) \\ &= 2(||\xi||^2 - ||\xi||^2) \\ &= 0 \end{aligned}$$

Now since φ is faithful, this gives $f = 0$, and so $v\xi = \xi$, as claimed. □

We can now formulate a main result, as follows:

THEOREM 5.16. *Any finite group G has a unique Haar integration, which can be constructed by starting with any faithful positive unital state $\varphi \in C(G)^*$, and setting:*

$$\int_G = \lim_{n \to \infty} \frac{1}{n} \sum_{k=1}^{n} \varphi^{*k}$$

Moreover, for any representation v we have the formula

$$\left(id \otimes \int_G \right) v = P$$

where P is the orthogonal projection onto $Fix(v) = \left\{ \xi \in \mathbb{C}^n \middle| v\xi = \xi \right\}$.

PROOF. We can prove this from what we have, in several steps, as follows:

(1) Let us first go back to the general context of Proposition 5.14. Since convolving one more time with φ will not change the Cesàro limit appearing there, the functional $\int_\varphi \in C(G)^*$ 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 5.15, our claim is that we have the following formula, valid this time for any $\psi \in C(G)^*$:

$$\int_\varphi * \psi = \psi * \int_\varphi = \psi(1) \int_\varphi$$

Moreover, it is enough to prove this formula on a coefficient of a representation:

$$f = (\tau \otimes id)v$$

(2) In order to do so, consider the following two matrices:

$$P = \left(id \otimes \int_\varphi\right) v \quad , \quad Q = (id \otimes \psi)v$$

We have then the following two computations, involving these matrices:

$$\left(\int_\varphi * \psi\right) f = \left(\tau \otimes \int_\varphi \otimes \psi\right)(v_{12}v_{13}) = \tau(PQ)$$

$$\left(\psi * \int_\varphi\right) f = \left(\tau \otimes \psi \otimes \int_\varphi\right)(v_{12}v_{13}) = \tau(QP)$$

Also, regarding the term on the right in our formula in (1), this is given by:

$$\psi(1) \int_\varphi f = \psi(1)\tau(P)$$

We conclude from all this that our claim is equivalent to the following equality:

$$PQ = QP = \psi(1)P$$

(3) But this latter equality holds indeed, coming from the fact, that we know from Proposition 5.15, that $P = (id \otimes \int_\varphi)v$ equals the orthogonal projection onto $Fix(v)$. Thus, we have proved our claim in (1), namely that the following formula holds:

$$\int_\varphi * \psi = \psi * \int_\varphi = \psi(1) \int_\varphi$$

(4) In order to finish now, it is convenient to introduce the following abstract operation, on the continuous functions $f, f' : C(G) \to \mathbb{C}$ on our group:

$$\Delta(f \otimes f')(g \otimes h) = f(g)f'(h)$$

With this convention, the formula that we established above can be written as:

$$\psi\left(\int_\varphi \otimes id\right)\Delta = \psi\left(id \otimes \int_\varphi\right)\Delta = \psi \int_\varphi (.)1$$

This formula being true for any $\psi \in C(G)^*$, we can simply delete ψ. We conclude that the following invariance formula holds indeed, with $\int_G = \int_\varphi$:

$$\left(\int_G \otimes id\right)\Delta = \left(id \otimes \int_G\right)\Delta = \int_G (.)1$$

But this is exactly the left and right invariance formula we were looking for.

(5) Finally, in order to prove the uniqueness assertion, assuming that we have two invariant integrals $\int_G, \int'_G$, we have, according to the above invariance formula:

$$\left(\int_G \otimes \int'_G\right)\Delta = \left(\int'_G \otimes \int_G\right)\Delta = \int_G (.)1 = \int'_G (.)1$$

Thus we have $\int_G = \int'_G$, and this finishes the proof. □

Summarizing, we can now integrate over G. As a first application, we have:

THEOREM 5.17. *Given a finite group G, we have the following formula, valid for any unitary group representation $v : G \to U_M$:*

$$\int_G \chi_v = \dim(Fix(v))$$

In particular, in the unitary matrix group case, $G \subset_u U_N$, the moments of the main character $\chi = \chi_u$ are given by the following formula:

$$\int_G \chi^k = \dim(Fix(u^{\otimes k}))$$

Thus, knowing the law of χ is the same as knowing the dimensions on the right.

PROOF. We have three assertions here, the idea being as follows:

(1) Given a unitary representation $v : G \to U_M$ as in the statement, its character χ_v is a coefficient, so we can use the integration formula for coefficients in Theorem 5.16. If we denote by P the projection onto $Fix(v)$, that formula gives, as desired:

$$\begin{aligned}\int_G \chi_v &= Tr(P)\\ &= \dim(Im(P))\\ &= dim(Fix(v))\end{aligned}$$

(2) This follows from (1), applied to the Peter-Weyl representations, as follows:

$$\begin{aligned}\int_G \chi^k &= \int_G \chi_u^k\\ &= \int_G \chi_{u^{\otimes k}}\\ &= \dim(Fix(u^{\otimes k}))\end{aligned}$$

(3) This follows from (2), and from the standard fact, which follows from definitions, that a probability measure is uniquely determined by its moments. □

As a key remark now, the integration formula in Theorem 5.16 allows the computation for the truncated characters too, because these truncated characters are coefficients as well. To be more precise, all the probabilistic questions about G, regarding characters, or truncated characters, or more complicated variables, require a good knowledge of the integration over G, and more precisely, of the various polynomial integrals over G:

DEFINITION 5.18. *Given a finite subgroup $G \subset U_N$, the quantities*

$$I_k = \int_G g_{i_1j_1}^{e_1} \ldots g_{i_kj_k}^{e_k} \, dg$$

depending on a colored integer $k = e_1 \ldots e_k$, are called polynomial integrals over G.

As a first observation, the knowledge of these integrals is the same as the knowledge of the integration functional over G. Indeed, since the coordinate functions $g \to g_{ij}$ separate the points of G, we can apply the Stone-Weierstrass theorem, and we obtain:

$$C(G) = < g_{ij} >$$

Thus, by linearity, the computation of any functional $f : C(G) \to \mathbb{C}$, and in particular of the integration functional, reduces to the computation of this functional on the polynomials of the coordinate functions $g \to g_{ij}$ and their conjugates $g \to \bar{g}_{ij}$.

By using now Peter-Weyl theory, everything reduces to algebra, as follows:

THEOREM 5.19. *The Haar integration over a closed subgroup $G \subset_u U_N$ is given on the dense subalgebra of smooth functions by the Weingarten formula*

$$\int_G g_{i_1j_1}^{e_1} \ldots g_{i_kj_k}^{e_k} \, dg = \sum_{\pi,\sigma \in D_k} \delta_\pi(i)\delta_\sigma(j) W_k(\pi, \sigma)$$

valid for any colored integer $k = e_1 \ldots e_k$ and any multi-indices i, j, where D_k is a linear basis of $Fix(u^{\otimes k})$, the associated generalized Kronecker symbols are given by

$$\delta_\pi(i) = < \pi, e_{i_1} \otimes \ldots \otimes e_{i_k} >$$

and $W_k = G_k^{-1}$ is the inverse of the Gram matrix, $G_k(\pi, \sigma) = < \pi, \sigma >$.

PROOF. We know from Peter-Weyl theory that the integrals in the statement form altogether the orthogonal projection P^k onto the following space:

$$Fix(u^{\otimes k}) = span(D_k)$$

Consider now the following linear map, with $D_k = \{\xi_k\}$ being as in the statement:

$$E(x) = \sum_{\pi \in D_k} < x, \xi_\pi > \xi_\pi$$

By a standard linear algebra computation, it follows that we have $P = WE$, where W is the inverse of the restriction of E to the following space:

$$K = span\left(T_\pi \middle| \pi \in D_k\right)$$

But this restriction is precisely the linear map given by the matrix G_k, and so W itself is the linear map given by the matrix W_k, and this gives the result. □

We will be back to this in Part III below, with some concrete applications.

In order to further develop now the Peter-Weyl theory, which is something very useful, we will need the following result, which is of independent interest:

PROPOSITION 5.20. *We have a Frobenius type isomorphism*

$$Hom(v, w) \simeq Fix(v \otimes \bar{w})$$

valid for any two representations v, w.

PROOF. According to the definitions, we have the following equivalences:

$$\begin{aligned} T \in Hom(v, w) &\iff Tv = wT \\ &\iff \sum_j T_{aj} v_{ji} = \sum_b w_{ab} T_{bi}, \forall a, i \end{aligned}$$

On the other hand, we have as well the following equivalences:

$$\begin{aligned} T \in Fix(v \otimes \bar{w}) &\iff (v \otimes \bar{w})T = \xi \\ &\iff \sum_{jb} v_{ij} w_{ab}^* T_{bj} = T_{ai} \forall a, i \end{aligned}$$

With these formulae in hand, both inclusions follow from the unitarity of v, w. □

We can now formulate our third Peter-Weyl theorem, as follows:

THEOREM 5.21 (PW3). *We have a direct sum decomposition of linear spaces*

$$C(G) = \bigoplus_{v \in Irr(G)} M_{\dim(v)}(\mathbb{C})$$

with the summands being pairwise orthogonal with respect to the scalar product

$$< a, b >= \int_G ab^*$$

where $\int_G$ is the averaging over G.

PROOF. This is something more tricky, the idea being as follows:

(1) By combining the previous two Peter-Weyl results, from Theorem 5.10 and Theorem 5.12, we deduce that we have a linear space decomposition as follows:

$$C(G) = \sum_{v\in Irr(G)} C_v = \sum_{v\in Irr(G)} M_{\dim(v)}(\mathbb{C})$$

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:

$$v \not\sim w \implies C_v \perp C_w$$

(2) We will need the basic fact, whose proof is elementary, that for any representation v we have the following formula, where P is the orthogonal projection on $Fix(v)$:

$$\left(id \otimes \int_G\right) v = P$$

(3) We will also need the basic fact, that we know from the above, that for any two representations v, w we have an isomorphism as follows, called Frobenius isomorphism:

$$Hom(v, w) \simeq Fix(v \otimes \bar{w})$$

(4) Now back to our orthogonality question from (1), let us set indeed:

$$P_{ia,jb} = \int_G v_{ij} w_{ab}^*$$

Then P is the orthogonal projection onto the following vector space:

$$Fix(v \otimes \bar{w}) \simeq Hom(v, w) = \{0\}$$

Thus we have $P = 0$, and this gives the result. □

Finally, we have the following result, completing the Peter-Weyl theory:

THEOREM 5.22 (PW4). *The characters of irreducible representations belong to*

$$C(G)_{central} = \left\{ f \in C(G) \middle| f(gh) = f(hg), \forall g, h \in G \right\}$$

called algebra of central functions on G, and form an orthonormal basis of it.

PROOF. We have several things to be proved, the idea being as follows:

(1) Observe first that $C(G)_{central}$ is indeed an algebra, which contains all the characters. Conversely, consider a function $f \in C(G)$, written as follows:

$$f = \sum_{v\in Irr(G)} f_v$$

The condition $f \in C(G)_{central}$ states then that for any $v \in Irr(G)$, we must have:

$$f_v \in C(G)_{central}$$

But this means precisely that the coefficient f_v must be a scalar multiple of χ_v, and so the characters form a basis of $C(G)_{central}$, as stated.

(2) The fact that we have an orthogonal basis follows from Theorem 5.21.

(3) 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 that the above integrals $\int_G v_{ij}v_{kl}^*$ form the orthogonal projection onto the following vector space:

$$Fix(v\otimes\bar{v}) \simeq End(v) = \mathbb{C}1$$

Thus, the proof of our theorem is now complete. □

5d. Central functions

As a key observation now, complementing Theorem 5.22, observe that a function $f : G \to \mathbb{C}$ is central, in the sense that it satisfies $f(gh) = f(hg)$, precisely when it satisfies the following condition, saying that it must be constant on conjugacy classes:

$$f(ghg^{-1}) = f(h), \forall g, h \in G$$

Thus, in the finite group case for instance, the algebra of central functions is something which is very easy to compute, and this gives useful information about $Rep(G)$. We will not get into this here, but some of our exercises will be about this.

As a basic illustration for all this, which clarifies some previous considerations from chapter 4, in relation with our study there of the abelian groups, we have:

THEOREM 5.23. *For a compact abelian group G the irreducible representations are all 1-dimensional, and form the dual discrete abelian group $\widehat{G}$.*

PROOF. This is clear from the Peter-Weyl theory, because when G is abelian any function $f : G \to \mathbb{C}$ is central, and so the algebra of central functions is $\mathcal{C}(G)$ itself, and so the irreducible representations $u \in Irr(G)$ coincide with their characters $\chi_u \in \widehat{G}$. □

So long for Peter-Weyl theory. As a comment, our approach here to this theory, which was rather functional analytic, was motivated by what we will be doing later in this book, in relation with compact groups, and with quantum groups too.

For a more standard presentation of the Peter-Weyl theory for finite groups, there are many good books available, such as the book of Serre [85].

5e. Exercises

Exercises:

EXERCISE 5.24.

EXERCISE 5.25.

EXERCISE 5.26.

EXERCISE 5.27.

EXERCISE 5.28.

EXERCISE 5.29.

EXERCISE 5.30.

EXERCISE 5.31.

Bonus exercise.

CHAPTER 6

Tannakian duality

6a. Generalities

We have seen that, no matter what we want to do with $G \subset U_N$, we must compute the spaces $Fix(u^{\otimes k})$. In the case $G \subset O_N$, it is convenient to introduce:

DEFINITION 6.1. *Associated to any closed subgroup $G \subset O_N$ are the vector spaces*

$$C_{kl} = \left\{ T \in \mathcal{L}(H^{\otimes k}, H^{\otimes l}) \middle| Tg^{\otimes k} = g^{\otimes l}T, \forall g \in G \right\}$$

where $H = \mathbb{C}^N$. We call Tannakian category of G the collection of spaces $C = (C_{kl})$.

Observe that, due to $g \in G \subset O_N \subset \mathcal{L}(H)$, we have $g^{\otimes k} \in \mathcal{L}(H^{\otimes k})$ for any k, so the equality $Tg^{\otimes k} = g^{\otimes l}T$ makes indeed sense, as an equality of maps as follows:

$$Tg^{\otimes k}, g^{\otimes l}T \in \mathcal{L}(H^{\otimes k}, H^{\otimes l})$$

It is also clear by definition that each C_{kl} is a complex vector space. Moreover, it is also clear by definition that $C = (C_{kl})$ is indeed a category, in the sense that:

$$T \in C_{kl} \ , \ S \in C_{lm} \implies ST \in C_{km}$$

Quite remarkably, the closed subgroup $G \subset O_N$ can be reconstructed from its Tannakian category $C = (C_{kl})$, and in a very simple way. More precisely, we have:

CLAIM 6.2. *Given a closed subgroup $G \subset O_N$, we have*

$$G = \left\{ g \in O_N \middle| Tg^{\otimes k} = g^{\otimes l}T, \forall k, l, \forall T \in C_{kl} \right\}$$

where $C = (C_{kl})$ is the associated Tannakian category.

So, this is what we will be talking about in this chapter. Let us begin with some simple observations. We first have the following elementary result:

PROPOSITION 6.3. *Given a closed subgroup $G \subset O_N$, set as before*

$$C_{kl} = \left\{ T \in \mathcal{L}(H^{\otimes k}, H^{\otimes l}) \middle| Tg^{\otimes k} = g^{\otimes l}T, \forall g \in G \right\}$$

where $H = \mathbb{C}^N$, and then set as in Claim 6.2:

$$\widetilde{G} = \left\{ g \in O_N \middle| Tg^{\otimes k} = g^{\otimes l}T, \forall k, l, \forall T \in C_{kl} \right\}$$

Then $\widetilde{G}$ is closed subgroup of O_N, and we have inclusions $G \subset \widetilde{G} \subset O_N$.

PROOF. Let us first prove that $\widetilde{G}$ is a group. Assuming $g,h\in\widetilde{G}$, we have $gh\in\widetilde{G}$, due to the following computation, valid for any k,l and any $T\in C_{kl}$:

$$\begin{aligned}T(gh)^{\otimes k}&=Tg^{\otimes k}h^{\otimes k}\\&=g^{\otimes l}Th^{\otimes k}\\&=g^{\otimes l}h^{\otimes l}T\\&=(gh)^{\otimes l}T\end{aligned}$$

Also, we have $1\in\widetilde{G}$, trivially. Finally, assuming $g\in\widetilde{G}$, we have:

$$\begin{aligned}T(g^{-1})^{\otimes k}&=(g^{-1})^{\otimes l}[g^{\otimes l}T](g^{-1})^{\otimes k}\\&=(g^{-1})^{\otimes l}[Tg^{\otimes k}](g^{-1})^{\otimes k}\\&=(g^{-1})^{\otimes l}T\end{aligned}$$

Thus we have $g^{-1}\in\widetilde{G}$, and so $\widetilde{G}$ is a group, as claimed. Finally, the fact that we have an inclusion $G\subset\widetilde{G}$, and that $\widetilde{G}\subset O_N$ is closed, are both clear from definitions. □

Let us work out some examples too. The orthogonal diagonal matrices form a subgroup $\mathbb{Z}_2^N\subset O_N$, and for the subgroups $G\subset\mathbb{Z}_2^N$ our theory is quite exciting, as follows:

THEOREM 6.4. *For the abelian groups of diagonal matrices, $G\subset\mathbb{Z}_2^N$, we have*

$$C_{kl}=\left\{T\in\mathcal{L}(H^{\otimes k},H^{\otimes l})\Big|\exists g\in G,g_{i_1}\ldots g_{i_k}\neq g_{j_1}\ldots g_{j_l}\implies T_{j_1\ldots j_l,i_1\ldots i_k}=0\right\}$$

with the notation $g=diag(g_1,\ldots,g_N)$, and Claim 6.2 holds when $|G|=1,2,2^{N-1},2^N$.

PROOF. We have several things to be proved, the idea being as follows:

(1) Case $G=\{1\}$. Here we obviously have, for any two integers k,l, the following formula, which confirms the general formula in the statement:

$$C_{kl}=\mathcal{L}(H^{\otimes k},H^{\otimes l})$$

Regarding now Claim 6.2, consider the intermediate subgroup $G\subset\widetilde{G}\subset O_N$, constructed in Proposition 6.3, that we must prove to be equal to G itself. Since any element $g\in\widetilde{G}$ must commute with the algebra $C_{11}=M_N(\mathbb{C})$, we must have:

$$g=\pm1$$

But from the relation $T=gT$, which must hold for any $T\in C_{01}=H$, we conclude that we must have $g=1$, so we obtain $\widetilde{G}=\{1\}$, as desired.

(2) Case $G=\mathbb{Z}_2$, with this meaning $G=\{1,-1\}$. This is something just a bit more complicated. Let us look at the relations defining C_{kl}, namely:

$$Tg^{\otimes k}=g^{\otimes l}T$$

These relations are automatic for $g = 1$. As for the other group element, namely $g = -1$, here the relations hold either when $k + l$ is even, or when $T = 0$. Thus, we have the following formula, which confirms again the general formula in the statement:

$$C_{kl} = \begin{cases} \mathcal{L}(H^{\otimes k}, H^{\otimes l}) & (k + l \in 2\mathbb{N}) \\ \{0\} & (k + l \notin 2\mathbb{N}) \end{cases}$$

As for Claim 6.2 for our group, this follows from the computation done in (1) above, the point being that $g \in \widetilde{G}$ commutes with $C_{11} = M_N(\mathbb{C})$ precisely when $g = \pm 1$.

(3) General case $G \subset \mathbb{Z}_2^N$. Let us look at the relations defining C_{kl}. We have:

$$\begin{aligned} T \in C_{kl} &\iff Tg^{\otimes k} = g^{\otimes l}T, \forall g \in G \\ &\iff (Tg^{\otimes k})_{ji} = (g^{\otimes l}T)_{ji}, \forall i, j, \forall g \in G \\ &\iff T_{j_1 \ldots j_l, i_1 \ldots i_k} g_{i_1} \ldots g_{i_k} = g_{j_1} \ldots g_{j_l} T_{j_1 \ldots j_k, i_1 \ldots i_l}, \forall i, j, \forall g \in G \\ &\iff (g_{j_1} \ldots g_{i_k} - g_{j_1} \ldots g_{j_l}) T_{j_1 \ldots j_l, i_1 \ldots i_k}, \forall i, j, \forall g \in G \end{aligned}$$

Thus, we are led to the formula in the statement, namely:

$$C_{kl} = \left\{ T \in \mathcal{L}(H^{\otimes k}, H^{\otimes l}) \middle| \exists g \in G, g_{i_1} \ldots g_{i_k} \neq g_{j_1} \ldots g_{j_l} \implies T_{j_1 \ldots j_l, i_1 \ldots i_k} = 0 \right\}$$

(4) Case $G = \mathbb{Z}_2^N$. Here the formula from (3) can be turned into something better, because due to the fact that the entries $g_1, \ldots, g_N \in \{-1, 1\}$ of a group element $g \in G$ can take all possible values, we have the following equivalence, with the symbol $\{\ \}_2$ standing for set with repetitions, with the pairs of elements of type $\{x, x\}$ removed:

$$g_{i_1} \ldots g_{i_k} = g_{j_1} \ldots g_{j_l}, \forall g \in G \iff \{i_1, \ldots, i_k\}_2 = \{j_1, \ldots, j_l\}_2$$

Thus, in this case we obtain the following formula, with $\{\ \}_2$ being as above:

$$C_{kl} = \left\{ T \in \mathcal{L}(H^{\otimes k}, H^{\otimes l}) \middle| \{i_1, \ldots, i_k\}_2 \neq \{j_1, \ldots, j_l\}_2 \implies T_{j_1 \ldots j_l, i_1 \ldots i_k} = 0 \right\}$$

Regarding now Claim 6.2, the idea is that, a bit as for $G = \mathbb{Z}_2$, we can get away with the commutation with C_{11}. Indeed, according to the above formulae, we have:

$$C_{11} = \left\{ T \in M_N(\mathbb{C}) \middle| i \neq j \implies T_{ij} = 0 \right\}$$

Thus we have $C_{11} = \Delta$, with $\Delta \subset M_N(\mathbb{C})$ being the algebra of diagonal matrices. Now if we construct $G \subset \widetilde{G} \subset O_N$ as before, we have, as desired:

$$\begin{aligned} g \in \widetilde{G} &\implies g \in C_{11}' = \Delta' = \Delta \\ &\implies g \in \Delta \cap O_N = G \end{aligned}$$

(5) Before getting into more examples, let us go back to the case where $G \subset \mathbb{Z}_2^N$ is arbitrary, and have a look at Claim 6.2 in this case. We know that we have $\{1\} \subset G \subset \mathbb{Z}_2^N$,

and by functoriality, at the level of the associated C_{11} spaces, we have:

$$\Delta \subset C_{11} \subset M_N(\mathbb{C})$$

Now construct the intermediate group $G \subset \widetilde{G} \subset O_N$ as before. For $g \in \widetilde{G}$ we have:

$$g \in C'_{11} \cap O_N \subset \Delta' \cap O_N = \Delta \cap O_N = \mathbb{Z}_2^N$$

Thus, we have $G \subset \widetilde{G} \subset \mathbb{Z}_2^N$. This looks encouraging, because our Claim 6.2 becomes now something regarding the abelian groups, that can be normally solved with group theory. However, as we will soon discover, the combinatorics can be quite complicated.

(6) General case $|G| = 2$. This is the same as saying that $G \simeq \mathbb{Z}_2$, or equivalently, that $G = \{1, g\}$ with $g \in \mathbb{Z}_2$, $g \neq 1$. By permuting the basis of $\mathbb{R}^N$ we can assume that our non-trivial group element $g \in G$ is as follows, for a certain integer $M < N$:

$$g = \begin{pmatrix} 1_M & 0 \\ 0 & -1_{N-M} \end{pmatrix}$$

By using the general formula found in (3), we obtain the following formula:

$$C_{11} = \left\{ T \in M_N(\mathbb{C}) \middle| T_{ij} = 0 \text{ when } i \leq M, j > M \text{ or } i > M, j \leq M \right\}$$

But this means that, in this case, the algebra C_{11} is block-diagonal, as follows:

$$C_{11} = \left\{ \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \middle| A \in M_M(\mathbb{C}), B \in M_{N-M}(\mathbb{C}) \right\}$$

Now since any element $h \in \widetilde{G}$ must commute with this algebra, we must have:

$$\widetilde{G} \subset \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$$

Summarizing, well done, but we are still not there. In order to finish we must use, as in (1), the relations $T = hT$ with $T \in C_{01}$. In order to do so, by using again the general formula from (3), this time with $k = 0, l = 1$, we obtain the following formula:

$$C_{01} = \left\{ T \in \mathbb{C}^N \middle| j > M \implies T_j = 0 \right\}$$

But this formula tells us that the space C_{01} appears as follows:

$$C_{01} = \left\{ \begin{pmatrix} \xi \\ 0 \end{pmatrix} \middle| \xi \in \mathbb{C}^M \right\}$$

Now since any element $h \in \widetilde{G}$ must satisfy $T = hT$, for any $T \in C_{01}$, this rules out half of the 4 solutions found above, and we end up with $\widetilde{G} = \{1, g\}$, as desired.

(7) A next step would be to investigate the case $|G| = 4$. Here we have $G = \{1, g, h, gh\}$ with $g, h \in \mathbb{Z}^2 - \{1\}$ distinct, and by permuting the basis, we can assume that:

$$g = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & -1 & \\ & & & -1 \end{pmatrix} \quad , \quad h = \begin{pmatrix} 1 & & & \\ & -1 & & \\ & & 1 & \\ & & & -1 \end{pmatrix} \quad , \quad gh = \begin{pmatrix} 1 & & & \\ & -1 & & \\ & & -1 & \\ & & & 1 \end{pmatrix}$$

However, the computations as in the proof of (6) become quite complicated, and in addition we won't get away in this case with C_{11}, C_{01} only, so all this becomes too technically involved, and we will stop here, in the lack of a better idea.

(8) Case $|G| = 2^{N-1}$. This is the last situation, announced in the statement, still having a reasonably simple direct proof, and we will discuss this now. At the level of examples, given a non-empty subset $I \subset \{1, \ldots, N\}$, we have an example, as follows:

$$G_I = \left\{ g \in \mathbb{Z}_2^N \Big| \prod_{i \in I} g_i = 1 \right\}$$

Indeed, this set $G_I \subset \mathbb{Z}_2^N$ is clearly a group, and since it is obtained by using one binary relation, namely $\prod_i g_i = \pm 1$ being assumed to be 1, the number of elements is:

$$|G_I| = \frac{|\mathbb{Z}_2^N|}{2} = \frac{2^N}{2} = 2^{N-1}$$

Our claim now is that all the index 2 subgroups $G \subset \mathbb{Z}_2^N$ appear in this way. Indeed, by taking duals these subgroups correspond to the order 2 subgroups $H \subset \mathbb{Z}_2^N$, and since we must have $H = \{1, g\}$ with $g \neq 1$, we have $2^N - 1$ choices for such subgroups. But this equals the number of choices for a non-empty subset $I \subset \{1, \ldots, N\}$, as desired.

(9) Case $|G| = 2^{N-1}$, continuation. We know from the above that we have $G = G_I$, for a certain non-empty subset $I \subset \{1, \ldots, N\}$, and we must prove Claim 6.2 for this group. In order to do so, let us go back to the formula of C_{kl} found in (4) for the group $\mathbb{Z}_2^N$. In the case of the subgroup $G_I \subset \mathbb{Z}_2^N$, which appears via the relation $\prod_i g_i = 1$, that formula adapts as follows, with the symbol $\{\ \}_{2I}$ standing for set with repetitions, with the pairs of elements of type $\{x, x\}$ removed, and with the subsets equal to I being removed too:

$$C_{kl} = \left\{ T \in \mathcal{L}(H^{\otimes k}, H^{\otimes l}) \Big| \{i_1, \ldots, i_k\}_{2I} \neq \{j_1, \ldots, j_l\}_{2I} \implies T_{j_1 \ldots j_l, i_1 \ldots i_k} = 0 \right\}$$

In order to prove now Claim 6.2 for our group, we already know from (5) that we have $\widetilde{G} \subset \mathbb{Z}_2^N$. It is also clear that, given $h \in \widetilde{G}$, when using $T = hT$ with $T \in C_{01}$, or more generally $T = h^{\otimes l} T$ with $T \in C_{0l}$ at small values of $l \in \mathbb{N}$, we won't obtain anything new. However, at $l = |I|$ we do obtain a constraint, and since this constaint must cut the target group $\mathbb{Z}_2^N$ by at least half, we end up with $G = \widetilde{G}$, as desired. □

The proof of Theorem 6.4 contains many interesting computations, that are useful in everyday life, and among the many things that can be highlighted, we have:

FACT 6.5. *The diagonal part of $C = (C_{kl})$, formed by the algebras*

$$C_{kk} = \left\{ T \in \mathcal{L}(H^{\otimes k}) \middle| Tg^{\otimes k} = g^{\otimes k}T, \forall g \in G \right\}$$

does not determine G. For instance $G = \{1\}, \mathbb{Z}_2$ are not distinguished by it.

Obviously, this is something quite annoying, because there are countless temptations to use $\Delta C = (C_{kk})$ instead of C, for instance because the spaces C_{kk} are algebras, and also, at a more advanced level, because ΔC is a planar algebra in the sense of Jones [59]. But, we are not allowed to do this, at least in general. More on this later.

What we have so far is quite interesting, and suggests further working on our problem. Unfortunately, at the other end, where $G \subset O_N$ is big, things become fairly complicated, and the only result that we can state and prove with bare hands is:

PROPOSITION 6.6. *Our Claim 6.2 holds for $G = O_N$ itself, trivially.*

PROOF. For the orthogonal group $G = O_N$ itself we have indeed $\widetilde{G} = G$, due to the inclusions $G \subset \widetilde{G} \subset O_N$. Observe however that some mystery remains for this group $G = O_N$, because the spaces C_{kl} do not look easy to compute. We will be back to this. □

As a conclusion now, we are definitely into interesting mathematics, and Claim 6.2 is definitely worth some attention, and a proof. So, time for a theorem about it:

THEOREM 6.7. *Given a closed subgroup $G \subset O_N$, we have*

$$G = \left\{ g \in O_N \middle| Tg^{\otimes k} = g^{\otimes l}T, \forall k, l, \forall T \in C_{kl} \right\}$$

where $C = (C_{kl})$ is the associated Tannakian category.

PROOF. We already know that this is something non-trivial. However, this can be proved by using either Peter-Weyl theory, or Tannakian duality, as follows:

(1) Consider, as before in Proposition 6.3 and afterwards, the following set:

$$\widetilde{G} = \left\{ g \in O_N \middle| Tg^{\otimes k} = g^{\otimes l}T, \forall k, l, \forall T \in C_{kl} \right\}$$

We know that $\widetilde{G} \subset O_N$ is a closed subgroup, and that $G \subset \widetilde{G}$. Thus, we have an intermediate subgroup as follows, that we want to prove to be equal to G itself:

$$G \subset \widetilde{G} \subset O_N$$

(2) In order to prove this, consider the Tannakian category of $\widetilde{G}$, namely:

$$\widetilde{C}_{kl} = \left\{ T \in \mathcal{L}(H^{\otimes k}, H^{\otimes l}) \middle| Tg^{\otimes k} = g^{\otimes l}T, \forall g \in \widetilde{G} \right\}$$

By functoriality, from $G \subset \widetilde{G}$ we obtain $\widetilde{C} \subset C$. On the other hand, according to the definition of $\widetilde{G}$, we have $C \subset \widetilde{C}$. Thus, we have the following equality:

$$C = \widetilde{C}$$

(3) Assume now by contradiction that $G \subset \widetilde{G}$ is not an equality. Then, at the level of algebras of functions, the following quotient map is not an isomorphism either:

$$C(\widetilde{G}) \to C(G)$$

On the other hand, we know from Peter-Weyl that we have decompositions as follows, with the sums being over all the irreducible unitary representations:

$$C(\widetilde{G}) = \overline{\bigoplus}_{\pi \in Irr(\widetilde{G})} M_{\dim \pi}(\mathbb{C}) \quad , \quad C(G) = \overline{\bigoplus}_{\nu \in Irr(G)} M_{\dim \nu}(\mathbb{C})$$

Now observe that each unitary representation $\pi : \widetilde{G} \to U_K$ restricts into a certain representation $\pi' : G \to U_K$. Since the quotient map $C(\widetilde{G}) \to C(G)$ is not an isomorphism, we conclude that there is at least one representation π satisfying:

$$\pi \in Irr(\widetilde{G}) \quad , \quad \pi' \notin Irr(G)$$

(4) We are now in position to conclude. By using Peter-Weyl theory again, the above representation $\pi \in Irr(\widetilde{G})$ appears in a certain tensor power of the fundamental representation $u : \widetilde{G} \subset U_N$. Thus, we have inclusions of representations, as follows:

$$\pi \in u^{\otimes k} \quad , \quad \pi' \in u'^{\otimes k}$$

Now since we know that π is irreducible, and that π' is not, by using one more time Peter-Weyl theory, we conclude that we have a strict inequality, as follows:

$$\dim(\widetilde{C}_{kk}) = dim(End(u^{\otimes k})) < dim(End(u'^{\otimes k})) = \dim(C_{kk})$$

But this contradicts the equality $C = \widetilde{C}$ found in (2), which finishes the proof.

(5) Alternatively, we can use Tannakian duality. This duality states that any compact group G appears as the group of endomorphisms of the canonical inclusion functor $Rep(G) \subset \mathcal{H}$, where $Rep(G)$ is the category of final dimensional continuous unitary representations of G, and $\mathcal{H}$ is the category of finite dimensional Hilbert spaces.

(6) Now in the case of a closed subgroup $G \subset_u O_N$, we know from Peter-Weyl theory that any $r \in Rep(G)$ appears as a subrepresentation $r \in u^{\otimes k}$. In categorical terms, this means that, with suitable definitions, $Rep(G)$ appears as a "completion" of the category $C = (C_{kl})$. Thus C uniquely determines G, and we obtain the result. □

All the above was of course quite brief, but we will be back to this topic, and to Tannakian duality in general, on numerous occasions, in what follows.

6b. Tensor categories

Getting started now with some more systematic theory, let us first formulate:

DEFINITION 6.8. *The Tannakian category associated to a closed subgroup $G \subset_u U_N$ is the collection $C = (C(k,l))$ of vector spaces*

$$C(k,l) = Hom(u^{\otimes k}, u^{\otimes l})$$

where the representations $u^{\otimes k}$ with $k = \circ \bullet \bullet \circ \ldots$ colored integer, defined by

$$u^{\otimes \emptyset} = 1 \quad , \quad u^{\otimes \circ} = u \quad , \quad u^{\otimes \bullet} = \bar{u}$$

and multiplicativity, $u^{\otimes kl} = u^{\otimes k} \otimes u^{\otimes l}$, are the 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:

$$u^{\otimes \circ\circ} = u \otimes u \quad , \quad u^{\otimes \circ\bullet} = u \otimes \bar{u}$$

$$u^{\otimes \bullet\circ} = \bar{u} \otimes u \quad , \quad u^{\otimes \bullet\bullet} = \bar{u} \otimes \bar{u}$$

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, which appear as:

$$Fix(u^{\otimes k}) = C(0,k)$$

Indeed, these latter spaces fully determine all the spaces $C(k,l)$, because of the Frobenius isomorphisms, which for the Peter-Weyl representations read:

$$\begin{aligned} C(k,l) &= Hom(u^{\otimes k}, u^{\otimes l}) \\ &\simeq Hom(1, \bar{u}^{\otimes k} \otimes u^{\otimes l}) \\ &= Hom(1, u^{\otimes \bar{k}l}) \\ &= Fix(u^{\otimes \bar{k}l}) \end{aligned}$$

We would like to first make a summary of what we have so far, regarding these spaces $C(k,l)$, coming from the general theory developed in chapter 5. We will need:

DEFINITION 6.9. *Let H be a finite dimensional Hilbert space. A tensor category over H is a collection $C = (C(k,l))$ of linear spaces*

$$C(k,l) \subset \mathcal{L}(H^{\otimes k}, H^{\otimes l})$$

satisfying the following conditions:

(1) *$S, T \in C$ implies $S \otimes T \in C$.*
(2) *If $S, T \in C$ are composable, then $ST \in C$.*
(3) *$T \in C$ implies $T^* \in C$.*
(4) *Each $C(k,k)$ contains the identity operator.*
(5) *$C(\emptyset, k)$ with $k = \circ\bullet, \bullet\circ$ contain the operator $R : 1 \to \sum_i e_i \otimes e_i$.*
(6) *$C(kl, lk)$ with $k, l = \circ, \bullet$ contain the flip operator $\Sigma : a \otimes b \to b \otimes a$.*

Here the tensor powers $H^{\otimes k}$, which are Hilbert spaces depending on a colored integer $k = \circ\bullet\bullet\circ\ldots$, are defined by the following formulae, and multiplicativity:

$$H^{\otimes\emptyset} = \mathbb{C} \quad , \quad H^{\otimes\circ} = H \quad , \quad H^{\otimes\bullet} = \bar{H} \simeq H$$

With these conventions, we have the following result, summarizing our knowledge on the subject, coming from the results from the previous chapter:

THEOREM 6.10. *For a closed subgroup $G \subset_u U_N$, the associated Tannakian category*

$$C(k,l) = Hom(u^{\otimes k}, u^{\otimes l})$$

is a tensor category over the Hilbert space $H = \mathbb{C}^N$.

PROOF. We know that the fundamental representation u acts on the Hilbert space $H = \mathbb{C}^N$, and that its conjugate $\bar{u}$ acts on the Hilbert space $\bar{H} = \mathbb{C}^N$. Now by multiplicativity we conclude that any Peter-Weyl representation $u^{\otimes k}$ acts on the Hilbert space $H^{\otimes k}$, so that we have embeddings as in Definition 6.9, as follows:

$$C(k,l) \subset \mathcal{L}(H^{\otimes k}, H^{\otimes l})$$

Regarding now the fact that the axioms (1-6) in Definition 6.9 are indeed satisfied, this is something that we basically already know, as follows:

(1,2,3) These results follow from definitions, and were explained in chapter 5.

(4) This is something trivial, coming from definitions.

(5) This follows from the fact that each element $g \in G$ is a unitary, which can be reformulated as follows, with $R : 1 \to \sum_i e_i \otimes e_i$ being the map in Definition 6.9:

$$R \in Hom(1, g \otimes \bar{g}) \quad , \quad R \in Hom(1, \bar{g} \otimes g)$$

Indeed, given an arbitrary matrix $g \in M_N(\mathbb{C})$, we have the following computation:

$$\begin{aligned}(g \otimes \bar{g})(R(1) \otimes 1) &= \left(\sum_{ijkl} e_{ij} \otimes e_{kl} \otimes g_{ij}\bar{g}_{kl}\right)\left(\sum_a e_a \otimes e_a \otimes 1\right)\\ &= \sum_{ika} e_i \otimes e_k \otimes g_{ia}\bar{g}^*_{ka}\\ &= \sum_{ik} e_i \otimes e_k \otimes (gg^*)_{ik}\end{aligned}$$

We conclude from this that we have the following equivalence:

$$R \in Hom(1, g \otimes \bar{g}) \iff gg^* = 1$$

By replacing g with its conjugate matrix $\bar{g}$, we have as well:

$$R \in Hom(1, \bar{g} \otimes g) \iff \bar{g}g^t = 1$$

Thus, the two intertwining conditions in Definition 6.9 (5) are both equivalent to the fact that g is unitary, and so these conditions are indeed satisfied, as desired.

(6) This is again something elementary, coming from the fact that the various matrix coefficients $g \to g_{ij}$ and their complex conjugates $g \to \bar{g}_{ij}$ commute with each other. To be more precise, with $\Sigma : a \otimes b \to b \otimes a$ being the flip operator, we have:

$$\begin{aligned}(g \otimes h)(\Sigma \otimes id)(e_a \otimes e_b \otimes 1) &= \left(\sum_{ijkl} e_{ij} \otimes e_{kl} \otimes g_{ij}h_{kl}\right)(e_b \otimes e_a \otimes 1)\\ &= \sum_{ik} e_i \otimes e_k \otimes g_{ib}h_{ka}\end{aligned}$$

On the other hand, we have as well the following computation:

$$\begin{aligned}(\Sigma \otimes id)(h \otimes g)(e_a \otimes e_b \otimes 1) &= (\Sigma \otimes id)\left(\sum_{ijkl} e_{ij} \otimes e_{kl} \otimes h_{ij}g_{kl}\right)(e_a \otimes e_b \otimes 1)\\ &= (\Sigma \otimes id)\left(\sum_{ik} e_i \otimes e_k \otimes h_{ia}g_{kb}\right)\\ &= \sum_{ik} e_k \otimes e_i \otimes h_{ia}g_{kb}\\ &= \sum_{ik} e_i \otimes e_k \otimes h_{ka}g_{ib}\end{aligned}$$

Now since functions commute, $g_{ib}h_{ka} = h_{ka}g_{ib}$, this gives the result. □

With the above in hand, our purpose now will be that of showing that any closed subgroup $G \subset U_N$ is uniquely determined by its Tannakian category $C = (C(k, l))$:

$$G \leftrightarrow C$$

This result, known as Tannakian duality, is something quite deep, and very useful. Indeed, the idea is that what we would have here is a "linearization" of G, allowing us to do combinatorics, and ultimately reach to very concrete and powerful results, regarding G itself. And as a consequence, solve our probability questions left.

Getting started now, we want to construct a correspondence $G \leftrightarrow C$, and we already know from Theorem 6.10 how the correspondence $G \to C$ appears, namely via:

$$C(k, l) = Hom(u^{\otimes k}, u^{\otimes l})$$

Regarding now the construction in the other sense, $C \to G$, this is something very simple as well, coming from the following elementary result:

THEOREM 6.11. *Given a tensor category $C = (C(k,l))$ over the space $H \simeq \mathbb{C}^N$,*

$$G = \left\{ g \in U_N \middle| Tg^{\otimes k} = g^{\otimes l}T \ , \ \forall k,l, \forall T \in C(k,l) \right\}$$

is a closed subgroup $G \subset U_N$.

PROOF. Consider indeed the closed subset $G \subset U_N$ constructed in the statement. We want to prove that G is indeed a group, and the verifications here go as follows:

(1) Given two matrices $g, h \in G$, their product satisfies $gh \in G$, due to the following computation, valid for any k, l and any $T \in C(k,l)$:

$$\begin{aligned} T(gh)^{\otimes k} &= Tg^{\otimes k}h^{\otimes k} \\ &= g^{\otimes l}Th^{\otimes k} \\ &= g^{\otimes l}h^{\otimes l}T \\ &= (gh)^{\otimes l}T \end{aligned}$$

(2) Also, we have $1 \in G$, trivially. Finally, for $g \in G$ and $T \in C(k,l)$, we have:

$$\begin{aligned} T(g^{-1})^{\otimes k} &= (g^{-1})^{\otimes l}[g^{\otimes l}T](g^{-1})^{\otimes k} \\ &= (g^{-1})^{\otimes l}[Tg^{\otimes k}](g^{-1})^{\otimes k} \\ &= (g^{-1})^{\otimes l}T \end{aligned}$$

Thus we have $g^{-1} \in G$, and so G is a group, as claimed. □

Summarizing, we have so far precise axioms for the tensor categories $C = (C(k,l))$, given in Definition 6.9, as well as correspondences as follows:

$$G \to C \quad , \quad C \to G$$

We will show in what follows that these correspondences are inverse to each other. In order to get started, we first have the following technical result:

THEOREM 6.12. *If we denote the correspondences in Theorem 6.9 and 6.10, between closed subgroups $G \subset U_N$ and tensor categories $C = (C(k,l))$ over $H = \mathbb{C}^N$, as*

$$G \to C_G \quad , \quad C \to G_C$$

then we have embeddings as follows, for any G and C respectively,

$$G \subset G_{C_G} \quad , \quad C \subset C_{G_C}$$

and proving that these correspondences are inverse to each other amounts in proving

$$C_{G_C} \subset C$$

for any tensor category $C = (C(k,l))$ over the space $H = \mathbb{C}^N$.

PROOF. This is something trivial, with the embeddings $G \subset G_{C_G}$ and $C \subset C_{G_C}$ being both clear from definitions, and with the last assertion coming from this. □

In order to establish Tannakian duality, we will need some abstract constructions. Following Malacarne [72], let us start with the following elementary fact:

PROPOSITION 6.13. *Given a tensor category $C = C((k,l))$ over a Hilbert space H,*

$$E_C = \bigoplus_{k,l} C(k,l) \subset \bigoplus_{k,l} B(H^{\otimes k}, H^{\otimes l}) \subset B\left(\bigoplus_k H^{\otimes k}\right)$$

is a closed $*$-subalgebra. Also, inside this algebra,

$$E_C^{(s)} = \bigoplus_{|k|,|l|\leq s} C(k,l) \subset \bigoplus_{|k|,|l|\leq s} B(H^{\otimes k}, H^{\otimes l}) = B\left(\bigoplus_{|k|\leq s} H^{\otimes k}\right)$$

is a finite dimensional $*$-subalgebra.

PROOF. This is clear indeed from the categorical axioms from Definition 6.9. □

Now back to our reconstruction question, we want to prove $C = C_{G_C}$, which is the same as proving $E_C = E_{C_{G_C}}$. We will use a standard commutant trick, as follows:

THEOREM 6.14. *For any $*$-algebra $A \subset M_N(\mathbb{C})$ we have the equality*

$$A = A''$$

where prime denotes the commutant, $X' = \big\{T \in M_N(\mathbb{C}) \big| Tx = xT, \forall x \in X\big\}$.

PROOF. This is a particular case of von Neumann's bicommutant theorem, which follows from the explicit description of A worked out in chapter 4, namely:

$$A = M_{n_1}(\mathbb{C}) \oplus \ldots \oplus M_{n_k}(\mathbb{C})$$

Indeed, the center of each matrix algebra being reduced to the scalars, the commutant of this algebra is as follows, with each copy of $\mathbb{C}$ corresponding to a matrix block:

$$A' = \mathbb{C} \oplus \ldots \oplus \mathbb{C}$$

Now when taking once again the commutant, the computation is trivial, and we obtain in this way A itself, and this leads to the conclusion in the statement. □

By using now the bicommutant theorem, we have:

PROPOSITION 6.15. *Given a Tannakian category C, the following are equivalent:*

(1) $C = C_{G_C}$.
(2) $E_C = E_{C_{G_C}}$.
(3) $E_C^{(s)} = E_{C_{G_C}}^{(s)}$, *for any* $s \in \mathbb{N}$.
(4) $E_C^{(s)'} = E_{C_{G_C}}^{(s)'}$, *for any* $s \in \mathbb{N}$.

In addition, the inclusions $\subset$, $\subset$, $\subset$, $\supset$ are automatically satisfied.

PROOF. This follows from the above results, as follows:

(1) $\iff$ (2) This is clear from definitions.

(2) $\iff$ (3) This is clear from definitions as well.

(3) $\iff$ (4) This comes from the bicommutant theorem. As for the last assertion, we have indeed $C \subset C_{G_C}$ from Theorem 6.12, and this shows that we have as well:

$$E_C \subset E_{C_{G_C}}$$

We therefore obtain by truncating $E_C^{(s)} \subset E_{C_{G_C}}^{(s)}$, and by taking the commutants, this gives $E_C^{(s)} \supset E_{C_{G_C}}^{(s)}$. Thus, we are led to the conclusion in the statement. □

Summarizing, we would like to prove that we have $E_C^{(s)'} \subset E_{C_{G_C}}^{(s)'}$. Let us first study the commutant on the right. As a first observation, we have:

PROPOSITION 6.16. *We have the following equality,*

$$E_{C_G}^{(s)} = End\left(\bigoplus_{|k|\leq s} u^{\otimes k}\right)$$

between subalgebras of $B\left(\bigoplus_{|k|\leq s} H^{\otimes k}\right)$.

PROOF. We know that the category C_G is by definition given by:

$$C_G(k,l) = Hom(u^{\otimes k}, u^{\otimes l})$$

Thus, the corresponding algebra $E_{C_G}^{(s)}$ appears as follows:

$$E_{C_G}^{(s)} = \bigoplus_{|k|,|l|\leq s} Hom(u^{\otimes k}, u^{\otimes l}) \subset \bigoplus_{|k|,|l|\leq s} B(H^{\otimes k}, H^{\otimes l}) = B\left(\bigoplus_{|k|\leq s} H^{\otimes k}\right)$$

On the other hand, the algebra of intertwiners of $\bigoplus_{|k|\leq s} u^{\otimes k}$ is given by:

$$End\left(\bigoplus_{|k|\leq s} u^{\otimes k}\right) = \bigoplus_{|k|,|l|\leq s} Hom(u^{\otimes k}, u^{\otimes l}) \subset \bigoplus_{|k|,|l|\leq s} B(H^{\otimes k}, H^{\otimes l}) = B\left(\bigoplus_{|k|\leq s} H^{\otimes k}\right)$$

Thus we have indeed the same algebra, and we are done. □

We have to compute the commutant of the above algebra. For this purpose, we can use the following general result, valid for any representation of a compact group:

PROPOSITION 6.17. *Given a unitary group representation $v : G \to U_n$ we have an algebra representation as follows,*

$$\pi_v : C(G)^* \to M_n(\mathbb{C}) \quad , \quad \varphi \to (\varphi(v_{ij}))_{ij}$$

whose image is given by $Im(\pi_v) = End(v)'$.

PROOF. The first assertion is clear, with the multiplicativity claim for π_v coming from the following computation, where $\Delta : C(G) \to C(G) \otimes C(G)$ is the comultiplication:

$$\begin{aligned}(\pi_v(\varphi * \psi))_{ij} &= (\varphi \otimes \psi)\Delta(v_{ij}) \\ &= \sum_k \varphi(v_{ik})\psi(v_{kj}) \\ &= \sum_k (\pi_v(\varphi))_{ik}(\pi_v(\psi))_{kj} \\ &= (\pi_v(\varphi)\pi_v(\psi))_{ij}\end{aligned}$$

Let us establish now the equality in the statement, namely:

$$Im(\pi_v) = End(v)'$$

Let us first prove the inclusion $\subset$. Given $\varphi \in C(G)^*$ and $T \in End(v)$, we have:

$$\begin{aligned}[\pi_v(\varphi), T] = 0 &\iff \sum_k \varphi(v_{ik})T_{kj} = \sum_k T_{ik}\varphi(v_{kj}), \forall i, j \\ &\iff \varphi\left(\sum_k v_{ik}T_{kj}\right) = \varphi\left(\sum_k T_{ik}v_{kj}\right), \forall i, j \\ &\iff \varphi((vT)_{ij}) = \varphi((Tv)_{ij}), \forall i, j\end{aligned}$$

But this latter formula is true, because $T \in End(v)$ means that we have:

$$vT = Tv$$

As for the converse inclusion $\supset$, the proof is quite similar. Indeed, by using the bicommutant theorem, this is the same as proving that we have:

$$Im(\pi_v)' \subset End(v)$$

But, by using the above equivalences, we have the following computation:

$$\begin{aligned}T \in Im(\pi_v)' &\iff [\pi_v(\varphi), T] = 0, \forall \varphi \\ &\iff \varphi((vT)_{ij}) = \varphi((Tv)_{ij}), \forall \varphi, i, j \\ &\iff vT = Tv\end{aligned}$$

Thus, we have obtained the desired inclusion, and we are done. □

By combining the above results, we obtain the following technical statement:

THEOREM 6.18. *We have the following equality,*

$$E_{C_G}^{(s)'} = Im(\pi_v)$$

where the representation v is the following direct sum,

$$v = \bigoplus_{|k|\leq s} u^{\otimes k}$$

and where the algebra representation $\pi_v : C(G)^* \to M_n(\mathbb{C})$ is given by $\varphi \to (\varphi(v_{ij}))_{ij}$.

PROOF. This follows indeed by combining the above results, and more precisely by combining Proposition 6.16 and Proposition 6.17. □

6c. The correspondence

We recall that we want to prove that we have $E_C^{(s)'} \subset E_{C_{G_C}}^{(s)'}$, for any $s \in \mathbb{N}$. And for this purpose, we must first refine Theorem 6.18, in the case $G = G_C$.

Generally speaking, in order to prove anything about G_C, we are in need of an explicit model for this group. In order to construct such a model, let $< u_{ij} >$ be the free $*$-algebra over $\dim(H)^2$ variables, with comultiplication and counit as follows:

$$\Delta(u_{ij}) = \sum_k u_{ik} \otimes u_{kj} \quad , \quad \varepsilon(u_{ij}) = \delta_{ij}$$

Following [72], we can model this $*$-bialgebra, in the following way:

PROPOSITION 6.19. *Consider the following pair of dual vector spaces,*

$$F = \bigoplus_k B\left(H^{\otimes k}\right) \quad , \quad F^* = \bigoplus_k B\left(H^{\otimes k}\right)^*$$

and let $f_{ij}, f_{ij}^* \in F^*$ be the standard generators of $B(H)^*, B(\bar{H})^*$.

(1) *F^* is a $*$-algebra, with multiplication $\otimes$ and involution as follows:*

$$f_{ij} \leftrightarrow f_{ij}^*$$

(2) *F^* is a $*$-bialgebra, with $*$-bialgebra operations as follows:*

$$\Delta(f_{ij}) = \sum_k f_{ik} \otimes f_{kj} \quad , \quad \varepsilon(f_{ij}) = \delta_{ij}$$

(3) *We have a $*$-bialgebra isomorphism $< u_{ij} > \simeq F^*$, given by $u_{ij} \to f_{ij}$.*

PROOF. Since F^* is spanned by the various tensor products between the variables f_{ij}, f_{ij}^*, we have a vector space isomorphism as follows:

$$< u_{ij} > \simeq F^* \quad , \quad u_{ij} \to f_{ij} \quad , \quad u_{ij}^* \to f_{ij}^*$$

The corresponding $*$-bialgebra structure induced on the vector space F^* is then the one in the statement, and this gives the result. □

Now back to our group G_C, we have the following modeling result for it:

PROPOSITION 6.20. *The smooth part of the algebra $A_C = C(G_C)$ is given by*

$$\mathcal{A}_C \simeq F^*/J$$

where $J \subset F^*$ is the ideal coming from the following relations, for any i, j,

$$\sum_{p_1,\ldots,p_k} T_{i_1\ldots i_l,p_1\ldots p_k} f_{p_1 j_1} \otimes \ldots \otimes f_{p_k j_k} = \sum_{q_1,\ldots,q_l} T_{q_1\ldots q_l,j_1\ldots j_k} f_{i_1 q_1} \otimes \ldots \otimes f_{i_l q_l}$$

one for each pair of colored integers k, l, and each $T \in C(k, l)$.

PROOF. As a first observation, A_C appears as enveloping C^*-algebra of the following universal $*$-algebra, where $u = (u_{ij})$ is regarded as a formal corepresentation:

$$\mathcal{A}_C = \left\langle (u_{ij})_{i,j=1,\ldots,N} \middle| T \in Hom(u^{\otimes k}, u^{\otimes l}), \forall k, l, \forall T \in C(k, l) \right\rangle$$

With this observation in hand, the conclusion is that we have a formula as follows, where I is the ideal coming from the relations $T \in Hom(u^{\otimes k}, u^{\otimes l})$, with $T \in C(k, l)$:

$$\mathcal{A}_C = < u_{ij} > /I$$

Now if we denote by $J \subset F^*$ the image of the ideal I via the $*$-algebra isomorphism $< u_{ij} > \simeq F^*$ from Proposition 6.22, we obtain an identification as follows:

$$\mathcal{A}_C \simeq F^*/J$$

With standard multi-index notations, and by assuming now that $k, l \in \mathbb{N}$ are usual integers, for simplifying the presentation, the general case being similar, a relation of type $T \in Hom(u^{\otimes k}, u^{\otimes l})$ inside $< u_{ij} >$ is equivalent to the following conditions:

$$\sum_{p_1,\ldots,p_k} T_{i_1\ldots i_l,p_1\ldots p_k} u_{p_1 j_1} \ldots u_{p_k j_k} = \sum_{q_1,\ldots,q_l} T_{q_1\ldots q_l,j_1\ldots j_k} u_{i_1 q_1} \ldots u_{i_l q_l}$$

Now by recalling that the isomorphism of $*$-algebras $< u_{ij} > \to F^*$ is given by $u_{ij} \to f_{ij}$, and that the multiplication operation of F^* corresponds to the tensor product operation $\otimes$, we conclude that $J \subset F^*$ is the ideal from the statement. □

With the above result in hand, let us go back to Theorem 6.18. We have:

PROPOSITION 6.21. *The linear space $\mathcal{A}_C^*$ is given by the formula*

$$\mathcal{A}_C^* = \left\{ a \in F \middle| Ta_k = a_l T, \forall T \in C(k, l) \right\}$$

and the representation

$$\pi_v : \mathcal{A}_C^* \to B\left(\bigoplus_{|k| \leq s} H^{\otimes k} \right)$$

appears diagonally, by truncating, $\pi_v : a \to (a_k)_{kk}$.

PROOF. We know from Proposition 6.20 that we have an identification of $*$-bialgebras $\mathcal{A}_C \simeq F^*/J$. But this gives a quotient map, as follows:

$$F^* \to \mathcal{A}_C$$

At the dual level, this gives $\mathcal{A}_C^* \subset F$. To be more precise, we have:

$$\mathcal{A}_C^* = \left\{ a \in F \middle| f(a) = 0, \forall f \in J \right\}$$

Now since $J =< f_T >$, where f_T are the relations in Proposition 6.20, we obtain:

$$\mathcal{A}_C^* = \left\{ a \in F \middle| f_T(a) = 0, \forall T \in C \right\}$$

Given $T \in C(k,l)$, for an arbitrary element $a = (a_k)$, we have:

$$\begin{aligned}
& f_T(a) = 0 \\
\iff & \sum_{p_1,\ldots,p_k} T_{i_1\ldots i_l,p_1\ldots p_k}(a_k)_{p_1\ldots p_k,j_1\ldots j_k} = \sum_{q_1,\ldots,q_l} T_{q_1\ldots q_l,j_1\ldots j_k}(a_l)_{i_1\ldots i_l,q_1\ldots q_l}, \forall i,j \\
\iff & (Ta_k)_{i_1\ldots i_l,j_1\ldots j_k} = (a_l T)_{i_1\ldots i_l,j_1\ldots j_k}, \forall i,j \\
\iff & Ta_k = a_l T
\end{aligned}$$

Thus, $\mathcal{A}_C^*$ is given by the formula in the statement. It remains to compute π_v:

$$\pi_v : \mathcal{A}_C^* \to B\left(\bigoplus_{|k|\leq s} H^{\otimes k}\right)$$

With $a = (a_k)$, we have the following computation:

$$\begin{aligned}
\pi_v(a)_{i_1\ldots i_k,j_1\ldots j_k} &= a(v_{i_1\ldots i_k,j_1\ldots j_k}) \\
&= (f_{i_1j_1} \otimes \ldots \otimes f_{i_kj_k})(a) \\
&= (a_k)_{i_1\ldots i_k,j_1\ldots j_k}
\end{aligned}$$

Thus, our representation π_v appears diagonally, by truncating, as claimed. □

In order to further advance, consider the following vector spaces:

$$F_s = \bigoplus_{|k|\leq s} B\left(H^{\otimes k}\right) \quad , \quad F_s^* = \bigoplus_{|k|\leq s} B\left(H^{\otimes k}\right)^*$$

We denote by $a \to a_s$ the truncation operation $F \to F_s$. We have:

PROPOSITION 6.22. *The following hold:*

(1) $E_C^{(s)'} \subset F_s$.
(2) $E_C' \subset F$.
(3) $\mathcal{A}_C^* = E_C'$.
(4) $Im(\pi_v) = (E_C')_s$.

PROOF. These results basically follow from what we have, as follows:

(1) We have an inclusion as follows, as a diagonal subalgebra:

$$F_s \subset B\left(\bigoplus_{|k|\leq s} H^{\otimes k}\right)$$

The commutant of this algebra is then given by:

$$F_s' = \left\{b \in F_s \middle| b = (b_k), b_k \in \mathbb{C}, \forall k\right\}$$

On the other hand, we know from the identity axiom for the category C that we have $F_s' \subset E_C^{(s)}$. Thus, our result follows from the bicommutant theorem, as follows:

$$F_s' \subset E_C^{(s)} \implies F_s \supset E_C^{(s)'}$$

(2) This follows from (1), by taking inductive limits.

(3) With the present notations, the formula of $\mathcal{A}_C^*$ from Proposition 6.21 reads $\mathcal{A}_C^* = F \cap E_C'$. Now since by (2) we have $E_C' \subset F$, we obtain from this $\mathcal{A}_C^* = E_C'$.

(4) This follows from (3), and from the formula of π_ν in Proposition 6.21. □

Following [72], we can now state and prove our main result, as follows:

THEOREM 6.23. *The Tannakian duality constructions*

$$C \to G_C \quad , \quad G \to C_G$$

are inverse to each other.

PROOF. According to our various results above, we have to prove that, for any Tannakian category C, and any $s \in \mathbb{N}$, we have an inclusion as follows:

$$E_C^{(s)'} \subset (E_C')_s$$

By taking duals, this is the same as proving that we have:

$$\left\{f \in F_s^* \middle| f_{|(E_C')_s} = 0\right\} \subset \left\{f \in F_s^* \middle| f_{|E_C^{(s)'}} = 0\right\}$$

In order to do so, we use the following formula, from Proposition 6.22:

$$\mathcal{A}_C^* = E_C'$$

We know from the above that we have an identification as follows:

$$\mathcal{A}_C = F^*/J$$

We conclude that the ideal J is given by the following formula:

$$J = \left\{f \in F^* \middle| f_{|E_C'} = 0\right\}$$

Our claim is that we have the following formula, for any $s \in \mathbb{N}$:

$$J \cap F_s^* = \left\{ f \in F_s^* \middle| f_{|E_C^{(s)\prime}} = 0 \right\}$$

Indeed, let us denote by X_s the spaces on the right. The axioms for C show that these spaces are increasing, that their union $X = \cup_s X_s$ is an ideal, and that:

$$X_s = X \cap F_s^*$$

We must prove that we have $J = X$, and this can be done as follows:

"$\subset$" This follows from the following fact, for any $T \in C(k,l)$ with $|k|, |l| \leq s$:

$$\begin{aligned} (f_T)_{|\{T\}'} = 0 &\implies (f_T)_{|E_C^{(s)\prime}} = 0 \\ &\implies f_T \in X_s \end{aligned}$$

"$\supset$" This follows from our description of J, because from $E_C^{(s)} \subset E_C$ we obtain:

$$f_{|E_C^{(s)\prime}} = 0 \implies f_{|E_C'} = 0$$

Summarizing, we have proved our claim. On the other hand, we have:

$$\begin{aligned} J \cap F_s^* &= \left\{ f \in F^* \middle| f_{|E_C'} = 0 \right\} \cap F_s^* \\ &= \left\{ f \in F_s^* \middle| f_{|E_C'} = 0 \right\} \\ &= \left\{ f \in F_s^* \middle| f_{|(E_C')_s} = 0 \right\} \end{aligned}$$

Thus, our claim is exactly the inclusion that we wanted to prove, and we are done. □

6d. Brauer theorems

Time for some applications. Let us start with the following definition:

DEFINITION 6.24. *Given a pairing $\pi \in P_2(k,l)$ and an integer $N \in \mathbb{N}$, we can construct a linear map between tensor powers of $\mathbb{C}^N$,*

$$T_\pi : (\mathbb{C}^N)^{\otimes k} \to (\mathbb{C}^N)^{\otimes l}$$

by the following formula, with $e_1, \ldots, e_N$ being the standard basis of $\mathbb{C}^N$,

$$T_\pi(e_{i_1} \otimes \ldots \otimes e_{i_k}) = \sum_{j_1 \ldots j_l} \delta_\pi \begin{pmatrix} i_1 & \ldots & i_k \\ j_1 & \ldots & j_l \end{pmatrix} e_{j_1} \otimes \ldots \otimes e_{j_l}$$

and with the coefficients on the right being Kronecker type symbols,

$$\delta_\pi \begin{pmatrix} i_1 & \ldots & i_k \\ j_1 & \ldots & j_l \end{pmatrix} \in \{0, 1\}$$

whose values depend on whether the indices fit or not.

To be more precise here, we put the multi-indices $i = (i_1, \ldots, i_k)$ and $j = (j_1, \ldots, j_l)$ on the legs of our pairing π, in the obvious way. In the case where all strings of π join pairs of equal indices of i, j, we set $\delta_\pi\binom{i}{j} = 1$. Otherwise, we set $\delta_\pi\binom{i}{j} = 0$.

The point with the above definition comes from the fact that most of the "familiar" maps, in the Tannakian context, are of the above form. Here are some examples:

PROPOSITION 6.25. *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) $T_\chi = (e_a \otimes e_b \to e_b \otimes e_a)$.

PROOF. We can assume that all legs of π are colored $\circ$, and then:

(1) We have $\cap \in P_2(\emptyset, \circ\circ)$, and $T_\cap : \mathbb{C} \to \mathbb{C}^N \otimes \mathbb{C}^N$ can be computed as follows:

$$\begin{aligned} T_\cap(1) &= \sum_{ij} \delta_\cap(i\ j) e_i \otimes e_j \\ &= \sum_{ij} \delta_{ij} e_i \otimes e_j \\ &= \sum_i e_i \otimes e_i \end{aligned}$$

(2) Here we have $\cup \in P_2(\circ\circ, \emptyset)$, and the map $T_\cap : \mathbb{C}^N \otimes \mathbb{C}^N \to \mathbb{C}$ is given by:

$$T_\cap(e_i \otimes e_j) = \delta_\cap(i\ j) = \delta_{ij}$$

(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:

$$\begin{aligned} T_{||\ldots||}(e_{i_1} \otimes \ldots \otimes e_{i_k}) &= \sum_{j_1\ldots j_k} \delta_{||\ldots||} \begin{pmatrix} i_1 & \ldots & i_k \\ j_1 & \ldots & j_k \end{pmatrix} e_{j_1} \otimes \ldots \otimes e_{j_k} \\ &= \sum_{j_1\ldots j_k} \delta_{i_1 j_1} \ldots \delta_{i_k j_k} e_{j_1} \otimes \ldots \otimes e_{j_k} \\ &= e_{i_1} \otimes \ldots \otimes e_{i_k} \end{aligned}$$

(4) For the basic crossing $\chi \in P_2(\circ\circ, \circ\circ)$, the corresponding linear map is as follows:

$$T_\chi : \mathbb{C}^N \otimes \mathbb{C}^N \to \mathbb{C}^N \otimes \mathbb{C}^N$$

This linear map can be computed as follows:

$$\begin{aligned} T_\chi(e_i\otimes e_j) &= \sum_{kl}\delta_\chi\begin{pmatrix}i&j\\k&l\end{pmatrix}e_k\otimes e_l\\ &= \sum_{kl}\delta_{il}\delta_{jk}e_k\otimes e_l\\ &= e_j\otimes e_i\end{aligned}$$

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 key result:

PROPOSITION 6.26. *The assignement $\pi\to T_\pi$ is categorical, in the sense that*

$$T_\pi\otimes T_\sigma=T_{[\pi\sigma]}\quad,\quad T_\pi T_\sigma=N^{c(\pi,\sigma)}T_{[\frac{\sigma}{\pi}]}\quad,\quad T_\pi^*=T_{\pi^*}$$

where $c(\pi,\sigma)$ is the number of circles appearing in the middle, when concatenating.

PROOF. The concatenation axiom follows from the following computation:

$$\begin{aligned} &(T_\pi\otimes T_\sigma)(e_{i_1}\otimes\ldots\otimes e_{i_p}\otimes e_{k_1}\otimes\ldots\otimes e_{k_r})\\ =\ &\sum_{j_1\ldots j_q}\sum_{l_1\ldots l_s}\delta_\pi\begin{pmatrix}i_1&\ldots&i_p\\j_1&\ldots&j_q\end{pmatrix}\delta_\sigma\begin{pmatrix}k_1&\ldots&k_r\\l_1&\ldots&l_s\end{pmatrix}e_{j_1}\otimes\ldots\otimes e_{j_q}\otimes e_{l_1}\otimes\ldots\otimes e_{l_s}\\ =\ &\sum_{j_1\ldots j_q}\sum_{l_1\ldots l_s}\delta_{[\pi\sigma]}\begin{pmatrix}i_1&\ldots&i_p&k_1&\ldots&k_r\\j_1&\ldots&j_q&l_1&\ldots&l_s\end{pmatrix}e_{j_1}\otimes\ldots\otimes e_{j_q}\otimes e_{l_1}\otimes\ldots\otimes e_{l_s}\\ =\ &T_{[\pi\sigma]}(e_{i_1}\otimes\ldots\otimes e_{i_p}\otimes e_{k_1}\otimes\ldots\otimes e_{k_r})\end{aligned}$$

The composition axiom follows from the following computation:

$$\begin{aligned} &T_\pi T_\sigma(e_{i_1}\otimes\ldots\otimes e_{i_p})\\ =\ &\sum_{j_1\ldots j_q}\delta_\sigma\begin{pmatrix}i_1&\ldots&i_p\\j_1&\ldots&j_q\end{pmatrix}\sum_{k_1\ldots k_r}\delta_\pi\begin{pmatrix}j_1&\ldots&j_q\\k_1&\ldots&k_r\end{pmatrix}e_{k_1}\otimes\ldots\otimes e_{k_r}\\ =\ &\sum_{k_1\ldots k_r}N^{c(\pi,\sigma)}\delta_{[\frac{\sigma}{\pi}]}\begin{pmatrix}i_1&\ldots&i_p\\k_1&\ldots&k_r\end{pmatrix}e_{k_1}\otimes\ldots\otimes e_{k_r}\\ =\ &N^{c(\pi,\sigma)}T_{[\frac{\sigma}{\pi}]}(e_{i_1}\otimes\ldots\otimes e_{i_p})\end{aligned}$$

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. □

The above result suggests the following general definition:

DEFINITION 6.27. *Let $P_2(k,l)$ be the set of pairings between an upper colored integer k, and a lower colored integer l. A collection of subsets*

$$D=\bigsqcup_{k,l}D(k,l)$$

with $D(k,l)\subset P_2(k,l)$ is called a category of pairings when it has the following properties:

(1) *Stability under the horizontal concatenation, $(\pi,\sigma)\to[\pi\sigma]$.*
(2) *Stability under vertical concatenation $(\pi,\sigma)\to\left[\begin{smallmatrix}\sigma\\\pi\end{smallmatrix}\right]$, 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 $P(\emptyset,\bullet\circ)$ both contain the semicircle $\cap$.*
(6) *The sets $P(k,\bar{k})$ with $|k|=2$ contain the crossing partition $\diagdown\!\!\diagup$.*

Observe the similarity with the axioms for Tannakian categories, given earlier in this chapter. In relation with the compact groups, we have the following result:

THEOREM 6.28. *Each category of pairings, in the above sense,*

$$D=(D(k,l))$$

produces a family of compact groups $G=(G_N)$, one for each $N\in\mathbb{N}$, via the formula

$$Hom(u^{\otimes k},u^{\otimes l})=span\left(T_\pi\middle|\pi\in D(k,l)\right)$$

and the Tannakian duality correspondence.

PROOF. Given an integer $N\in\mathbb{N}$, consider the correspondence $\pi\to T_\pi$ constructed in Definition 6.24, and then the collection of linear spaces in the statement, namely:

$$C_{kl}=span\left(T_\pi\middle|\pi\in D(k,l)\right)$$

According to Proposition 6.26, and to our axioms for the categories of partitions, from Definition 6.27, this collection of spaces $C=(C_{kl})$ satisfies the axioms for the Tannakian

categories, from the beginning of this chapter. Thus the Tannakian duality result there applies, and provides us with a closed subgroup $G_N \subset U_N$ such that:

$$C_{kl} = Hom(u^{\otimes k}, u^{\otimes l})$$

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

We can establish now a useful result, namely the Brauer theorem for U_N:

THEOREM 6.29. *For the unitary group U_N we have*

$$Hom(u^{\otimes k}, u^{\otimes l}) = span\left(T_\pi \middle| \pi \in \mathcal{P}_2(k,l)\right)$$

where $\mathcal{P}_2$ denotes as usual the category of all matching pairings.

PROOF. Consider the spaces on the right in the statement, namely:

$$C_{kl} = span\left(T_\pi \middle| \pi \in \mathcal{P}_2(k,l)\right)$$

According to Proposition 6.26 these spaces form a tensor category. Thus, by Tannakian duality, these spaces must come from a certain closed subgroup $G \subset U_N$. To be more precise, if we denote by v the fundamental representation of G, then:

$$C_{kl} = Hom(v^{\otimes k}, v^{\otimes l})$$

We must prove that we have $G = U_N$. For this purpose, let us recall that the unitary group U_N is defined via the following relations:

$$u^* = u^{-1} \quad , \quad u^t = \bar{u}^{-1}$$

But these relations tell us precisely that the following two operators must be in the associated Tannakian category C:

$$T_\pi \quad : \quad \pi = \ \overset{\cap}{\circ\bullet} \ , \ \overset{\cap}{\bullet\circ}$$

Thus the associated Tannakian category is $C = span(T_\pi | \pi \in D)$, with:

$$D = < \ \overset{\cap}{\circ\bullet} \ , \ \overset{\cap}{\bullet\circ} > = \mathcal{P}_2$$

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

Regarding the orthogonal group O_N, we have here a similar result, as follows:

THEOREM 6.30. *For the orthogonal group O_N we have*

$$Hom(u^{\otimes k}, u^{\otimes l}) = span\left(T_\pi \middle| \pi \in P_2(k,l)\right)$$

where P_2 denotes as usual the category of all pairings.

PROOF. Consider the spaces on the right in the statement, namely:

$$C_{kl} = span\left(T_\pi \middle| \pi \in P_2(k,l)\right)$$

According to Proposition 6.26 these spaces form a tensor category. Thus, by Tannakian duality, these spaces must come from a certain closed subgroup $G \subset U_N$. To be more precise, if we denote by v the fundamental representation of G, then:

$$C_{kl} = Hom(v^{\otimes k}, v^{\otimes l})$$

We must prove that we have $G = O_N$. For this purpose, let us recall that the orthogonal group $O_N \subset U_N$ is defined by imposing the following relations:

$$u_{ij} = \bar{u}_{ij}$$

But these relations tell us precisely that the following two operators must be in the associated Tannakian category C:

$$T_\pi \quad : \quad \pi = \; \circ\!\!\updownarrow\!\!\bullet \; , \; \bullet\!\!\updownarrow\!\!\circ$$

Thus the associated Tannakian category is $C = span(T_\pi | \pi \in D)$, with:

$$D = < \mathcal{P}_2, \circ\!\!\updownarrow\!\!\bullet, \bullet\!\!\updownarrow\!\!\circ > = P_2$$

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

6e. Exercises

Exercises:

EXERCISE 6.31.

EXERCISE 6.32.

EXERCISE 6.33.

EXERCISE 6.34.

EXERCISE 6.35.

EXERCISE 6.36.

EXERCISE 6.37.

EXERCISE 6.38.

Bonus exercise.

CHAPTER 7

Diagrams, easiness

7a. Easy groups

We have seen in the previous chapter that the Tannakian duals of the groups O_N, U_N are very simple objects. To be more precise, the Brauer theorem for these two groups states that we have equalities as follows, with $D = P_2, \mathcal{P}_2$ respectively:

$$Hom(u^{\otimes k}, u^{\otimes l}) = span\left(T_\pi \middle| \pi \in D(k,l)\right)$$

Our goal here will be that of axiomatizing and studying the closed subgroups $G \subset U_N$ which are of this type, but with D being allowed to be, more generally, a category of partitions. We will call such groups "easy", and our results will be as follows:

(1) At the level of the continuous examples, we will see that besides O_N, U_N, we have the bistochastic groups B_N, C_N. This is something which is interesting, and also instructive, making it clear why we have to upgrade, from pairings to partitions.

(2) At the level of discrete examples, we have none so far, but we will see that the symmetric group S_N, the hyperoctahedral group H_N, and more generally the complex reflection groups H_N^s with $s \in \mathbb{N} \cup \{\infty\}$, are all easy, in the above generalized sense.

(3) Still at the level of the basic examples, some key Lie groups such as SU_2, SO_3, or the symplectic group Sp_N, are not easy, but the point is that these are however covered by a suitable "super-easiness" version of the easiness, as defined above.

(4) At the level of the general theory, we will develop some algebraic theory in this chapter, for the most in relation with various product operations, the idea being that in the easy case, everything eventually reduces to computations with partitions.

(5) Also at the level of the general theory, we will develop as well some analytic theory, later in Part III, based on the same idea, namely that in the easy case, everything eventually reduces to some elementary computations with partitions.

All this sounds quite exciting, good theory that we will be developing here, hope you agree with me. In order to get started now, let us formulate the following key definition, extending to the case of arbitrary partitions what we already know about pairings:

DEFINITION 7.1. *Given a partition $\pi \in P(k,l)$ and an integer $N \in \mathbb{N}$, we define*

$$T_\pi : (\mathbb{C}^N)^{\otimes k} \to (\mathbb{C}^N)^{\otimes l}$$

by the following formula, with $e_1, \ldots, e_N$ being the standard basis of $\mathbb{C}^N$,

$$T_\pi(e_{i_1} \otimes \ldots \otimes e_{i_k}) = \sum_{j_1 \ldots j_l} \delta_\pi \begin{pmatrix} i_1 & \ldots & i_k \\ j_1 & \ldots & j_l \end{pmatrix} e_{j_1} \otimes \ldots \otimes e_{j_l}$$

and with the coefficients on the right being Kronecker type symbols.

To be more precise here, in order to compute the Kronecker type symbols $\delta_\pi\binom{i}{j} \in \{0,1\}$, we proceed exactly as in the pairing case, namely by putting the multi-indices $i = (i_1, \ldots, i_k)$ and $j = (j_1, \ldots, j_l)$ on the legs of π, in the obvious way. In case all the blocks of π contain equal indices of i, j, we set $\delta_\pi\binom{i}{j} = 1$. Otherwise, we set $\delta_\pi\binom{i}{j} = 0$.

With the above notion in hand, we can now formulate the following key definition, motivated by the Brauer theorems for O_N, U_N, as indicated before:

DEFINITION 7.2. *A closed subgroup $G \subset U_N$ is called easy when*

$$Hom(u^{\otimes k}, u^{\otimes l}) = span\left(T_\pi \middle| \pi \in D(k,l)\right)$$

for any two colored integers $k, l = \circ \bullet \circ \bullet \ldots$, for certain sets of partitions

$$D(k,l) \subset P(k,l)$$

where $\pi \to T_\pi$ is the standard implementation of the partitions, as linear maps.

In other words, we call a group G easy when its Tannakian category appears in the simplest possible way: from the linear maps associated to partitions. The terminology is quite natural, because Tannakian duality is basically our only serious tool.

As basic examples, the orthogonal and unitary groups O_N, U_N are both easy, coming respectively from the following collections of sets of partitions:

$$P_2 = \bigsqcup_{k,l} P_2(k,l) \quad , \quad \mathcal{P}_2 = \bigsqcup_{k,l} \mathcal{P}_2(k,l)$$

In the general case now, as an important theoretical remark, in the context of Definition 7.2, consider the following collection of sets of partitions:

$$D = \bigsqcup_{k,l} D(k,l)$$

This collection of sets D obviously determines G, but the converse is not true. Indeed, at $N = 1$ for instance, both the choices $D = P_2, \mathcal{P}_2$ produce the same easy group, namely $G = \{1\}$. We will be back to this issue on several occasions, with results about it.

In order to advance, our first goal will be that of establishing a duality between easy groups and certain special classes of collections of sets as above, namely:

$$D = \bigsqcup_{k,l} D(k,l)$$

Let us begin with a general definition, as follows:

DEFINITION 7.3. *Let $P(k,l)$ be the set of partitions between an upper colored integer k, and a lower colored integer l. A collection of subsets*

$$D = \bigsqcup_{k,l} D(k,l)$$

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 $(\pi, \sigma) \to \left[\begin{smallmatrix}\sigma\\ \pi\end{smallmatrix}\right]$, 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 $P(\emptyset, \bullet\circ)$ both contain the semicircle $\cap$.*
(6) *The sets $P(k, \bar{k})$ with $|k| = 2$ contain the crossing partition $\times$.*

As before, this is something that we already met in chapter 6, but for the pairings only. Observe the similarity with the axioms for Tannakian categories, also from chapter 6. We will see in a moment that this similarity can be turned into something very precise, the idea being that such a category produces a family of easy quantum groups $(G_N)_{N \in \mathbb{N}}$, one for each $N \in \mathbb{N}$, via the formula in Definition 7.1, and Tannakian duality.

As basic examples, that we have already met in chapter 6, in connection with the representation theory of O_N, U_N, we have the categories $P_2, \mathcal{P}_2$ of pairings, and of matching pairings. Further basic examples include the categories P, P_{even} of all partitions, and of all partitions whose blocks have even size. We will see in a moment that these latter categories are related to the symmetric and hyperoctahedral groups S_N, H_N.

The relation with the Tannakian categories comes from the following result:

PROPOSITION 7.4. *The assignement $\pi \to T_\pi$ is categorical, in the sense that*

$$T_\pi \otimes T_\sigma = T_{[\pi\sigma]} \quad , \quad T_\pi T_\sigma = N^{c(\pi,\sigma)} T_{\left[\begin{smallmatrix}\sigma\\ \pi\end{smallmatrix}\right]} \quad , \quad T_\pi^* = T_{\pi^*}$$

where $c(\pi, \sigma)$ are certain integers, coming from the erased components in the middle.

PROOF. This is something that we already know for pairings, and the proof in general is similar. The concatenation axiom follows from the following computation:

$$\begin{aligned}
&(T_\pi\otimes T_\sigma)(e_{i_1}\otimes\ldots\otimes e_{i_p}\otimes e_{k_1}\otimes\ldots\otimes e_{k_r})\\
&=\sum_{j_1\ldots j_q}\sum_{l_1\ldots l_s}\delta_\pi\begin{pmatrix}i_1&\ldots&i_p\\j_1&\ldots&j_q\end{pmatrix}\delta_\sigma\begin{pmatrix}k_1&\ldots&k_r\\l_1&\ldots&l_s\end{pmatrix}e_{j_1}\otimes\ldots\otimes e_{j_q}\otimes e_{l_1}\otimes\ldots\otimes e_{l_s}\\
&=\sum_{j_1\ldots j_q}\sum_{l_1\ldots l_s}\delta_{[\pi\sigma]}\begin{pmatrix}i_1&\ldots&i_p&k_1&\ldots&k_r\\j_1&\ldots&j_q&l_1&\ldots&l_s\end{pmatrix}e_{j_1}\otimes\ldots\otimes e_{j_q}\otimes e_{l_1}\otimes\ldots\otimes e_{l_s}\\
&=T_{[\pi\sigma]}(e_{i_1}\otimes\ldots\otimes e_{i_p}\otimes e_{k_1}\otimes\ldots\otimes e_{k_r})
\end{aligned}$$

The composition axiom follows from the following computation:

$$\begin{aligned}
&T_\pi T_\sigma(e_{i_1}\otimes\ldots\otimes e_{i_p})\\
&=\sum_{j_1\ldots j_q}\delta_\sigma\begin{pmatrix}i_1&\ldots&i_p\\j_1&\ldots&j_q\end{pmatrix}\sum_{k_1\ldots k_r}\delta_\pi\begin{pmatrix}j_1&\ldots&j_q\\k_1&\ldots&k_r\end{pmatrix}e_{k_1}\otimes\ldots\otimes e_{k_r}\\
&=\sum_{k_1\ldots k_r}N^{c(\pi,\sigma)}\delta_{[\sigma]}\begin{pmatrix}i_1&\ldots&i_p\\k_1&\ldots&k_r\end{pmatrix}e_{k_1}\otimes\ldots\otimes e_{k_r}\\
&=N^{c(\pi,\sigma)}T_{[\sigma]}(e_{i_1}\otimes\ldots\otimes e_{i_p})
\end{aligned}$$

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. □

Time now to put everyting together. All the above was pure combinatorics, and in relation with the compact groups, we have the following result:

THEOREM 7.5. *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*

$$Hom(u^{\otimes k},u^{\otimes l})=span\left(T_\pi\middle|\pi\in D(k,l)\right)$$

and the Tannakian duality correspondence.

PROOF. Given an integer $N \in \mathbb{N}$, consider the correspondence $\pi \to T_\pi$ constructed in Definition 7.1, and then the collection of linear spaces in the statement, namely:

$$C_{kl} = span\left(T_\pi \middle| \pi \in D(k,l)\right)$$

According to the formulae in Proposition 7.4, and to our axioms for the categories of partitions, from Definition 7.3, this collection of spaces $C = (C_{kl})$ satisfies the axioms for the Tannakian categories, from chapter 6. Thus the Tannakian duality result there applies, and provides us with a closed subgroup $G_N \subset U_N$ such that:

$$C_{kl} = Hom(u^{\otimes k}, u^{\otimes l})$$

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

In relation with the easiness property, we can now formulate a key result, which can serve as an alternative definition for the easy groups, as follows:

THEOREM 7.6. *A closed subgroup $G \subset U_N$ is easy precisely when*

$$Hom(u^{\otimes k}, u^{\otimes l}) = span\left(T_\pi \middle| \pi \in D(k,l)\right)$$

for any colored integers k, l, for a certain category of partitions $D \subset P$.

PROOF. This basically follows from Theorem 7.5, as follows:

(1) In one sense, we know from Theorem 7.5 that any category of partitions $D \subset P$ produces a family of closed groups $G \subset U_N$, one for each $N \in \mathbb{N}$, according to Tannakian duality and to the Hom space formula there, namely:

$$Hom(u^{\otimes k}, u^{\otimes l}) = span\left(T_\pi \middle| \pi \in D(k,l)\right)$$

But these groups $G \subset U_N$ are indeed easy, in the sense of Definition 7.2.

(2) In the other sense now, assume that $G \subset U_N$ is easy, in the sense of Definition 7.2, coming via the above Hom space formula, from a collection of sets as follows:

$$D = \bigsqcup_{k,l} D(k,l)$$

Consider now the category of partitions $\widetilde{D} =< D >$ generated by this family. This is by definition the smallest category of partitions containing D, whose existence follows by starting with D, and performing the various categorical operations, namely horizontal and vertical concatenation, and upside-down turning. It follows then, via another application of Tannakian duality, that we have the following formula, for any k, l:

$$Hom(u^{\otimes k}, u^{\otimes l}) = span\left(T_\pi \middle| \pi \in \widetilde{D}(k,l)\right)$$

Thus, our group $G \subset U_N$ can be viewed as well as coming from $\widetilde{D}$, and so appearing as particular case of the construction in Theorem 7.5, and this gives the result. □

As already mentioned above, Theorem 7.6 can be regarded as an alternative definition for easiness, with the assumption that $D \subset P$ must be a category of partitions being added. In what follows we will rather use this new definition, which is more precise.

Generally speaking, the same comments as before apply. First, G is easy when its Tannakian category appears in the simplest possible way: from a category of partitions. The terminology is quite natural, because Tannakian duality is our only serious tool.

Also, the category of partitions D is not unique, for instance because at $N = 1$ all the categories of partitions produce the same easy group, namely $G = \{1\}$. We will be back to this issue on several occasions, with various results about it.

We will see in what follows that many interesting examples of compact quantum groups are easy. Moreover, most of the known series of "basic" compact quantum groups, $G = (G_N)$ with $N \in \mathbb{N}$, can be in principle made fit into some suitable extensions of the easy quantum group formalism. We will discuss this too, in what follows.

The notion of easiness goes back to the results of Brauer in [13] regarding the orthogonal group O_N, and the unitary group U_N, which reformulate as follows:

Theorem 7.7. *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. This is something that we already know, from chapter 6, based on Tannakian duality, the idea of the proof being as follows:

(1) The group U_N being defined via the relations $u^* = u^{-1}$, $u^t = \bar{u}^{-1}$, the associated Tannakian category is $C = span(T_\pi | \pi \in D)$, with:

$$D = < \overset{\cap}{\circ\bullet}\ ,\ \overset{\cap}{\bullet\circ} > = \mathcal{P}_2$$

(2) The group $O_N \subset U_N$ being defined by imposing the relations $u_{ij} = \bar{u}_{ij}$, the associated Tannakian category is $C = span(T_\pi | \pi \in D)$, with:

$$D = < \mathcal{P}_2, \substack{\circ \\ | \\ \bullet}, \substack{\bullet \\ | \\ \circ} > = P_2$$

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

There are many other examples of easy groups, and we will gradually explore this. To start with, we have the following interesting result, still in the continuous case:

Theorem 7.8. *We have the following results:*

1. *The unitary bistochastic group C_N is easy, coming from the category $\mathcal{P}_{12}$ of matching singletons and pairings.*
2. *The orthogonal bistochastic group B_N is easy, coming from the category P_{12} of singletons and pairings.*

PROOF. The proof here is similar to the proof of Theorem 7.7. To be more precise, we can use the results there, and the proof goes as follows:

(1) The group $C_N \subset U_N$ is defined by imposing the following relations, with ξ being the all-one vector, which correspond to the bistochasticity condition:

$$u\xi = \xi \quad , \quad \bar{u}\xi = \xi$$

But these relations tell us precisely that the following two operators, with the partitions on the right being singletons, must be in the associated Tannakian category C:

$$T_\pi \quad : \quad \pi = \downharpoonleft \ , \ \downharpoonleft$$

Thus the associated Tannakian category is $C = span(T_\pi | \pi \in D)$, with:

$$D =< \mathcal{P}_2, \downharpoonleft, \downharpoonleft >= \mathcal{P}_{12}$$

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

(2) In order to deal now with the real bistochastic group B_N, we can either use a similar argument, or simply use the following intersection formula:

$$B_N = C_N \cap O_N$$

Indeed, at the categorical level, this intersection formula tells us that the associated Tannakian category is given by $C = span(T_\pi | \pi \in D)$, with:

$$D =< \mathcal{P}_{12}, P_2 >= P_{12}$$

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

As a comment here, we have used in the above the fact, which is something quite trivial, that the category of partitions associated to an intersection of easy quantum groups is generated by the corresponding categories of partitions. We will be back to this, and to some other product operations as well, with similar results, later on.

We can put now the results that we have together, as follows:

THEOREM 7.9. *The basic unitary and bistochastic groups,*

$$\begin{array}{ccc} C_N & \longrightarrow & U_N \\ \uparrow & & \uparrow \\ B_N & \longrightarrow & O_N \end{array}$$

are all easy, coming from the various categories of singletons and pairings.

PROOF. We know from the above that the groups in the statement are indeed easy, the corresponding diagram of categories of partitions being as follows:

$$\begin{array}{ccc} \mathcal{P}_{12} & \longleftarrow & \mathcal{P}_2 \\ \downarrow & & \downarrow \\ P_{12} & \longleftarrow & P_2 \end{array}$$

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

Summarizing, what we have so far is a general notion of "easiness", coming from the Brauer theorems for O_N, U_N, and their straightforward extensions to B_N, C_N.

7b. Reflection groups

In view of the above, the notion of easiness is a quite interesting one, deserving a full, systematic investigation. As a first natural question that we would like to solve, we would like to compute the easy group associated to the category of all partitions P itself. And here, no surprise, we are led to the most basic, but non-trivial, classical group that we know, namely the symmetric group S_N. To be more precise, we have the following Brauer type theorem for S_N, which answers our question formulated above:

THEOREM 7.10. *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 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 "fork" partition $Y \in P(2,1)$, we have:

$$C(G) = C(O_N) \Big/ \Big\langle T_Y \in Hom(u^{\otimes 2}, u) \Big\rangle$$

The linear map associated to Y is given by the following formula:

$$T_Y(e_i \otimes e_j) = \delta_{ij} e_i$$

In order to do the computations, we use the following formulae:

$$u = (u_{ij})_{ij} \quad , \quad u^{\otimes 2} = (u_{ij}u_{kl})_{ik,jl} \quad , \quad T_Y = (\delta_{ijk})_{i,jk}$$

We therefore obtain the following formula:

$$(T_Y u^{\otimes 2})_{i,jk} = \sum_{lm} (T_Y)_{i,lm} (u^{\otimes 2})_{lm,jk} = u_{ij} u_{ik}$$

On the other hand, we have as well the following formula:

$$(uT_Y)_{i,jk} = \sum_{l} u_{il} (T_Y)_{l,jk} = \delta_{jk} u_{ij}$$

Thus, the relation defining $G \subset O_N$ reformulates as follows:

$$T_Y \in Hom(u^{\otimes 2}, u) \iff u_{ij} u_{ik} = \delta_{jk} u_{ij}, \forall i, j, k$$

In other words, the elements u_{ij} must be projections, which must be pairwise orthogonal on the rows of $u = (u_{ij})$. 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. □

As a continuation of this, let us discuss now the hyperoctahedral group H_N. The result here is quite similar to the one for the symmetric groups, as follows:

THEOREM 7.11. *The hyperoctahedral group H_N, regarded as a group of matrices,*

$$S_N \subset H_N \subset O_N$$

is easy, coming from the category of partitions with even blocks P_{even}.

PROOF. This follows as usual from Tannakian duality. To be more precise, consider the following one-block partition, which, as the name indicates, looks like a H letter:

$$H \in P(2, 2)$$

The linear map associated to this partition is then given by:

$$T_H(e_i \otimes e_j) = \delta_{ij} e_i \otimes e_i$$

By using this formula, we have the following computation:

$$\begin{aligned}
(T_H \otimes id) u^{\otimes 2} (e_a \otimes e_b) &= (T_H \otimes id) \left(\sum_{ijkl} e_{ij} \otimes e_{kl} \otimes u_{ij} u_{kl} \right) (e_a \otimes e_b) \\
&= (T_H \otimes id) \left(\sum_{ik} e_i \otimes e_k \otimes u_{ia} u_{kb} \right) \\
&= \sum_{i} e_i \otimes e_i \otimes u_{ia} u_{ib}
\end{aligned}$$

On the other hand, we have as well the following computation:

$$\begin{aligned} u^{\otimes 2}(T_H \otimes id)(e_a \otimes e_b) &= \delta_{ab}\left(\sum_{ijkl} e_{ij} \otimes e_{kl} \otimes u_{ij}u_{kl}\right)(e_a \otimes e_a) \\ &= \delta_{ab}\sum_{ij} e_i \otimes e_k \otimes u_{ia}u_{ka} \end{aligned}$$

We conclude from this that we have the following equivalence:

$$T_H \in End(u^{\otimes 2}) \iff \delta_{ik}u_{ia}u_{ib} = \delta_{ab}u_{ia}u_{ka}, \forall i, k, a, b$$

But the relations on the right tell us that the entries of $u = (u_{ij})$ must satisfy $\alpha\beta = 0$ on each row and column of u, and so that the corresponding closed subgroup $G \subset O_N$ consists of the matrices $g \in O_N$ which are permutation-like, with ± 1 nonzero entries. Thus, the corresponding group is $G = H_N$, and as a conclusion to this, we have:

$$C(H_N) = C(O_N)\Big/\Big\langle T_H \in End(u^{\otimes 2})\Big\rangle$$

According now to our conventions for easiness, this means that the hyperoctahedral group H_N is easy, coming from the following category of partitions:

$$D =< H >$$

But the category on the right can be computed by drawing pictures, and we have:

$$< H >= P_{even}$$

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

More generally now, we have in fact the following grand result, regarding the series of complex reflection groups H_N^s, which covers both the groups S_N, H_N:

THEOREM 7.12. *The complex reflection group $H_N^s = \mathbb{Z}_s \wr S_N$ is easy, the corresponding category P^s consisting of the partitions satisfying the condition*

$$\#\circ = \#\bullet\,(s)$$

as a weighted sum, in each block. In particular, we have the following results:

(1) *S_N is easy, coming from the category P.*
(2) *$H_N = \mathbb{Z}_2 \wr S_N$ is easy, coming from the category P_{even}.*
(3) *$K_N = \mathbb{T} \wr S_N$ is easy, coming from the category $\mathcal{P}_{even}$.*

PROOF. This is something that we already know at $s = 1, 2$, from Theorems 7.10 and 7.11. In general, the proof is similar, based on Tannakian duality. To be more precise, in what regards the main assertion, the idea here is that the one-block partition $\pi \in P(s)$, which generates the category of partitions P^s in the statement, implements the relations producing the subgroup $H_N^s \subset S_N$. As for the last assertions, these are all elementary:

(1) At $s = 1$ we know that we have $H_N^1 = S_N$. Regarding now the corresponding category, here the condition $\#\circ = \#\bullet\,(1)$ is automatic, and so $P^1 = P$.

(2) At $s = 2$ we know that we have $H_N^2 = H_N$. Regarding now the corresponding category, here the condition $\#\circ = \#\bullet\,(2)$ reformulates as follows:

$$\#\circ + \#\bullet = 0(2)$$

Thus each block must have even size, and we obtain, as claimed, $P^2 = P_{even}$.

(3) At $s = \infty$ we know that we have $H_N^\infty = K_N$. Regarding now the corresponding category, here the condition $\#\circ = \#\bullet\,(\infty)$ reads:

$$\#\circ = \#\bullet$$

But this is the condition defining $\mathcal{P}_{even}$, and so $P^\infty = \mathcal{P}_{even}$, as claimed. □

Summarizing, we have many examples. In fact, our list of easy groups has currently become quite big, and here is a selection of the main results that we have so far:

THEOREM 7.13. *We have a diagram of compact groups as follows,*

$$\begin{array}{ccc} K_N & \longrightarrow & U_N \\ \uparrow & & \uparrow \\ H_N & \longrightarrow & O_N \end{array}$$

where $H_N = \mathbb{Z}_2 \wr S_N$ and $K_N = \mathbb{T} \wr S_N$, and all these groups are easy.

PROOF. This follows from the above results. To be more precise, we know that the above groups are all easy, the corresponding categories of partitions being as follows:

$$\begin{array}{ccc} \mathcal{P}_{even} & \longleftarrow & \mathcal{P}_2 \\ \downarrow & & \downarrow \\ P_{even} & \longleftarrow & P_2 \end{array}$$

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

Summarizing, most of the groups that we investigated in this book are covered by the easy group formalism. One exception is the symplectic group Sp_N, but this group is covered as well, by a suitable extension of the easy group formalism. See [16].

7c. Basic operations

Let us discuss now some basic composition operations, in general, and for the easy groups. We will be mainly interested in the following operations:

DEFINITION 7.14. *The closed subgroups of U_N are subject to intersection and generation operations, constructed as follows:*

(1) *Intersection: $H \cap K$ is the usual intersection of H, K.*
(2) *Generation: $< H, K >$ is the closed subgroup generated by H, K.*

Alternatively, we can define these operations at the function algebra level, by performing certain operations on the associated ideals, as follows:

PROPOSITION 7.15. *Assuming that we have presentation results as follows,*

$$C(H) = C(U_N)/I \quad , \quad C(K) = C(U_N)/J$$

the groups $H \cap K$ and $< H, K >$ are given by the following formulae,

$$C(H \cap K) = C(U_N)/ < I, J >$$

$$C(< H, K >) = C(U_N)/(I \cap J)$$

at the level of the associated algebras of functions.

PROOF. This is indeed clear from the definition of the operations $\cap$ and $<, >$, as formulated above, and from the Stone-Weierstrass theorem. □

In what follows we will need Tannakian formulations of the above two operations. The result here, that we have already used a couple of times in the above, is as follows:

THEOREM 7.16. *The intersection and generation operations $\cap$ and $<, >$ can be constructed via the Tannakian correspondence $G \to C_G$, as follows:*

(1) *Intersection: defined via $C_{G \cap H} =< C_G, C_H >$.*
(2) *Generation: defined via $C_{<G,H>} = C_G \cap C_H$.*

PROOF. This follows from Proposition 7.15, and from Tannakian duality. Indeed, it follows from Tannakian duality that given a closed subgroup $G \subset U_N$, with fundamental representation v, the algebra of functions $C(G)$ has the following presentation:

$$C(G) = C(U_N) \Big/ \left\langle T \in Hom(u^{\otimes k}, u^{\otimes l}) \middle| \forall k, \forall l, \forall T \in Hom(v^{\otimes k}, v^{\otimes l}) \right\rangle$$

In other words, given a closed subgroup $G \subset U_N$, we have a presentation of the following type, with I_G being the ideal coming from the Tannakian category of G:

$$C(G) = C(U_N)/I_G$$

But this leads to the conclusion in the statement. □

In relation now with our easiness questions, we first have the following result:

PROPOSITION 7.17. *Assuming that H, K are easy, then so is $H \cap K$, and we have*

$$D_{H\cap K} =< D_H, D_K >$$

at the level of the corresponding categories of partitions.

PROOF. We have indeed the following computation:

$$\begin{aligned} C_{H\cap K} &= < C_H, C_K > \\ &= < span(D_H), span(D_K) > \\ &= span(< D_H, D_K >) \end{aligned}$$

Thus, by Tannakian duality we obtain the result. □

Regarding now the generation operation, the situation here is more complicated, due to a number of technical reasons, and we only have the following statement:

PROPOSITION 7.18. *Assuming that H, K are easy, we have an inclusion*

$$< H, K > \subset \{H, K\}$$

coming from an inclusion of Tannakian categories as follows,

$$C_H \cap C_K \supset span(D_H \cap D_K)$$

where $\{H, K\}$ is the easy group having as category of partitions $D_H \cap D_K$.

PROOF. This follows from the definition and properties of the generation operation, explained above, and from the following computation:

$$\begin{aligned} C_{<H,K>} &= C_H \cap C_K \\ &= span(D_H) \cap span(D_K) \\ &\supset span(D_H \cap D_K) \end{aligned}$$

Indeed, by Tannakian duality we obtain from this all the assertions. □

It is not clear if the inclusions in Proposition 7.18 are isomorphisms or not, and this even under a supplementary $N >> 0$ assumption. Technically speaking, the problem comes from the fact that the operation $\pi \to T_\pi$ does not produce linearly independent maps, and so all that we are doing is sensitive to the value of $N \in \mathbb{N}$. The subject here is quite technical, to be further developed in Part III below, with probabilistic motivations in mind, without however solving the present algebraic questions.

Summarizing, we have some problems here, and we must proceed as follows:

THEOREM 7.19. *The intersection and easy generation operations $\cap$ and $\{\,,\}$ can be constructed via the Tannakian correspondence $G \to D_G$, as follows:*

(1) *Intersection: defined via $D_{G\cap H} =< D_G, D_H >$.*
(2) *Easy generation: defined via $D_{\{G,H\}} = D_G \cap D_H$.*

PROOF. Here the situation is as follows:

(1) This is a true and honest result, coming from Proposition 7.17.

(2) This is more of an empty statement, coming from Proposition 7.18. □

As already mentioned, there is some interesting mathematics still to be worked out, in relation with all this, and we will be back to this later, with further details. With the above notions in hand, however, even if not fully satisfactory, we can formulate a nice result, which improves our main result so far, namely Theorem 7.13, as follows:

THEOREM 7.20. *The basic unitary and reflection groups, namely*

$$\begin{array}{ccc} K_N & \longrightarrow & U_N \\ \uparrow & & \uparrow \\ H_N & \longrightarrow & O_N \end{array}$$

are all easy, and they form an intersection and easy generation diagram, in the sense that the above square diagram satisfies $U_N = \{K_N, O_N\}$, and $H_N = K_N \cap O_N$.

PROOF. We know from Theorem 7.13 that the groups in the statement are easy, the corresponding categories of partitions being as follows:

$$\begin{array}{ccc} \mathcal{P}_{even} & \longleftarrow & \mathcal{P}_2 \\ \downarrow & & \downarrow \\ P_{even} & \longleftarrow & P_2 \end{array}$$

Now observe that this latter diagram is an intersection and generation diagram. By using Theorem 7.19, this reformulates into the fact that the diagram of quantum groups is an intersection and easy generation diagram, as claimed. □

It is possible to further improve the above result, by proving that the diagram there is actually a plain generation diagram. However, this is something more technical, and for a discussion here, you can check for instance my quantum group book [9].

Moving forward, as a continuation of the above, it is possible to develop some more general theory, along the above lines. Given a closed subgroup $G \subset U_N$, we can talk about its "easy envelope", which is the smallest easy group $\widetilde{G}$ containing G. This easy envelope appears by definition as an intermediate closed subgroup, as follows:

$$G \subset \widetilde{G} \subset U_N$$

With this notion in hand, Proposition 7.18 can be refined into a result stating that given two easy groups H, K, we have inclusions as follows:

$$< H, K > \subset \widetilde{< H, K >} \subset \{H, K\}$$

In order to discuss all this, let us start with the following definition:

DEFINITION 7.21. *A closed subgroup $G \subset U_N$ is called homogeneous when*

$$S_N \subset G \subset U_N$$

with $S_N \subset U_N$ being the standard embedding, via permutation matrices.

We will be interested in such groups, which cover for instance all the easy groups, and many more. At the Tannakian level, we have the following result:

THEOREM 7.22. *The homogeneous groups $S_N \subset G \subset U_N$ are in one-to-one correspondence with the intermediate tensor categories*

$$span\left(T_\pi\middle|\pi \in \mathcal{P}_2\right) \subset C \subset span\left(T_\pi\middle|\pi \in P\right)$$

where P is the category of all partitions, $\mathcal{P}_2$ is the category of the matching pairings, and $\pi \to T_\pi$ is the standard implementation of partitions, as linear maps.

PROOF. This follows from Tannakian duality, and from the Brauer type results for S_N, U_N. To be more precise, we know from Tannakian duality that each closed subgroup $G \subset U_N$ can be reconstructed from its Tannakian category $C = (C(k,l))$, as follows:

$$C(G) = C(U_N)\Big/\left\langle T \in Hom(u^{\otimes k}, u^{\otimes l})\middle|\forall k, l, \forall T \in C(k,l)\right\rangle$$

Thus we have a one-to-one correspondence $G \leftrightarrow C$, given by Tannakian duality, and since the endpoints $G = S_N, U_N$ are both easy, corresponding to the categories $C = span(T_\pi|\pi \in D)$ with $D = P, \mathcal{P}_2$, this gives the result. □

Our purpose now will be that of using the Tannakian result in Theorem 7.22, in order to introduce and study a combinatorial notion of "easiness level", for the arbitrary intermediate groups $S_N \subset G \subset U_N$. Let us begin with the following simple fact:

PROPOSITION 7.23. *Given a homogeneous group $S_N \subset G \subset U_N$, with associated Tannakian category $C = (C(k,l))$, the sets*

$$D^1(k,l) = \left\{\pi \in P(k,l)\middle|T_\pi \in C(k,l)\right\}$$

form a category of partitions, in the sense of Definition 7.3.

PROOF. We use the basic categorical properties of the correspondence $\pi \to T_\pi$ between partitions and linear maps, that we established in the above, namely:

$$T_{[\pi\sigma]} = T_\pi \otimes T_\sigma \quad , \quad T_{[\frac{\sigma}{\pi}]} \sim T_\pi T_\sigma \quad , \quad T_{\pi^*} = T_\pi^*$$

Together with the fact that C is a tensor category, we deduce from these formulae that we have the following implication:

$$\begin{aligned}\pi,\sigma\in D^1&\implies T_\pi,T_\sigma\in C\\&\implies T_\pi\otimes T_\sigma\in C\\&\implies T_{[\pi\sigma]}\in C\\&\implies [\pi\sigma]\in D^1\end{aligned}$$

On the other hand, we have as well the following implication:

$$\begin{aligned}\pi,\sigma\in D^1&\implies T_\pi,T_\sigma\in C\\&\implies T_\pi T_\sigma\in C\\&\implies T_{[\sigma\atop\pi]}\in C\\&\implies \left[\sigma\atop\pi\right]\in D^1\end{aligned}$$

Finally, we have as well the following implication:

$$\begin{aligned}\pi\in D^1&\implies T_\pi\in C\\&\implies T_\pi^*\in C\\&\implies T_{\pi^*}\in C\\&\implies \pi^*\in D^1\end{aligned}$$

Thus D^1 is indeed a category of partitions, as claimed. □

We can further refine the above observation, in the following way:

PROPOSITION 7.24. *Given a compact group $S_N\subset G\subset U_N$, construct $D^1\subset P$ as above, and let $S_N\subset G^1\subset U_N$ be the easy group associated to D^1. Then:*

(1) *We have $G\subset G^1$, as subgroups of U_N.*
(2) *G^1 is the smallest easy group containing G.*
(3) *G is easy precisely when $G\subset G^1$ is an isomorphism.*

PROOF. All this is elementary, the proofs being as follows:

(1) We know that the Tannakian category of G^1 is given by:

$$C_{kl}^1=span\left(T_\pi\middle|\pi\in D^1(k,l)\right)$$

Thus we have $C^1\subset C$, and so $G\subset G^1$, as subgroups of U_N.

(2) Assuming that we have $G\subset G'$, with G' easy, coming from a Tannakian category $C'=span(D')$, we must have $C'\subset C$, and so $D'\subset D^1$. Thus, $G^1\subset G'$, as desired.

(3) This is a trivial consequence of (2). □

Summarizing, we have now a notion of "easy envelope", as follows:

DEFINITION 7.25. *The easy envelope of a homogeneous group $S_N \subset G \subset U_N$ is the easy group $S_N \subset G^1 \subset U_N$ associated to the category of partitions*

$$D^1(k,l) = \left\{\pi \in P(k,l)\Big|T_\pi \in C(k,l)\right\}$$

where $C = (C(k,l))$ is the Tannakian category of G.

At the level of examples, most of the known homogeneous groups $S_N \subset G \subset U_N$ are in fact easy. However, there are non-easy interesting examples as well, such as the generic reflection groups H_N^{sd} from chapter 3, and we will certainly have an exercise at the end of this chapter, regarding the computation of the corresponding easy envelopes.

As a technical observation now, we can in fact generalize the above construction to any closed subgroup $G \subset U_N$, and we have the following result:

PROPOSITION 7.26. *Given a closed subgroup $G \subset U_N$, construct $D^1 \subset P$ as above, and let $S_N \subset G^1 \subset U_N$ be the easy group associated to D^1. We have then*

$$G^1 = (< G, S_N >)^1$$

where $< G, S_N > \subset U_N$ is the smallest closed subgroup containing G, S_N.

PROOF. According to our Tannakian results, the subgroup $< G, S_N > \subset U_N$ in the statement exists indeed, and can be obtained by intersecting categories, as follows:

$$C_{<G,S_N>} = C_G \cap C_{S_N}$$

We conclude from this that for any $\pi \in P(k,l)$ we have:

$$T_\pi \in C_{<G,S_N>}(k,l) \iff T_\pi \in C_G(k,l)$$

It follows that the D^1 categories for the groups $< G, S_N >$ and G coincide, and so the easy envelopes $(< G, S_N >)^1$ and G^1 coincide as well, as stated. □

In order now to fine-tune all this, by using an arbitrary parameter $p \in \mathbb{N}$, which can be thought of as being an "easiness level", we can proceed as follows:

DEFINITION 7.27. *Given a compact group $S_N \subset G \subset U_N$, and an integer $p \in \mathbb{N}$, we construct the family of linear spaces*

$$E^p(k,l) = \left\{\alpha_1 T_{\pi_1} + \ldots + \alpha_p T_{\pi_p} \in C(k,l)\Big|\alpha_i \in \mathbb{C}, \pi_i \in P(k,l)\right\}$$

and we denote by C^p the smallest tensor category containing $E^p = (E^p(k,l))$, and by $S_N \subset G^p \subset U_N$ the compact group corresponding to this category C^p.

As a first observation, at $p = 1$ we have $C^1 = E^1 = span(D^1)$, where D^1 is the category of partitions constructed in Proposition 7.24. Thus the group G^1 constructed above coincides with the "easy envelope" of G, from Definition 7.25.

In the general case, $p \in \mathbb{N}$, the family $E^p = (E^p(k,l))$ constructed above is not necessarily a tensor category, but we can of course consider the tensor category C^p generated by it, as indicated. Finally, in the above definition we have used of course the Tannakian duality results, in order to perform the operation $C^p \to G^p$.

In practice, the construction in Definition 7.27 is often something quite complicated, and it is convenient to use the following observation:

PROPOSITION 7.28. *The category C^p constructed above is generated by the spaces*

$$E^p(l) = \left\{\alpha_1 T_{\pi_1} + \ldots + \alpha_p T_{\pi_p} \in C(l) \middle| \alpha_i \in \mathbb{C}, \pi_i \in P(l)\right\}$$

where $C(l) = C(0,l), P(l) = P(0,l)$, with l ranging over the colored integers.

PROOF. We use the well-known fact, that we know from chapter 5, that given a closed subgroup $G \subset U_N$, we have a Frobenius type isomorphism, as follows:

$$Hom(u^{\otimes k}, u^{\otimes l}) \simeq Fix(u^{\otimes \bar{k}l})$$

If we apply this to the group G^p, we obtain an isomorphism as follows:

$$C(k,l) \simeq C(\bar{k}l)$$

On the other hand, we have as well an isomorphism $P(k,l) \simeq P(\bar{k}l)$, obtained by performing a counterclockwise rotation to the partitions $\pi \in P(k,l)$. According to the above definition of the spaces $E^p(k,l)$, this induces an isomorphism as follows:

$$E^p(k,l) \simeq E^p(\bar{k}l)$$

We deduce from this that for any partitions $\pi_1, \ldots, \pi_p \in C(k,l)$, having rotated versions $\rho_1, \ldots, \rho_p \in C(\bar{k}l)$, and for any scalars $\alpha_1, \ldots, \alpha_p \in \mathbb{C}$, we have:

$$\alpha_1 T_{\pi_1} + \ldots + \alpha_p T_{\pi_p} \in C(k,l) \iff \alpha_1 T_{\rho_1} + \ldots + \alpha_p T_{\rho_p} \in C(\bar{k}l)$$

But this gives the conclusion in the statement, and we are done. □

The main properties of the construction $G \to G^p$ can be summarized as follows:

THEOREM 7.29. *Given a compact group $S_N \subset G \subset U_N$, the compact groups G^p constructed above form a decreasing family, whose intersection is G:*

$$G = \bigcap_{p \in \mathbb{N}} G^p$$

Moreover, G is easy when this decreasing limit is stationary, $G = G^1$.

PROOF. By definition of $E^p(k,l)$, and by using Proposition 7.28, these linear spaces form an increasing filtration of $C(k,l)$. The same remains true when completing into tensor categories, and so we have an increasing filtration, as follows:

$$C=\bigcup_{p\in\mathbb{N}}C^p$$

At the compact group level now, we obtain the decreasing intersection in the statement. Finally, the last assertion is clear from Proposition 7.28. □

As a main consequence of the above results, we can now formulate:

DEFINITION 7.30. *We say that a homogeneous compact group*

$$S_N\subset G\subset U_N$$

is easy at order p when $G=G^p$, with p being chosen minimal with this property.

Observe that the order 1 notion corresponds to the usual easiness. In general, all this is quite abstract, but there are several explicit examples, that can be worked out. For more on all this, you can check my quantum group book [9].

7d. Classification results

Let us go back now to plain easiness, and discuss some classification results, following the old papers, and then the more recent paper of Tarrago-Weber [89]. In order to cut from the complexity, we must impose an extra axiom, and we will use here:

THEOREM 7.31. *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 explained above, as follows:

(1) $\iff$ (2) This is something standard, coming from the inclusion $S_N\subset G_N$, which 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 representation 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:

$$\begin{aligned}\xi_\pi \in Fix(v^{\otimes k}) &\iff (v^{\otimes k}\xi_\pi)_{i_1\ldots i_k} = (\xi_\pi)_{i_1\ldots i_k}, \forall i\\ &\iff \sum_j (v^{\otimes k})_{i_1\ldots i_k, j_1\ldots j_k}(\xi_\pi)_{j_1\ldots j_k} = (\xi_\pi)_{i_1\ldots i_k}, \forall i\\ &\iff \sum_j \delta_\pi(j_1,\ldots,j_k)v_{i_1j_1}\ldots v_{i_kj_k} = \delta_\pi(i_1,\ldots,i_k), \forall i\end{aligned}$$

Now let us recall that our representation 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. □

We can now formulate a first classification result, as follows:

THEOREM 7.32. *The uniform orthogonal easy groups are as follows,*

$$\begin{array}{ccc} B_N & \longrightarrow & O_N \\ \uparrow & & \uparrow \\ S_N & \longrightarrow & H_N \end{array}$$

and this diagram is an intersection and easy generation diagram.

PROOF. We know that the quantum groups in the statement are indeed easy and uniform, the corresponding categories of partitions being as follows:

$$\begin{array}{ccc} P_{12} & \longleftarrow & P_2 \\ \downarrow & & \downarrow \\ P & \longleftarrow & P_{even} \end{array}$$

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 arbitrary easy group, as follows:

$$S_N \subset G_N \subset O_N$$

This group must then come from a category of partitions, as follows:

$$P_2 \subset D \subset P$$

Now if we assume $G = (G_N)$ to be uniform, this category of partitions D is uniquely determined by the subset $L \subset \mathbb{N}$ consisting of the sizes of the blocks of the partitions in D. Our claim now is that the admissible sets are 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.

Indeed, in one sense, this follows from our easiness results for O_N, B_N, H_N, S_N. In the other sense now, assume that $L \subset \mathbb{N}$ is such that the set P_L consisting of partitions whose sizes of the blocks belong to L is a category of partitions. We know from the axioms of the categories of partitions that the semicircle $\cap$ must be in the category, so we have $2 \in L$. Our claim is that the following conditions must be satisfied as well:

$$k, l \in L,\ k > l \implies k - l \in L$$

$$k \in L,\ k \geq 2 \implies 2k - 2 \in L$$

Indeed, we will prove that both conditions follow from the axioms of the categories of partitions. Let us denote by $b_k \in P(0, k)$ the one-block partition, as follows:

$$b_k = \begin{Bmatrix} \sqcap\!\sqcap & \ldots & \sqcap \\ 1 \ \ 2 & \ldots & k \end{Bmatrix}$$

For $k > l$, we can write b_{k-l} in the following way:

$$b_{k-l} = \left\{\begin{array}{ccccccc} \sqcap\!\sqcap & \ldots & \ldots & \ldots & \ldots & \sqcap \\ 1\ 2 & \ldots & l & l+1 & \ldots & k \\ \sqcup\!\sqcup & \ldots & \sqcup & | & \ldots & | \\ & & & 1 & \ldots & k-l \end{array}\right\}$$

In other words, we have the following formula:

$$b_{k-l} = (b_l^* \otimes |^{\otimes k-l})b_k$$

Since all the terms of this composition are in P_L, we have $b_{k-l} \in P_L$, and this proves our first formula. As for the second formula, this can be proved in a similar way, by capping two adjacent k-blocks with a 2-block, in the middle.

With the above two formulae in hand, we can conclude in the following way:

Case 1. Assume $1 \in L$. By using the first formula with $l = 1$ we get:

$$k \in L \implies k - 1 \in L$$

This condition shows that we must have $L = \{1, 2, \ldots, m\}$, for a certain number $m \in \{1, 2, \ldots, \infty\}$. On the other hand, by using the second formula we get:

$$\begin{aligned} m \in L &\implies 2m - 2 \in L \\ &\implies 2m - 2 \leq m \\ &\implies m \in \{1, 2, \infty\} \end{aligned}$$

The case $m = 1$ being excluded by the condition $2 \in L$, we reach to one of the two sets producing the groups S_N, B_N.

Case 2. Assume $1 \notin L$. By using the first formula with $l = 2$ we get:

$$k \in L \implies k - 2 \in L$$

This condition shows that we must have $L = \{2, 4, \ldots, 2p\}$, for a certain number $p \in \{1, 2, \ldots, \infty\}$. On the other hand, by using the second formula we get:

$$\begin{aligned} 2p \in L &\implies 4p - 2 \in L \\ &\implies 4p - 2 \leq 2p \\ &\implies p \in \{1, \infty\} \end{aligned}$$

Thus L must be one of the two sets producing O_N, H_N, and we are done. □

All the above is very nice, but the continuation of the story is more complicated. When lifting the uniformity assumption, the final classification results become more technical, due to the presence of various copies of $\mathbb{Z}_2$, that can be added, while keeping the easiness

property still true. To be more precise, in the real case it is known that we have exactly 6 solutions, which are as follows, with the convention $G'_N = G_N \times \mathbb{Z}_2$:

$$\begin{array}{ccccc} B_N & \longrightarrow & B'_N & \longrightarrow & O_N \\ \uparrow & & \uparrow & & \uparrow \\ S_N & \longrightarrow & S'_N & \longrightarrow & H_N \end{array}$$

In the unitary case now, the classification is quite similar, but more complicated, as explained in the paper of Tarrago-Weber [89]. In particular we have:

THEOREM 7.33. *The uniform easy groups which are purely unitary, in the sense that they appear as complexifications of real easy groups, are as follows,*

$$\begin{array}{ccc} C_N & \longrightarrow & U_N \\ \uparrow & & \uparrow \\ S_N & \longrightarrow & K_N \end{array}$$

and this diagram is an intersection and easy generation diagram.

PROOF. We know from the above that the groups in the statement are indeed easy and uniform, the corresponding categories of partitions being as follows:

$$\begin{array}{ccc} \mathcal{P}_{12} & \longleftarrow & \mathcal{P}_2 \\ \downarrow & & \downarrow \\ P & \longleftarrow & \mathcal{P}_{even} \end{array}$$

Since this latter diagram is an intersection and generation diagram, we conclude that we have an intersection and easy generation diagram of groups, as stated. As for the uniqueness result, the proof here is similar to the proof from the real case, from Theorem 7.32, by examining the possible sizes of the blocks of the partitions in the category, and doing some direct combinatorics. For details here, we refer to Tarrago-Weber [89]. □

Finally, let us mention that the easy quantum group formalism can be extended into a "super-easy" group formalism, covering as well the symplectic group Sp_N. This is something a bit technical, and we refer here to the paper of Collins-Śniady [16].

7e. Exercises

Exercises:

EXERCISE 7.34.

EXERCISE 7.35.

EXERCISE 7.36.

EXERCISE 7.37.

EXERCISE 7.38.

EXERCISE 7.39.

EXERCISE 7.40.

EXERCISE 7.41.

Bonus exercise.

CHAPTER 8

Low dimensions

8a. Rotation groups

In this chapter we study the finite subgroups of the rotation groups, in low dimensions. Things will be quite technical here, mixing representation theory and other methods.

To start with, here is a useful reformulation of our main result so far regarding SU_2, obtained by further building on the parametrization from chapter 1:

THEOREM 8.1. *We have the formula*

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

which makes SU_2 isomorphic to the unit real sphere $S^3_{\mathbb{R}} \subset \mathbb{R}^3$.

PROOF. We recall from chapter 1 that we have the following formula:

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

Now let us write our parameters $a, b \in \mathbb{C}$, which belong to the complex unit sphere $S^1_{\mathbb{C}} \subset \mathbb{C}^2$, in terms of their real and imaginary parts, as follows:

$$a = x+iy \quad , \quad b = z+it$$

In terms of $x, y, z, t \in \mathbb{R}$, our formula for a generic matrix $U \in SU_2$ becomes the one in the statement. As for the condition to be satisfied by the parameters $x, y, z, t \in \mathbb{R}$, this comes the condition $|a|^2+|b|^2=1$ to be satisfied by $a, b \in \mathbb{C}$, which reads:

$$x^2+y^2+z^2+t^2=1$$

Thus, we are led to the conclusion in the statement. Regarding now the last assertion, recall that the unit sphere $S^3_{\mathbb{R}} \subset \mathbb{R}^4$ is given by:

$$S^3_{\mathbb{R}} = \left\{ (x,y,z,t) \;\middle|\; x^2+y^2+z^2+t^2=1 \right\}$$

Thus, we have an isomorphism of compact spaces, as follows:

$$SU_2 \simeq S^3_{\mathbb{R}} \quad , \quad \begin{pmatrix} x+iy & z+it \\ -z+it & x-iy \end{pmatrix} \to (x,y,z,t)$$

We have therefore proved our theorem. □

As a philosophical comment here, the above parametrization of SU_2 is something very nice, because the parameters (x,y,z,t) range now over the sphere of space-time. Thus, we are probably doing some kind of physics here. More on this later.

Regarding now the group U_2, we have here a similar result, as follows:

THEOREM 8.2. *We have the following formula,*

$$U_2=\left\{(p+iq)\begin{pmatrix}x+iy&z+it\\-z+it&x-iy\end{pmatrix}\;\middle|\;x^2+y^2+z^2+t^2=1,\ p^2+q^2=1\right\}$$

which makes U_2 be a quotient compact space, as follows,

$$S^3_{\mathbb{R}}\times S^1_{\mathbb{R}}\to U_2$$

but with this parametrization being no longer bijective.

PROOF. We recall from chapter 1 that we have the following formula:

$$U_2=\left\{d\begin{pmatrix}a&b\\-\bar{b}&\bar{a}\end{pmatrix}\;\middle|\;|a|^2+|b|^2=1,\ |d|=1\right\}$$

Now let us write our parameters $a,b\in\mathbb{C}$, which belong to the complex unit sphere $S^1_{\mathbb{C}}\subset\mathbb{C}^2$, and $d\in\mathbb{T}$, in terms of their real and imaginary parts, as follows:

$$a=x+iy\quad,\quad b=z+it\quad,\quad d=p+iq$$

In terms of these new parameters $x,y,z,t,p,q\in\mathbb{R}$, our formula for a generic matrix $U\in SU_2$, that we established before, reads:

$$U=(p+iq)\begin{pmatrix}x+iy&z+it\\-z+it&x-iy\end{pmatrix}$$

As for the condition to be satisfied by the parameters $x,y,z,t,p,q\in\mathbb{R}$, this comes the conditions $|a|^2+|b|^2=1$ and $|d|=1$ to be satisfied by $a,b,d\in\mathbb{C}$, which read:

$$x^2+y^2+z^2+t^2=1\quad,\quad p^2+q^2=1$$

Thus, we are led to the conclusion in the statement. Regarding now the last assertion, recall that the unit spheres $S^3_{\mathbb{R}}\subset\mathbb{R}^4$ and $S^1_{\mathbb{R}}\subset\mathbb{R}^2$ are given by:

$$S^3_{\mathbb{R}}=\left\{(x,y,z,t)\;\middle|\;x^2+y^2+z^2+t^2=1\right\}$$

$$S^1_{\mathbb{R}}=\left\{(p,q)\;\middle|\;p^2+q^2=1\right\}$$

Thus, we have quotient map of compact spaces, as follows:

$$S^3_{\mathbb{R}}\times S^1_{\mathbb{R}}\to U_2\quad,\quad((x,y,z,t),(p,q))\to(p+iq)\begin{pmatrix}x+iy&z+it\\-z+it&x-iy\end{pmatrix}$$

However, the parametrization is no longer bijective, because when we globally switch signs, the element $((-x,-y,-z,-t),(-p,-q))$ produces the same element of U_2. □

Here is now another reformulation of our main result so far, regarding SU_2, obtained by further building on the parametrization from Theorem 8.1:

THEOREM 8.3. *We have the following formula,*

$$SU_2 = \left\{ xc_1 + yc_2 + zc_3 + tc_4 \;\middle|\; x^2 + y^2 + z^2 + t^2 = 1 \right\}$$

where c_1, c_2, c_3, c_4 are matrices given by

$$c_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad , \quad c_2 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

$$c_3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad , \quad c_4 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

called Pauli spin matrices.

PROOF. We recall from Theorem 8.1 that the group SU_2 can be parametrized by the real sphere $S^3_{\mathbb{R}} \subset \mathbb{R}^4$, in the following way:

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

Thus, the elements $U \in SU_2$ are precisely the matrices as follows, depending on parameters $x, y, z, t \in \mathbb{R}$ satisfying $x^2 + y^2 + z^2 + t^2 = 1$:

$$U = x \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + y \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + z \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + t \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

But this gives the formula for SU_2 in the statement. □

The above result is often the most convenient one, when dealing with SU_2. This is because the Pauli matrices have a number of remarkable properties, which are very useful when doing computations. These properties can be summarized as follows:

THEOREM 8.4. *The Pauli matrices multiply according to the formulae*

$$c_2^2 = c_3^2 = c_4^2 = -1$$

$$c_2 c_3 = -c_3 c_2 = c_4$$

$$c_3 c_4 = -c_4 c_3 = c_2$$

$$c_4 c_2 = -c_2 c_4 = c_3$$

they conjugate according to the following rules,

$$c_1^* = c_1 \ , \ c_2^* = -c_2 \ , \ c_3^* = -c_3 \ , \ c_4^* = -c_4$$

and they form an orthonormal basis of $M_2(\mathbb{C})$, with respect to the scalar product

$$< a, b >= tr(ab^*)$$

with $tr : M_2(\mathbb{C}) \to \mathbb{C}$ being the normalized trace of 2×2 matrices, $tr = Tr/2$.

PROOF. The first two assertions, regarding the multiplication and conjugation rules for the Pauli matrices, follow from some elementary computations. As for the last assertion, this follows by using these rules. Indeed, the fact that the Pauli matrices are pairwise orthogonal follows from computations of the following type, for $i \neq j$:

$$< c_i, c_j >= tr(c_i c_j^*) = tr(\pm c_i c_j) = tr(\pm c_k) = 0$$

As for the fact that the Pauli matrices have norm 1, this follows from:

$$< c_i, c_i >= tr(c_i c_i^*) = tr(\pm c_i^2) = tr(c_1) = 1$$

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

We should mention here that the Pauli matrices are cult objects in physics, due to the fact that they describe the spin of the electron. Indeed, a bit like our Earth spins around its axis, the electrons spin too. And it took scientists a lot of skill in order to understand the physics and mathematics of the spin, the conclusion being that the Schrödinger wave function space for the electron $H = L^2(\mathbb{R}^3)$ has to be enlarged with a copy of the space $K = \mathbb{C}^2$, via a direct sum, as to take into account the spin, and with this spin being described by the Pauli matrices, in some appropriate, quantum mechanical sense.

As usual, we refer to Feynman [33], Griffiths [41] or Weinberg [94] for more on all this. And with the remark that the Pauli matrices are actually subject to several possible normalizations, depending on formalism, but let us not get into all this here.

8b. Euler-Rodrigues

Back to mathematics, let us discuss now the basic unitary groups in 3 or more dimensions. The situation here becomes fairly complicated, but it is possible however to explicitly compute the rotation groups SO_3 and O_3, and explaining this result, due to Euler-Rodrigues, which is something non-trivial and very useful, will be our next goal.

The proof of the Euler-Rodrigues formula is something quite tricky. Let us start with the following construction, whose usefulness will become clear in a moment:

PROPOSITION 8.5. *The adjoint action $SU_2 \curvearrowright M_2(\mathbb{C})$, given by*

$$T_U(M) = UMU^*$$

leaves invariant the following real vector subspace of $M_2(\mathbb{C})$,

$$E = span_{\mathbb{R}}(c_1, c_2, c_3, c_4)$$

and we obtain in this way a group morphism $SU_2 \to GL_4(\mathbb{R})$.

PROOF. We have two assertions to be proved, as follows:

(1) We must first prove that, with $E \subset M_2(\mathbb{C})$ being the real vector space in the statement, we have the following implication:

$$U \in SU_2, M \in E \implies UMU^* \in E$$

But this is clear from the multiplication rules for the Pauli matrices, from Theorem 8.4. Indeed, let us write our matrices U, M as follows:

$$U = xc_1 + yc_2 + zc_3 + tc_4$$

$$M = ac_1 + bc_2 + cc_3 + dc_4$$

We know that the coefficients x, y, z, t and a, b, c, d are real, due to $U \in SU_2$ and $M \in E$. The point now is that when computing UMU^*, by using the various rules from Theorem 8.4, we obtain a matrix of the same type, namely a combination of c_1, c_2, c_3, c_4, with real coefficients. Thus, we have $UMU^* \in E$, as desired.

(2) In order to conclude, let us identify $E \simeq \mathbb{R}^4$, by using the basis c_1, c_2, c_3, c_4. The result found in (1) shows that we have a correspondence as follows:

$$SU_2 \to M_4(\mathbb{R}) \quad , \quad U \to (T_U)_{|E}$$

Now observe that for any $U \in SU_2$ and any $M \in M_2(\mathbb{C})$ we have:

$$T_{U^*}T_U(M) = U^*UMU^*U = M$$

Thus $T_{U^*} = T_U^{-1}$, and so the correspondence that we found can be written as:

$$SU_2 \to GL_4(\mathbb{R}) \quad , \quad U \to (T_U)_{|E}$$

But this a group morphism, due to the following computation:

$$T_UT_V(M) = UVMV^*U^* = T_{UV}(M)$$

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

The point now, which makes the link with SO_3, and which will ultimately elucidate the structure of SO_3, is that Proposition 8.5 can be improved as follows:

THEOREM 8.6. *The adjoint action $SU_2 \curvearrowright M_2(\mathbb{C})$, given by*

$$T_U(M) = UMU^*$$

leaves invariant the following real vector subspace of $M_2(\mathbb{C})$,

$$F = span_{\mathbb{R}}(c_2, c_3, c_4)$$

and we obtain in this way a group morphism $SU_2 \to SO_3$.

PROOF. We can do this in several steps, as follows:

(1) Our first claim is that the group morphism $SU_2 \to GL_4(\mathbb{R})$ constructed in Proposition 8.3 is in fact a morphism $SU_2 \to O_4$. In order to prove this, recall the following formula, valid for any $U \in SU_2$, from the proof of Proposition 8.5:

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

We want to prove that the matrices $T_U \in GL_4(\mathbb{R})$ are orthogonal, and in view of the above formula, it is enough to prove that we have:

$$T_U^* = (T_U)^t$$

So, let us prove this. For any two matrices $M, N \in E$, we have:

$$\begin{aligned} < T_{U^*}(M), N > &= < U^*MU, N > \\ &= tr(U^*MUN) \\ &= tr(MUNU^*) \end{aligned}$$

On the other hand, we have as well the following formula:

$$\begin{aligned} < (T_U)^t(M), N > &= < M, T_U(N) > \\ &= < M, UNU^* > \\ &= tr(MUNU^*) \end{aligned}$$

Thus we have indeed $T_U^* = (T_U)^t$, which proves our $SU_2 \to O_4$ claim.

(2) In order now to finish, recall that we have by definition $c_1 = 1$, as a matrix. Thus, the action of SU_2 on the vector $c_1 \in E$ is given by:

$$T_U(c_1) = Uc_1U^* = UU^* = 1 = c_1$$

We conclude that $c_1 \in E$ is invariant under SU_2, and by orthogonality the following subspace of E must be invariant as well under the action of SU_2:

$$e_1^\perp = span_{\mathbb{R}}(c_2, c_3, c_4)$$

Now if we call this subspace F, and we identify $F \simeq \mathbb{R}^3$ by using the basis c_2, c_3, c_4, we obtain by restriction to F a morphism of groups as follows:

$$SU_2 \to O_3$$

But since this morphism is continuous and SU_2 is connected, its image must be connected too. Now since the target group decomposes as $O_3 = SO_3 \sqcup (-SO_3)$, and $1 \in SU_2$ gets mapped to $1 \in SO_3$, the whole image must lie inside SO_3, and we are done. □

The above result is quite interesting, because we will see in a moment that the morphism $SU_2 \to SO_3$ constructed there is surjective. Thus, we will have a way of parametrizing the elements $V \in SO_3$ by elements $U \in SO_2$, and so ultimately by parameters

$(x,y,z,t) \in S^3_{\mathbb{R}}$. In order to work out all this, let us start with the following result, coming as a continuation of Proposition 8.5, independently of Theorem 8.6:

THEOREM 8.7. *With respect to the standard basis c_1, c_2, c_3, c_4 of the vector space $\mathbb{R}^4 = span(c_1, c_2, c_3, c_4)$, the morphism $T : SU_2 \to GL_4(\mathbb{R})$ is given by:*

$$T_U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & x^2+y^2-z^2-t^2 & 2(yz-xt) & 2(xz+yt) \\ 0 & 2(xt+yz) & x^2+z^2-y^2-t^2 & 2(zt-xy) \\ 0 & 2(yt-xz) & 2(xy+zt) & x^2+t^2-y^2-z^2 \end{pmatrix}$$

Thus, when looking at T as a group morphism $SU_2 \to O_4$, what we have in fact is a group morphism $SU_2 \to O_3$, and even $SU_2 \to SO_3$.

PROOF. With notations from Proposition 8.5 and its proof, let us first look at the action $L : SU_2 \curvearrowright \mathbb{R}^4$ by left multiplication, which is by definition given by:

$$L_U(M) = UM$$

In order to compute the matrix of this action, let us write, as usual:

$$U = xc_1 + yc_2 + zc_3 + tc_4$$

$$M = ac_1 + bc_2 + cc_3 + dc_4$$

By using the multiplication formulae in Theorem 8.4, we obtain:

$$\begin{aligned} UM &= (xc_1 + yc_2 + zc_3 + tc_4)(ac_1 + bc_2 + cc_3 + dc_4) \\ &= (xa - yb - zc - td)c_1 \\ &+ (xb + ya + zd - tc)c_2 \\ &+ (xc - yd + za + tb)c_3 \\ &+ (xd + yc - zb + ta)c_4 \end{aligned}$$

We conclude that the matrix of the left action considered above is:

$$L_U = \begin{pmatrix} x & -y & -z & -t \\ y & x & -t & z \\ z & t & x & -y \\ t & -z & y & x \end{pmatrix}$$

Similarly, let us look now at the action $R : SU_2 \curvearrowright \mathbb{R}^4$ by right multiplication, which is by definition given by the following formula:

$$R_U(M) = MU^*$$

In order to compute the matrix of this action, let us write, as before:

$$U = xc_1 + yc_2 + zc_3 + tc_4$$

$$M = ac_1 + bc_2 + cc_3 + dc_4$$

By using the multiplication formulae in Theorem 8.4, we obtain:

$$\begin{aligned} MU^* &= (ac_1+bc_2+cc_3+dc_4)(xc_1-yc_2-zc_3-tc_4)\\ &= (ax+by+cz+dt)c_1\\ &+ (-ay+bx-ct+dz)c_2\\ &+ (-az+bt+cx-dy)c_3\\ &+ (-at-bz+cy+dx)c_4 \end{aligned}$$

We conclude that the matrix of the right action considered above is:

$$R_U=\begin{pmatrix} x & y & z & t\\ -y & x & -t & z\\ -z & t & x & -y\\ -t & -z & y & x \end{pmatrix}$$

Now by composing, the matrix of the adjoint matrix in the statement is:

$$\begin{aligned} T_U &= R_UL_U\\ &= \begin{pmatrix} x & y & z & t\\ -y & x & -t & z\\ -z & t & x & -y\\ -t & -z & y & x \end{pmatrix}\begin{pmatrix} x & -y & -z & -t\\ y & x & -t & z\\ z & t & x & -y\\ t & -z & y & x \end{pmatrix}\\ &= \begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & x^2+y^2-z^2-t^2 & 2(yz-xt) & 2(xz+yt)\\ 0 & 2(xt+yz) & x^2+z^2-y^2-t^2 & 2(zt-xy)\\ 0 & 2(yt-xz) & 2(xy+zt) & x^2+t^2-y^2-z^2 \end{pmatrix} \end{aligned}$$

Thus, we have indeed the formula in the statement. As for the remaining assertions, these are all clear either from this formula, or from Theorem 8.6. □

We can now formulate the Euler-Rodrigues result, as follows:

THEOREM 8.8. *We have a double cover map, obtained via the adjoint representation,*

$$SU_2\to SO_3$$

and this map produces the Euler-Rodrigues formula

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

for the generic elements of SO_3.

PROOF. We know from the above that we have a group morphism $SU_2\to SO_3$, given by the formula in the statement, and the problem now is that of proving that this is a double cover map, in the sense that it is surjective, and with kernel $\{\pm 1\}$.

(1) Regarding the kernel, this is elementary to compute, as follows:

$$\begin{aligned}\ker(SU_2 \to SO_3) &= \left\{U \in SU_2 \middle| T_U(M) = M, \forall M \in E\right\}\\ &= \left\{U \in SU_2 \middle| UM = MU, \forall M \in E\right\}\\ &= \left\{U \in SU_2 \middle| Uc_i = c_iU, \forall i\right\}\\ &= \{\pm 1\}\end{aligned}$$

(2) Thus, we are done with this, and as a side remark here, this result shows that our morphism $SU_2 \to SO_3$ is ultimately a morphism as follows:

$$PU_2 \subset SO_3 \quad , \quad PU_2 = SU_2/\{\pm 1\}$$

Here P stands for "projective", and it is possible to say more about the construction $G \to PG$, which can be performed for any subgroup $G \subset U_N$. But we will not get here into this, our next goal being anyway that of proving that we have $PU_2 = SO_3$.

(3) We must prove now that the morphism $SU_2 \to SO_3$ is surjective. This is something non-trivial, and there are several advanced proofs for this, as follows:

– A first proof is by using Lie theory. To be more precise, the tangent spaces at 1 of both SU_2 and SO_3 can be explicitly computed, by doing some linear algebra, and the morphism $SU_2 \to SO_3$ follows to be surjective around 1, and then globally.

– Another proof is via representation theory, as developed above, in chapters 5-7. Indeed, the representations of SU_2 and SO_3 are subject to very similar formulae, called Clebsch-Gordan rules, and this shows that $SU_2 \to SO_3$ is surjective.

– Yet another advanced proof, which is actually quite bordeline for what can be called "proof", is by using the ADE/McKay classification of the subgroups $G \subset SO_3$, which shows that there is no room strictly inside SO_3 for something as big as PU_2.

(4) In short, with some good knowledge of group theory, we are done. However, this is not our case, and we will present in what follows a more pedestrian proof, which was actually the original proof, based on the fact that any rotation $U \in SO_3$ has an axis.

(5) As a first computation, let us prove that any rotation $U \in Im(SU_2 \to SO_3)$ has an axis. We must look for fixed points of such rotations, and by linearity it is enough to look for fixed points belonging to the sphere $S^2_{\mathbb{R}} \subset \mathbb{R}^3$. Now recall that in our picture for the quotient map $SU_2 \to SO_3$, the space $\mathbb{R}^3$ appears as $F = span_{\mathbb{R}}(c_2, c_3, c_4)$, naturally embedded into the space $\mathbb{R}^4$ appearing as $E = span_{\mathbb{R}}(c_1, c_2, c_3, c_4)$. Thus, we must look for fixed points belonging to the sphere $S^3_{\mathbb{R}} \subset \mathbb{R}^4$ whose first coordinate vanishes. But, in our $\mathbb{R}^4 = E$ picture, this sphere $S^3_{\mathbb{R}}$ is the group SU_2. Thus, we must look for fixed points $V \in SU_2$ whose first coordinate with respect to c_1, c_2, c_3, c_4 vanishes, which amounts in saying that the diagonal entries of V must be purely imaginary numbers.

(6) Long story short, via our various identifications, we are led into solving the equation $UV = VU$ with $U, V \in SU_2$, and with V having a purely imaginary diagonal. So, with standard notations for SU_2, we must solve the following equation, with $p \in i\mathbb{R}$:

$$\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \begin{pmatrix} p & q \\ -\bar{q} & \bar{p} \end{pmatrix} = \begin{pmatrix} p & q \\ -\bar{q} & \bar{p} \end{pmatrix} \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$$

(7) But this is something which is routine. Indeed, by identifying coefficients we obtain the following equations, each appearing twice:

$$b\bar{q} = \bar{b}q \quad , \quad b(p - \bar{p}) = (a - \bar{a})q$$

In the case $b = 0$ the only equation which is left is $q = 0$, and reminding that we must have $p \in i\mathbb{R}$, we do have solutions, namely two of them, as follows:

$$V = \pm \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$$

(8) In the remaining case $b \neq 0$, the first equation reads $b\bar{q} \in \mathbb{R}$, so we must have $q = \lambda b$ with $\lambda \in \mathbb{R}$. Now with this substitution made, the second equation reads $p - \bar{p} = \lambda(a - \bar{a})$, and since we must have $p \in i\mathbb{R}$, this gives $2p = \lambda(a - \bar{a})$. Thus, our equations are:

$$q = \lambda b \quad , \quad p = \lambda \cdot \frac{a - \bar{a}}{2}$$

Getting back now to our problem about finding fixed points, assuming $|a|^2 + |b|^2 = 1$ we must find $\lambda \in \mathbb{R}$ such that the above numbers p, q satisfy $|p|^2 + |q|^2 = 1$. But:

$$\begin{aligned} |p|^2 + |q|^2 &= |\lambda b|^2 + \left| \lambda \cdot \frac{a - \bar{a}}{2} \right|^2 \\ &= \lambda^2(|b|^2 + Im(a)^2) \\ &= \lambda^2(1 - Re(a)^2) \end{aligned}$$

Thus, we have again two solutions to our fixed point problem, given by:

$$\lambda = \pm \frac{1}{\sqrt{1 - Re(a)^2}}$$

(9) Summarizing, we have proved that any rotation $U \in Im(SU_2 \to SO_3)$ has an axis, and with the direction of this axis, corresponding to a pair of opposite points on the sphere $S^2_{\mathbb{R}} \subset \mathbb{R}^3$, being given by the above formulae, via $S^2_{\mathbb{R}} \subset S^3_{\mathbb{R}} = SU_2$.

(10) In order to finish, we must argue that any rotation $U \in SO_3$ has an axis. But this follows for instance from some topology, by using the induced map $S^2_{\mathbb{R}} \to S^2_{\mathbb{R}}$. Now since $U \in SO_3$ is uniquely determined by its rotation axis, which can be regarded as a point of $S^2_{\mathbb{R}}/\{\pm 1\}$, plus its rotation angle $t \in [0, 2\pi)$, by using $S^2_{\mathbb{R}} \subset S^3_{\mathbb{R}} = SU_2$ as in (9) we are led to the conclusion that U is uniquely determined by an element of $SU_2/\{\pm 1\}$, and so appears indeed via the Euler-Rodrigues formula, as desired. □

So long for the Euler-Rodrigues formula. As already mentioned, all the above is just the tip of the iceberg, and there are many more things that can be said, which are all interesting, and worth learning. We will be back to this.

Regarding now O_3, the extension from SO_3 is very simple, as follows:

THEOREM 8.9. *We have the Euler-Rodrigues formula*

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

for the generic elements of O_3.

PROOF. This follows from Theorem 8.8, because the determinant of an orthogonal matrix $U\in O_3$ must satisfy $\det U=\pm1$, and in the case $\det U=-1$, we have:

$$\det(-U)=(-1)^3\det U=-\det U=1$$

Thus, assuming $\det U=-1$, we can therefore rescale U into an element $-U\in SO_3$, and this leads to the conclusion in the statement. □

8c. Clebsch-Gordan

As a last piece of Lie group theory, we are now in position of dealing, in a quite conceptual way, with both the representations and the subgroups of SU_2 and SO_3. The idea will be, as before, that of using the following key isomorphism:

$$SU_2\simeq S^3_{\mathbb{R}}$$

In order to get started with our study, we would first like to understand how the various products of coordinates integrate over 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 $\cos t,\sin t$. We can first integrate arbitrary powers of these coordinates, as follows:

PROPOSITION 8.10. *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 I_p. We have:

$$\begin{aligned}(\cos^p t\sin t)' &= p\cos^{p-1}t(-\sin t)\sin t+\cos^p t\cos t\\ &= p\cos^{p+1}t-p\cos^{p-1}t+\cos^{p+1}t\\ &= (p+1)\cos^{p+1}t-p\cos^{p-1}t\end{aligned}$$

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:

$$I_0=\int_0^{\pi/2}1\,dt=\frac{\pi}{2}$$

Also, at $p=1$ we have the following formula:

$$I_1=\int_0^{\pi/2}\cos t\,dt=1$$

Thus, we obtain the result, by recurrence. As for the second formula, regarding $\sin t$, this follows from the first formula, with the change of variables $t=\frac{\pi}{2}-s$. □

Next, we have the following formula, which is more general:

THEOREM 8.11. *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. Let I_{pq} be the integral in the statement. 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 the formulae in chapter 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. □

As an application of Theorem 8.11, we can now compute the volumes of spheres:

THEOREM 8.12. *The volume of the unit sphere in $\mathbb{R}^N$ is given by*

$$V = \left(\frac{\pi}{2}\right)^{[N/2]} \frac{2^N}{(N+1)!!}$$

with our usual double factorial convention, $N!! = (N-1)(N-3)(N-5)\ldots$

PROOF. If we denote by B^+ the positive part of the unit sphere, we have:

$$\begin{aligned}
V^+ &= \int_{B^+} 1 \\
&= \int_0^1 \int_0^{\pi/2} \ldots \int_0^{\pi/2} r^{N-1} \sin^{N-2} t_1 \ldots \sin t_{N-2}\, dr dt_1 \ldots dt_{N-1} \\
&= \int_0^1 r^{N-1}\, dr \int_0^{\pi/2} \sin^{N-2} t_1\, dt_1 \ldots \int_0^{\pi/2} \sin t_{N-2} dt_{N-2} \int_0^{\pi/2} 1 dt_{N-1} \\
&= \frac{1}{N} \times \left(\frac{\pi}{2}\right)^{[N/2]} \times \frac{(N-2)!!}{(N-1)!!} \cdot \frac{(N-3)!!}{(N-2)!!} \ldots \frac{2!!}{3!!} \cdot \frac{1!!}{2!!} \cdot 1 \\
&= \frac{1}{N} \times \left(\frac{\pi}{2}\right)^{[N/2]} \times \frac{1}{(N-1)!!} \\
&= \left(\frac{\pi}{2}\right)^{[N/2]} \frac{1}{(N+1)!!}
\end{aligned}$$

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

Next, we can now integrate over the spheres, as follows:

THEOREM 8.13. *The polynomial integrals over the unit sphere $S_{\mathbb{R}}^{N-1} \subset \mathbb{R}^N$, with respect to the normalized, mass 1 measure, are given by the following formula,*

$$\int_{S_{\mathbb{R}}^{N-1}} x_1^{k_1} \ldots x_N^{k_N}\, dx = \frac{(N-1)!! k_1!! \ldots k_N!!}{(N+\Sigma k_i - 1)!!}$$

valid when all exponents k_i are even. If an exponent is odd, the integral vanishes.

PROOF. Assume first that one of the exponents k_i is odd. We can make then the following change of variables, which shows that the integral in the statement vanishes:

$$x_i \to -x_i$$

Assume now that all the exponents k_i are even. As a first observation, the result holds indeed at $N = 2$, due to the formula from Theorem 8.11, which reads:

$$\begin{aligned}
\int_0^{\pi/2} \cos^p t \sin^q t\, dt &= \left(\frac{\pi}{2}\right)^{\varepsilon(p)\varepsilon(q)} \frac{p!!q!!}{(p+q+1)!!} \\
&= \frac{p!!q!!}{(p+q+1)!!}
\end{aligned}$$

Indeed, this formula computes the integral in the statement over the first quadrant. But since the exponents $p, q \in \mathbb{N}$ are assumed to be even, the integrals over the other quadrants are given by the same formula, so when averaging we obtain the result.

In the general case now, where the dimension $N \in \mathbb{N}$ is arbitrary, the integral in the statement can be written in spherical coordinates, as follows:

$$I = \frac{2^N}{A} \int_0^{\pi/2} \ldots \int_0^{\pi/2} x_1^{k_1} \ldots x_N^{k_N} \, J \, dt_1 \ldots dt_{N-1}$$

Here A is the area 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. According to Theorem 8.12, the normalization constant in front of the integral is:

$$\frac{2^N}{A} = \left(\frac{2}{\pi}\right)^{[N/2]} (N-1)!!$$

As for the unnormalized integral, this is given by:

$$\begin{aligned} I' = \int_0^{\pi/2} \ldots \int_0^{\pi/2} \quad & (\cos t_1)^{k_1} (\sin t_1 \cos t_2)^{k_2} \\ & \vdots \\ & (\sin t_1 \sin t_2 \ldots \sin t_{N-2} \cos t_{N-1})^{k_{N-1}} \\ & (\sin t_1 \sin t_2 \ldots \sin t_{N-2} \sin t_{N-1})^{k_N} \\ & \sin^{N-2} t_1 \sin^{N-3} t_2 \ldots \sin^2 t_{N-3} \sin t_{N-2} \\ & dt_1 \ldots dt_{N-1} \end{aligned}$$

By rearranging the terms, we obtain:

$$\begin{aligned} I' \;=\; & \int_0^{\pi/2} \cos^{k_1} t_1 \sin^{k_2+\ldots+k_N+N-2} t_1 \, dt_1 \\ & \int_0^{\pi/2} \cos^{k_2} t_2 \sin^{k_3+\ldots+k_N+N-3} t_2 \, dt_2 \\ & \vdots \\ & \int_0^{\pi/2} \cos^{k_{N-2}} t_{N-2} \sin^{k_{N-1}+k_N+1} t_{N-2} \, dt_{N-2} \\ & \int_0^{\pi/2} \cos^{k_{N-1}} t_{N-1} \sin^{k_N} t_{N-1} \, dt_{N-1} \end{aligned}$$

Now by using the above-mentioned formula at $N=2$, this gives:

$$\begin{aligned} I' &= \frac{k_1!!(k_2+\ldots+k_N+N-2)!!}{(k_1+\ldots+k_N+N-1)!!}\left(\frac{\pi}{2}\right)^{\varepsilon(N-2)} \\ &\quad \frac{k_2!!(k_3+\ldots+k_N+N-3)!!}{(k_2+\ldots+k_N+N-2)!!}\left(\frac{\pi}{2}\right)^{\varepsilon(N-3)} \\ &\quad \vdots \\ &\quad \frac{k_{N-2}!!(k_{N-1}+k_N+1)!!}{(k_{N-2}+k_{N-1}+l_N+2)!!}\left(\frac{\pi}{2}\right)^{\varepsilon(1)} \\ &\quad \frac{k_{N-1}!!k_N!!}{(k_{N-1}+k_N+1)!!}\left(\frac{\pi}{2}\right)^{\varepsilon(0)} \end{aligned}$$

Now let F be the part involving the double factorials, and P be the part involving the powers of $\pi/2$, so that $I'=F\cdot P$. Regarding F, by cancelling terms we have:

$$F=\frac{k_1!!\ldots k_N!!}{(\Sigma k_i+N-1)!!}$$

As in what regards P, by summing the exponents, we obtain $P=\left(\frac{\pi}{2}\right)^{[N/2]}$. We can now put everything together, and we obtain:

$$\begin{aligned} I &= \frac{2^N}{A}\times F\times P \\ &= \left(\frac{2}{\pi}\right)^{[N/2]}(N-1)!!\times\frac{k_1!!\ldots k_N!!}{(\Sigma k_i+N-1)!!}\times\left(\frac{\pi}{2}\right)^{[N/2]} \\ &= \frac{(N-1)!!k_1!!\ldots k_N!!}{(\Sigma k_i+N-1)!!} \end{aligned}$$

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

Good news, we can now come back to SU_2, and we have the following result:

THEOREM 8.14. *The irreducible representations of SU_2 are all self-adjoint, and can be labelled by positive integers, with their fusion rules being as follows,*

$$r_k\otimes r_l=r_{|k-l|}+r_{|k-l|+2}+\ldots+r_{k+l}$$

called Clebsch-Gordan rules. The corresponding dimensions are $\dim r_k=k+1$.

PROOF. There are several proofs for this fact, the simplest one, with the knowledge that we have, being via purely algebraic methods, as follows:

(1) Our first claim is that we have the following estimate, telling us that the even moments of the main character are smaller than the Catalan numbers:

$$\int_{SU_2}\chi^{2k}\leq C_k$$

But this is something which is elementary, obtained by using $SU_2 \simeq S^3_{\mathbb{R}}$ and standard spherical integrals, and with the stronger statement that we have in fact equality $=$. However, for the purposes of what follows, the above $\leq$ estimate will do.

(2) Alternatively, the above estimate can be deduced with purely algebraic methods, by using an easiness type argument for SU_2, as follows:

$$\begin{aligned}\int_{SU_2}\chi^{2k} &= \dim(Fix(u^{\otimes 2k}))\\ &= \dim\left(span\left(T'_\pi\middle|\pi\in NC_2(2k)\right)\right)\\ &\leq |NC_2(2k)|\\ &= C_k\end{aligned}$$

To be more precise, SU_2 is not exactly easy, but rather "super-easy", coming from a different implementation $\pi\to T'_\pi$ of the pairings, involving some signs. And with this being proved exactly as the Brauer theorem for O_N, with modifications where needed.

(3) Long story short, we have our estimate in (1), and this is all that we need. Our claim is that we can construct, by recurrence on $k\in\mathbb{N}$, a sequence r_k of irreducible, self-adjoint and distinct representations of SU_2, satisfying:

$$r_0=1\quad,\quad r_1=u\quad,\quad r_k+r_{k-2}=r_{k-1}\otimes r_1$$

Indeed, assume that $r_0,\ldots,r_{k-1}$ are constructed, and let us construct r_k. We have:

$$r_{k-1}+r_{k-3}=r_{k-2}\otimes r_1$$

Thus $r_{k-1}\subset r_{k-2}\otimes r_1$, and since r_{k-2} is irreducible, by Frobenius we have:

$$r_{k-2}\subset r_{k-1}\otimes r_1$$

We conclude there exists a certain representation r_k such that:

$$r_k+r_{k-2}=r_{k-1}\otimes r_1$$

(4) By recurrence, r_k is self-adjoint. Now observe that according to our recurrence formula, we can split $u^{\otimes k}$ as a sum of the following type, with positive coefficients:

$$u^{\otimes k}=c_kr_k+c_{k-2}r_{k-2}+\ldots$$

We conclude by Peter-Weyl that we have an inequality as follows, with equality precisely when r_k is irreducible, and non-equivalent to the other summands r_i:

$$\sum_i c_i^2\leq\dim(End(u^{\otimes k}))$$

(5) But by (1) the number on the right is $\leq C_k$, and some straightforward combinatorics, based on the fusion rules, shows that the number on the left is C_k as well:

$$C_k=\sum_i c_i^2\leq\dim(End(u^{\otimes k}))=\int_{SU_2}\chi^{2k}\leq C_k$$

Thus we have equality in our estimate, so our representation r_k is irreducible, and non-equivalent to $r_{k-2},r_{k-4},\ldots$ Moreover, this representation r_k is not equivalent to $r_{k-1},r_{k-3},\ldots$ either, with this coming from $r_p\subset u^{\otimes p}$ for any p, and from:

$$\dim(Fix(u^{\otimes 2s+1}))=\int_{SU_2}\chi^{2s+1}=0$$

(6) Thus, we proved our claim. Now since each irreducible representation of SU_2 appears into some $u^{\otimes k}$, and we know how to decompose each $u^{\otimes k}$ into sums of representations r_k, these representations r_k are all the irreducible representations of SU_2, and we are done with the main assertion. As for the dimension formula, this is clear. □

Regarding now SO_3, we have here a similar result, as follows:

THEOREM 8.15. *The irreducible representations of SO_3 are all self-adjoint, and can be labelled by positive integers, with their fusion rules being as follows,*

$$r_k\otimes r_l=r_{|k-l|}+r_{|k-l|+1}+\ldots+r_{k+l}$$

also called Clebsch-Gordan rules. The corresponding dimensions are $\dim r_k=2k+1$.

PROOF. As before with SU_2, there are many possible proofs here, which are all instructive. Here is our take on the subject, in the spirit of our proof for SU_2:

(1) Our first claim is that we have the following formula, telling us that the moments of the main character equal the Catalan numbers:

$$\int_{SO_3}\chi^k=C_k$$

But this is something that we know from before, coming from Euler-Rodrigues. Alternatively, this can be deduced as well from Tannakian duality, a bit as for SU_2.

(2) Our claim now is that we can construct, by recurrence on $k\in\mathbb{N}$, a sequence r_k of irreducible, self-adjoint and distinct representations of SO_3, satisfying:

$$r_0=1\quad,\quad r_1=u-1\quad,\quad r_k+r_{k-1}+r_{k-2}=r_{k-1}\otimes r_1$$

Indeed, assume that $r_0,\ldots,r_{k-1}$ are constructed, and let us construct r_k. The Frobenius trick from the proof for SU_2 will no longer work, due to some technical reasons, so we have to invoke (1). To be more precise, by integrating characters we obtain:

$$r_{k-1},r_{k-2}\subset r_{k-1}\otimes r_1$$

Thus there exists a representation r_k such that:

$$r_{k-1} \otimes r_1 = r_k + r_{k-1} + r_{k-2}$$

(3) Once again by integrating characters, we conclude that r_k is irreducible, and non-equivalent to $r_1, \ldots, r_{k-1}$, and this proves our claim. Also, since any irreducible representation of SO_3 must appear in some tensor power of u, and we can decompose each $u^{\otimes k}$ into sums of representations r_p, we conclude that these representations r_p are all the irreducible representations of SO_3. Finally, the dimension formula is clear. □

There are of course many other things that can be said about SU_2 and SO_3. For instance, with the proof of Theorem 8.14 and Theorem 8.15 done in a purely algebraic fashion, by using the super-easiness property of SU_2 and SO_3, the Euler-Rodrigues formula can be deduced afterwards from this, without any single computation, the argument being that by Peter-Weyl the embedding $PU_2 \subset SO_3$ must be indeed an equality.

8d. McKay subgroups

McKay subgroups.

8e. Exercises

Exercises:

Exercise 8.16.

Exercise 8.17.

Exercise 8.18.

Exercise 8.19.

Exercise 8.20.

Exercise 8.21.

Exercise 8.22.

Exercise 8.23.

Bonus exercise.

Part III

Analytic aspects

It was dark all around, there was frost in the ground
When the tigers broke free
And no one survived
From the Royal Fusiliers Company Z

CHAPTER 9

Character laws

9a. Poisson laws

Welcome to analysis. You would probably say, not much analysis to do on a finite group G. But this is wrong, with many interesting computations, which require some good analysis knowledge, being possible to invent. We will discuss all this in the present Part III, with an overview of what can be done, and with the main results on the subject explained. And, coming after, Part IV will be actually quite analytic too.

As a first topic of discussion, we would like to know more about something quite mysterious, that we discovered a long time ago, in chapter 2, namely:

FACT 9.1. *For the symmetric group S_N, the number of fixed points, regarded as variable*

$$\chi : S_N \to \mathbb{N}$$

follows with $N \to \infty$ limit the Poisson law p_1. More generally, given a number $t \in (0, 1]$, the number of fixed points among $\{1, \ldots, [tN]\}$, regarded as variable

$$\chi_t : S_N \to \mathbb{N}$$

follows with $N \to \infty$ limit the Poisson law p_t.

So, what to do with this? Many things. To start with, in order to know what we are talking about, we need a crash course in discrete probability. Let us start with:

DEFINITION 9.2. *The Poisson law of parameter 1 is the following measure,*

$$p_1 = \frac{1}{e} \sum_{k \geq 0} \frac{\delta_k}{k!}$$

and the Poisson law of parameter $t > 0$ is the following measure,

$$p_t = e^{-t} \sum_{k \geq 0} \frac{t^k}{k!} \, \delta_k$$

with the letter "p" standing for Poisson.

We will see in the moment why these measures appear a bit everywhere, in the discrete context, the reasons for this coming from the Poisson Limit Theorem (PLT). For the moment, let us first develop some general theory. We first have:

PROPOSITION 9.3. *The mean and variance of p_t are given by:*

$$E = t \quad , \quad V = t$$

In particular for the Poisson law p_1 we have $E = 1, V = 1$.

PROOF. We have two computations to be performed, as follows:

(1) Regarding the mean, this can be computed as follows:

$$\begin{aligned} E &= e^{-t}\sum_{k\geq 0}\frac{t^k}{k!}\cdot k \\ &= e^{-t}\sum_{k\geq 1}\frac{t^k}{(k-1)!} \\ &= e^{-t}\sum_{l\geq 0}\frac{t^{l+1}}{l!} \\ &= te^{-t}\sum_{l\geq 0}\frac{t^l}{l!} \\ &= t \end{aligned}$$

(2) For the variance, we first compute the second moment, as follows:

$$\begin{aligned} M_2 &= e^{-t}\sum_{k\geq 0}\frac{t^k}{k!}\cdot k^2 \\ &= e^{-t}\sum_{k\geq 1}\frac{t^k k}{(k-1)!} \\ &= e^{-t}\sum_{l\geq 0}\frac{t^{l+1}(l+1)}{l!} \\ &= te^{-t}\sum_{l\geq 0}\frac{t^l l}{l!} + te^{-t}\sum_{l\geq 0}\frac{t^l}{l!} \\ &= te^{-t}\sum_{l\geq 1}\frac{t^l}{(l-1)!} + t \\ &= t^2e^{-t}\sum_{m\geq 0}\frac{t^m}{m!} + t \\ &= t^2 + t \end{aligned}$$

Thus the variance is $V = M_2 - E^2 = (t^2 + t) - t^2 = t$, as claimed. □

At the theoretical level now, we first have the following result:

THEOREM 9.4. *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. By using $\delta_k * \delta_l = \delta_{k+l}$ and the binomial formula, we obtain:

$$\begin{aligned}
p_s * p_t &= e^{-s} \sum_k \frac{s^k}{k!} \delta_k * e^{-t} \sum_l \frac{t^l}{l!} \delta_l \\
&= e^{-s-t} \sum_n \delta_n \sum_{k+l=n} \frac{s^k t^l}{k!l!} \\
&= e^{-s-t} \sum_n \frac{\delta_n}{n!} \sum_{k+l=n} \frac{n!}{k!l!} s^k t^l \\
&= e^{-s-t} \sum_n \frac{(s+t)^n}{n!} \delta_n \\
&= p_{s+t}
\end{aligned}$$

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

Next in line, we have the following result, which is fundamental as well:

THEOREM 9.5. *The Poisson laws appear as formal 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 on the right is:

$$\begin{aligned}
\mu &= \sum_k \frac{t^k}{k!} \sum_{r+s=k} (-1)^s \frac{k!}{r!s!} \delta_r \\
&= \sum_k t^k \sum_{r+s=k} (-1)^s \frac{\delta_r}{r!s!} \\
&= \sum_r \frac{t^r \delta_r}{r!} \sum_s \frac{(-1)^s t^s}{s!} \\
&= \frac{1}{e^t} \sum_r \frac{t^r \delta_r}{r!} \\
&= p_t
\end{aligned}$$

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

Regarding now the Fourier transform computation, this is as follows:

THEOREM 9.6. *The Fourier transform of p_t is given by*

$$F_{p_t}(y) = \exp\left((e^{iy} - 1)t\right)$$

for any $t > 0$.

PROOF. We have indeed the following computation:

$$\begin{aligned} F_{p_t}(y) &= e^{-t} \sum_k \frac{t^k}{k!} F_{\delta_k}(y) \\ &= e^{-t} \sum_k \frac{t^k}{k!} e^{iky} \\ &= e^{-t} \sum_k \frac{(e^{iy}t)^k}{k!} \\ &= \exp(-t)\exp(e^{iy}t) \\ &= \exp\left((e^{iy} - 1)t\right) \end{aligned}$$

Thus, we obtain the formula in the statement. □

Observe that the above result provides us with an alternative proof for Theorem 9.4, due to the fact that the logarithm of the Fourier transform is linear in t.

We can now establish the Poisson Limit Theorem, as follows:

THEOREM 9.7 (PLT). *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 ν_n the measure under the convolution sign. We have the following computation, for the Fourier transform of the limit:

$$\begin{aligned} F_{\delta_r}(y) = e^{iry} &\implies F_{\nu_n}(y) = \left(1 - \frac{t}{n}\right) + \frac{t}{n}\,e^{iy} \\ &\implies F_{\nu_n^{*n}}(y) = \left(\left(1 - \frac{t}{n}\right) + \frac{t}{n}\,e^{iy}\right)^n \\ &\implies F_{\nu_n^{*n}}(y) = \left(1 + \frac{(e^{iy} - 1)t}{n}\right)^n \\ &\implies F(y) = \exp\left((e^{iy} - 1)t\right) \end{aligned}$$

Thus, we obtain indeed the Fourier transform of p_t, as desired. □

At the level of moments now, things are quite subtle. We first have:

THEOREM 9.8. *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:

$$M_k = \frac{1}{e} \sum_r \frac{r^k}{r!}$$

We therefore have the following recurrence formula for these moments:

$$\begin{aligned} M_{k+1} &= \frac{1}{e} \sum_r \frac{(r+1)^{k+1}}{(r+1)!} \\ &= \frac{1}{e} \sum_r \frac{r^k}{r!} \left(1 + \frac{1}{r}\right)^k \\ &= \frac{1}{e} \sum_r \frac{r^k}{r!} \sum_s \binom{k}{s} r^{-s} \\ &= \sum_s \binom{k}{s} \cdot \frac{1}{e} \sum_r \frac{r^{k-s}}{r!} \\ &= \sum_s \binom{k}{s} M_{k-s} \end{aligned}$$

With this done, 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 s neighbors for 1, among the k numbers available, and then partitioning the $k - s$ elements left. Thus, we have:

$$B_{k+1} = \sum_s \binom{k}{s} B_{k-s}$$

Thus, our moments M_k satisfy the same recurrence as the numbers B_k. Regarding now the initial values, in what concerns the first moment of p_1, we have:

$$M_1 = \frac{1}{e} \sum_r \frac{r}{r!} = 1$$

Also, by using the above recurrence for the numbers M_k, we obtain from this:

$$M_2 = \sum_s \binom{1}{s} M_{k-s} = 1 + 1 = 2$$

On the other hand, $B_1 = 1$ and $B_2 = 2$. Thus we obtain $M_k = B_k$, as claimed. □

More generally now, we have the following result, dealing with the case $t > 0$:

THEOREM 9.9. *The moments of p_t with $t > 0$ are given by*

$$M_k(p_t) = \sum_{\pi \in P(k)} t^{|\pi|}$$

where $|.|$ is the number of blocks.

PROOF. The moments of the Poisson law p_t with $t > 0$ are given by:

$$M_k = e^{-t} \sum_r \frac{t^r r^k}{r!}$$

We have the following recurrence formula for these moments:

$$\begin{aligned} M_{k+1} &= e^{-t} \sum_r \frac{t^{r+1}(r+1)^{k+1}}{(r+1)!} \\ &= e^{-t} \sum_r \frac{t^{r+1} r^k}{r!} \left(1 + \frac{1}{r}\right)^k \\ &= e^{-t} \sum_r \frac{t^{r+1} r^k}{r!} \sum_s \binom{k}{s} r^{-s} \\ &= \sum_s \binom{k}{s} \cdot e^{-t} \sum_r \frac{t^{r+1} r^{k-s}}{r!} \\ &= t \sum_s \binom{k}{s} M_{k-s} \end{aligned}$$

Regarding now the initial values, the first moment of p_t is given by:

$$M_1 = e^{-t} \sum_r \frac{t^r r}{r!} = e^{-t} \sum_r \frac{t^r}{(r-1)!} = t$$

Now by using the above recurrence we obtain from this:

$$M_2 = t \sum_s \binom{1}{s} M_{k-s} = t(1+t) = t + t^2$$

On the other hand, consider the numbers in the statement, namely:

$$S_k = \sum_{\pi \in P(k)} t^{|\pi|}$$

Since a partition of $\{1,\ldots,k+1\}$ appears by choosing s neighbors for 1, among the k numbers available, and then partitioning the $k-s$ elements left, we have:

$$S_{k+1}=t\sum_s\binom{k}{s}S_{k-s}$$

As for the initial values of these numbers, these are $S_1=t$, $S_2=t+t^2$. Thus the initial values coincide, and so these numbers are the moments of p_t, as stated. □

9b. Symmetric groups

Back now to group theory and to our Fact 9.1, we would like to make a connection with the representation theory machinery developed in Part II. So, let us formulate the following definition, fine-tuning the notion of character from there:

DEFINITION 9.10. *Given a subgroup $G\subset U_N$, we can talk about its main character:*

$$\chi:G\to\mathbb{C}\quad,\quad g\to Tr(g)$$

More generally, given a number $t\in(0,1]$, we can talk about the variable

$$\chi_t:G\to\mathbb{C}\quad,\quad g\to\sum_{i=1}^{[tN]}g_{ii}$$

called truncated character.

Observe the similarity with what we have in Fact 9.1. In fact, this is not just a similarity, but rather something very precise, the point being that we have:

THEOREM 9.11. *For the symmetric group S_N, regarded as group of permutation matrices, $S_N\subset O_N$, the main character counts the number of fixed points:*

$$\chi(g)=\#\left\{i\in\{1,\ldots,N\}\Big|\sigma(i)=i\right\}$$

More generally, the truncated characters count the following fixed points:

$$\chi_t(g)=\#\left\{i\in\{1,\ldots,[tN]\}\Big|\sigma(i)=i\right\}$$

The same goes for any $G\subset S_N$, regarded as a matrix group via $G\subset S_N\subset O_N$.

PROOF. According to our definition of the embedding $S_N\subset O_N$, given by the permutation matrices, the formula for the corresponding coordinates is as follows:

$$g_{ij}=\chi\left(\sigma\in S_N\Big|\sigma(j)=i\right)$$

But with this formula in hand, the character formulae in the statement follow from it, by summing over $i = j$. To be more precise, we have:

$$\begin{aligned}\chi_t(\sigma) &= \sum_{i=1}^{[tN]} \sigma_{ii}\\ &= \sum_{i=1}^{[tN]} \delta_{\sigma(i)i}\\ &= \#\left\{i \in \{1,\ldots,[tN]\}\Big|\sigma(i) = i\right\}\end{aligned}$$

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

The point now is that, with the above interpretation of characters in hand, what we have in Fact 9.1 reformulates into something quite conceptual, as follows:

FACT 9.12 (update). *For the symmetric group S_N, the main character*

$$\chi : S_N \to \mathbb{N}$$

follows with $N \to \infty$ limit the Poisson law p_1. More generally, the truncated character

$$\chi_t : S_N \to \mathbb{N}$$

follows with $N \to \infty$ limit the Poisson law p_t, for any $t \in (0, 1]$.

Very nice all this, and needless to say, this is not exactly a Fact, but rather a Theorem, coming from the computations in chapter 2. In what follows, in the remainder of this chapter, we will explore various versions and generalizations of this result.

As a first task, still staying with the symmetric group S_N itself, let us improve as well the proof that we have, for Fact 9.12. We can indeed replace the inclusion-exclusion computations from chapter 2 with something more conceptual and analytic, namely:

THEOREM 9.13. *Consider the symmetric group S_N, with its standard coordinates:*

$$g_{ij} = \chi\left(\sigma \in S_N\Big|\sigma(j) = i\right)$$

The products of these coordinates span the algebra $C(S_N)$, and we have

$$\int_{S_N} g_{i_1j_1}\ldots g_{i_kj_k} = \begin{cases}\frac{(N-|\ker i|)!}{N!} & \text{if } \ker i = \ker j\\ 0 & \text{otherwise}\end{cases}$$

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 the matrix coordinates 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 9.14. *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 can use here the integration formula in Theorem 9.13. With S_{kb} being the Stirling numbers, counting the partitions of $\{1, \ldots, k\}$

having exactly b blocks, we have indeed the following formula:

$$\begin{aligned}\int_{S_N}\chi_t^k &= \sum_{i_1\ldots i_k=1}^{[tN]}\int_{S_N} g_{i_1i_1}\cdots g_{i_ki_k}\\ &= \sum_{\pi\in P(k)}\frac{[tN]!}{([tN]-|\pi|!)}\cdot\frac{(N-|\pi|!)}{N!}\\ &= \sum_{b=1}^{[tN]}\frac{[tN]!}{([tN]-b)!}\cdot\frac{(N-b)!}{N!}\cdot S_{kb}\end{aligned}$$

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. □

As another result now regarding S_N, here is a useful related formula:

THEOREM 9.15. *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 $\{1,\ldots,s\}$:

$$\int_{S_N}(u_{11}+\ldots+u_{ss})^k=\frac{1}{N!}\sum_{f=0}^{s}m_ff^k$$

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 $\{1,\ldots,s\}$. But 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 in this way:

$$\begin{aligned}
\nu_{sN} &= \frac{1}{N!}\sum_{f=0}^{s}\binom{s}{f}\left(\sum_{k=0}^{s-f}(-1)^k\binom{s-f}{k}(N-f-k)!\right)\delta_f\\
&= \sum_{f=0}^{s}\sum_{k=0}^{s-f}(-1)^k\frac{1}{N!}\cdot\frac{s!}{f!(s-f)!}\cdot\frac{(s-f)!(N-f-k)!}{k!(s-f-k)!}\,\delta_f\\
&= \frac{s!}{N!}\sum_{f=0}^{s}\sum_{k=0}^{s-f}\frac{(-1)^k(N-f-k)!}{f!k!(s-f-k)!}\,\delta_f
\end{aligned}$$

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. □

Observe that the above formula is finer than most of our previous formulae, which were asymptotic, because it is valid at any $N\in\mathbb{N}$. We can use this formula as follows:

THEOREM 9.16. *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 can use indeed the formula in Theorem 9.15, as follows:

(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:

$$\begin{aligned}c_p&=\frac{(tN)!}{N!}\cdot\frac{(N-p)!}{(tN-p)!}\\&\simeq\frac{(tN)^{tN}}{N^N}\cdot\frac{(N-p)^{N-p}}{(tN-p)^{tN-p}}\\&=\left(\frac{tN}{tN-p}\right)^{tN-p}\left(\frac{N-p}{N}\right)^{N-p}\left(\frac{tN}{N}\right)^{p}\end{aligned}$$

But the last expression can be estimated by using the definition of the exponentials, and we obtain in this way the following estimate:

$$c_p\simeq e^pe^{-p}t^p=t^p$$

We can now compute the Fourier transform with respect to a variable y:

$$\begin{aligned}\mathcal{F}\left(\text{law}(u_{11}+\ldots+u_{ss})\right)&\simeq\sum_{p=0}^{s}t^p\cdot\frac{(e^y-1)^p}{p!}\\&=e^{t(e^y-1)}\end{aligned}$$

But this is precisely the Fourier transform of the Poisson law p_t, as desired. □

Let us discuss now, as an instructive variation of the above, the computation for the alternating group $A_N\subset S_N$. We first have the following result:

THEOREM 9.17. *Consider the alternating group A_N, regarded as group of permutation matrices, with its standard coordinates:*

$$g_{ij}=\chi\left(\sigma\in A_N\Big|\sigma(j)=i\right)$$

The products of these coordinates span the algebra $C(A_N)$, and we have

$$\int_{A_N}g_{i_1j_1}\ldots g_{i_kj_k}\simeq\begin{cases}\frac{(N-|\ker i|)!}{N!}&\text{if }\ker i=\ker j\\0&\text{otherwise}\end{cases}$$

with $N\to\infty$, 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. Regarding now the second assertion, the integrals in the statement are given by:

$$\int_{A_N} g_{i_1j_1}\ldots g_{i_kj_k}=\frac{1}{N!/2}\#\left\{\sigma\in A_N\Big|\sigma(j_1)=i_1,\ldots,\sigma(j_k)=i_k\right\}$$

Now observe that, as before for S_N, 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. But when assuming $N>>0$, and more specifically $N>k$, half of these bijections will be alternating, and so we have $(N-b)!/2$ solutions. Thus, the integral is:

$$\begin{aligned}\int_{A_N} g_{i_1j_1}\ldots g_{i_kj_k}&=\frac{1}{N!/2}\#\left\{\sigma\in A_N\Big|\sigma(j_1)=i_1,\ldots,\sigma(j_k)=i_k\right\}\\&=\frac{(N-b)!/2}{N!/2}\\&=\frac{(N-b)!}{N!}\end{aligned}$$

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

At the level of truncated characters now, we have the following result:

THEOREM 9.18. *For the alternating group $A_N\subset O_N$, regarded as a compact group of matrices, $A_N\subset O_N$, 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. We can use here the formula in Theorem 9.17. With S_{kb} being the Stirling numbers, counting the partitions of $\{1,\ldots,k\}$ having exactly b blocks, we have:

$$\begin{aligned}\int_{A_N}\chi_t^k&=\sum_{i_1\ldots i_k=1}^{[tN]}\int_{A_N}g_{i_1i_1}\ldots g_{i_ki_k}\\&\simeq\sum_{\pi\in P(k)}\frac{[tN]!}{([tN]-|\pi|!)}\cdot\frac{(N-|\pi|!)}{N!}\\&=\sum_{b=1}^{[tN]}\frac{[tN]!}{([tN]-b)!}\cdot\frac{(N-b)!}{N!}\cdot S_{kb}\end{aligned}$$

In particular with $N\to\infty$ we obtain the k-th moment of p_t, as desired. □

9c. Bessel laws

Regarding now the character laws for H_N, we can compute them by using the same method as for the symmetric group S_N, namely inclusion-exclusion, and we have:

THEOREM 9.19. *For the hyperoctahedral group $H_N \subset O_N$, the law of the variable*

$$\chi_t = \sum_{i=1}^{[tN]} g_{ii}$$

becomes 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:

$$u_{11} + \ldots + u_{ss} = \uparrow g - \downarrow g$$

Let us 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 then 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 we know well from chapter 11, that the probability of $\sigma \in S_N$ to have no fixed points is asymptotically given by:

$$P_0 = \frac{1}{e}$$

Thus the probability of $\sigma \in S_N$ to have m fixed points is asymptotically given by:

$$P_m = \frac{1}{em!}$$

In terms of probabilities over H_N, we obtain from this, as desired:

$$\begin{aligned}\lim_{N\to\infty} D(k) &= \lim_{N\to\infty}\sum_{p=0}^{\infty}(1/2)^{k+2p}\binom{k+2p}{k+p}P_N(\uparrow g+\downarrow g=k+2p)\\ &= \sum_{p=0}^{\infty}(1/2)^{k+2p}\binom{k+2p}{k+p}\frac{1}{e(k+2p)!}\\ &= \frac{1}{e}\sum_{p=0}^{\infty}\frac{(1/2)^{k+2p}}{(k+p)!p!}\end{aligned}$$

As for the general case $0<t\leq 1$, here the result 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 9.20. *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 following function,

$$f_k(t) = \sum_{p=0}^{\infty}\frac{t^{|k|+2p}}{(|k|+p)!p!}$$

Bessel function of the first kind.

Let us study now these Bessel laws. We first have the following result:

THEOREM 9.21. *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 9.20, 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 all this, we will need a number of probabilistic preliminaries. We recall that, conceptually speaking, the Poisson laws are the laws appearing via the Poisson Limit Theorem (PLT). In order to generalize this construction, as to cover for instance for Bessel laws that we found in connection with the hyperoctahedral group H_N, we have the following notion, extending the Poisson limit theory:

DEFINITION 9.22. *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 other words, what we are doing here is to generalize the construction in the Poisson Limit Theorem, by allowing the only parameter there, which was the positive real number $t > 0$, to be replaced by a certain probability measure ν, of arbitrary mass $c > 0$.

In what follows we will be interested in the case where ν is discrete, as is for instance the case for the measure $\nu = t\delta_1$ with $t > 0$, which produces via the above procedure the Poisson laws. To be more precise, we will be mainly interested in the case where ν is a multiple of the uniform measure on the s-th roots of unity. More on this later.

The following result allows us to detect compound Poisson laws:

PROPOSITION 9.23. *For a discrete measure, $\nu = \sum_{i=1}^s c_i\delta_{z_i}$ with $c_i > 0$ and $z_i \in \mathbb{R}$, we have the formula*

$$F_{p_\nu}(y) = \exp\left(\sum_{i=1}^s c_i(e^{iyz_i} - 1) \right)$$

where F denotes as usual the Fourier transform.

PROOF. Let μ_n be the measure appearing in Definition 9.22, namely:

$$\mu_n = \left(1 - \frac{c}{n}\right) \delta_0 + \frac{1}{n}\nu$$

We have the following computation, in the context of Definition 9.22:

$$F_{\mu_n}(y) = \left(1 - \frac{c}{n}\right) + \frac{1}{n}\sum_{i=1}^s c_i e^{iyz_i}$$

$$\implies F_{\mu_n^{*n}}(y) = \left(\left(1 - \frac{c}{n}\right) + \frac{1}{n}\sum_{i=1}^s c_i e^{iyz_i} \right)^n$$

$$\implies F_{p_\nu}(y) = \exp\left(\sum_{i=1}^s c_i(e^{iyz_i} - 1) \right)$$

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

We have as well the following result, providing an alternative to Definition 9.22, and which will be our formulation of the Compound Poisson Limit Theorem (CPLT):

THEOREM 9.24. *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 the formula

$$p_\nu = \text{law}\left(\sum_{i=1}^{s} z_i \alpha_i\right)$$

where the variables α_i are Poisson (c_i), independent.

PROOF. Let α be the sum of Poisson variables in the statement:

$$\alpha = \sum_{i=1}^{s} z_i \alpha_i$$

By using some well-known Fourier transform formulae, we have:

$$\begin{aligned} F_{\alpha_i}(y) = \exp(c_i(e^{iy} - 1) \quad &\implies \quad F_{z_i\alpha_i}(y) = \exp(c_i(e^{iyz_i} - 1)) \\ &\implies \quad F_\alpha(y) = \exp\left(\sum_{i=1}^{s} c_i(e^{iyz_i} - 1)\right) \end{aligned}$$

Thus we have the same formula as in Proposition 9.23, as desired. □

Getting back now to the Bessel laws, we have the following result:

THEOREM 9.25. *The Bessel laws b_t are compound Poisson laws, given by*

$$b_t = p_{t\varepsilon}$$

where $\varepsilon = \frac{1}{2}(\delta_{-1} + \delta_1)$ is the uniform measure on $\mathbb{Z}_2$.

PROOF. This follows indeed by comparing the formula of the Fourier transform of b_t, from the proof of Theorem 9.21, with the formula in Proposition 9.23. □

Getting now to the examples, let us start with the following definition:

DEFINITION 9.26. *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.

Of particular interest are the cases $s = 1, 2, \infty$, where we obtain the Poisson laws p_t, and then certain measures b_t, B_t, called real and purely complex Bessel laws:

$$b_t^1 = p_t \quad , \quad b_t^2 = b_t \quad , \quad b_t^\infty = B_t$$

As a basic result on the Bessel laws, generalizing those about p_t, we have:

THEOREM 9.27. *The Fourier transform of b_t^s is given by*

$$\log F_t^s(z) = t\left(\exp_s z - 1\right)$$

where $\exp_s z$ is the level s exponential function, given by the formula

$$\exp_s z = \sum_{k=0}^{\infty} \frac{z^{sk}}{(sk)!}$$

so in particular the measures b_t^s have the property $b_t^s * b_{t'}^s = b_{t+t'}^s$.

PROOF. We know from Theorem 9.24 that b_t^s appears as follows, with $a_1, \ldots, a_s$ being independent, each of them following the Poisson law of parameter t/s, and $w = e^{2\pi i/s}$:

$$b_t^s = law\left(\sum_{k=1}^{s} w^k a_k\right)$$

We have the following computation, for the corresponding Fourier transform:

$$\begin{aligned}
\log F(z) &= \sum_{k=1}^{s} \log F_{a_k}(w^k z) \\
&= \sum_{k=1}^{s} \frac{t}{s}\left(\exp(w^k z) - 1\right) \\
&= t\left(\left(\frac{1}{s}\sum_{k=1}^{s} \exp(w^k z)\right) - 1\right) \\
&= t\left(\exp_s z - 1\right)
\end{aligned}$$

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

Let us study now the density of b_t^s. We have here the following result:

THEOREM 9.28. *We have the formula*

$$b_t^s = e^{-t} \sum_{p_1=0}^{\infty} \cdots \sum_{p_s=0}^{\infty} \frac{1}{p_1! \ldots p_s!} \left(\frac{t}{s}\right)^{p_1+\ldots+p_s} \delta\left(\sum_{k=1}^{s} w^k p_k\right)$$

where $w = e^{2\pi i/s}$, and the δ symbol is a Dirac mass.

PROOF. The Fourier transform of the measure on the right is given by:

$$\begin{aligned}
F(z) &= e^{-t} \sum_{p_1=0}^{\infty} \cdots \sum_{p_s=0}^{\infty} \frac{1}{p_1! \ldots p_s!} \left(\frac{t}{s}\right)^{p_1+\ldots+p_s} \exp\left(\sum_{k=1}^{s} w^k p_k z\right) \\
&= e^{-t} \sum_{r=0}^{\infty} \left(\frac{t}{s}\right)^{r} \sum_{\Sigma p_i = r} \frac{\exp\left(\sum_{k=1}^{s} w^k p_k z\right)}{p_1! \ldots p_s!}
\end{aligned}$$

We multiply now by e^t, and we compute the derivative with respect to t:

$$\begin{aligned}(e^tF(z))' &= \sum_{r=1}^{\infty}\frac{r}{s}\left(\frac{t}{s}\right)^{r-1}\sum_{\Sigma p_i=r}\frac{\exp\left(\sum_{k=1}^s w^kp_kz\right)}{p_1!\ldots p_s!}\\ &= \frac{1}{s}\sum_{r=1}^{\infty}\left(\frac{t}{s}\right)^{r-1}\sum_{\Sigma p_i=r}\sum_{l=1}^{s}\frac{\exp\left(\sum_{k=1}^s w^kp_kz\right)}{p_1!\ldots p_{l-1}!(p_l-1)!p_{l+1}!\ldots p_s!}\end{aligned}$$

By using the variable $u=r-1$, we obtain from this the following formula:

$$\begin{aligned}(e^tF(z))' &= \frac{1}{s}\sum_{u=0}^{\infty}\left(\frac{t}{s}\right)^{u}\sum_{\Sigma q_i=u}\sum_{l=1}^{s}\frac{\exp\left(w^lz+\sum_{k=1}^s w^kq_kz\right)}{q_1!\ldots q_s!}\\ &= \left(\frac{1}{s}\sum_{l=1}^{s}\exp(w^lz)\right)\left(\sum_{u=0}^{\infty}\left(\frac{t}{s}\right)^{u}\sum_{\Sigma q_i=u}\frac{\exp\left(\sum_{k=1}^s w^kq_kz\right)}{q_1!\ldots q_s!}\right)\\ &= (\exp_s z)(e^tF(z))\end{aligned}$$

But this gives $\log F=t(\exp_s z-1)$, as in Theorem 9.27, as desired. □

Getting back now to group theory, we have here the following result:

THEOREM 9.29. *For the complex reflection group H_N^s we have, with $N\to\infty$:*

$$\chi_t\sim b_t^s$$

Moreover, the asymptotic moments of this variable are the numbers

$$M_k(b_t^s)=\sum_{\pi\in P^s(k)}t^{|\pi|}$$

where $P^s(k)$ are the partitions of $\{1,\ldots,k\}$ satisfying $\#\circ=\#\bullet(s)$, in each block.

PROOF. This is something quite technical, the idea being as follows:

(1) At $s=1$ the reflection group is $H_N^1=S_N$, the Bessel law is the Poisson law, $b_t^1=p_t$, and the formula $\chi_t\sim p_t$ with $N\to\infty$ is something that we know. As for the moment formula, where $P^1=P$, this is something that we know too.

(2) At $s=2$ the reflection group is $H_N^2=H_N$, the Bessel law is $b_t^2=b_t$, and the formula $\chi_t\sim b_t$ with $N\to\infty$ is something that we know. As for the moment formula, where $P^2=P_{even}$, this is something more technical, which can be established too.

(3) At $s=\infty$ the reflection group is $H_N^\infty=K_N$, the Bessel law is $b_t^\infty=B_t$, and the formula $\chi_t\sim B_t$ with $N\to\infty$ is something that can be proved as for S_N,H_N. As for the moment formula, where $P^\infty=\mathcal{P}_{even}$, this can be established too.

(4) In the general case, $s \in \mathbb{N} \cup \{\infty\}$, the formula $\chi_t \sim b_t^s$ with $N \to \infty$ can be established like for S_N, H_N, and the moment formula is something more technical. For details on all this, and for the whole story, you can have a look at my book [7]. □

9d. Further results

We have the following formula, in the general easy group setting:

PROPOSITION 9.30. *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:

$$\begin{aligned}
\int_G (g_{11} + \ldots + g_{ss})^k &= \sum_{i_1=1}^{s} \ldots \sum_{i_k=1}^{s} \int_G g_{i_1 i_1} \ldots g_{i_k i_k} \\
&= \sum_{\pi,\sigma \in D(k)} W_{kN}(\pi, \sigma) \sum_{i_1=1}^{s} \ldots \sum_{i_k=1}^{s} \delta_\pi(i) \delta_\sigma(i) \\
&= \sum_{\pi,\sigma \in D(k)} W_{kN}(\pi, \sigma) G_{ks}(\sigma, \pi) \\
&= Tr(W_{kN} G_{ks})
\end{aligned}$$

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

In order to further process now the above formula, and reach to concrete results, we can impose the uniformity condition. To be more precise, we obtain in this way:

THEOREM 9.31. *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 Proposition 9.30. By setting $s = [tN]$, with $t > 0$ being a given parameter, 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 recover our character results, as follows:

THEOREM 9.32. *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 that we found in Theorem 9.31, namely:

$$\lim_{N\to\infty}\int_{G_N}\chi_t^k=\sum_{\pi\in D(k)}t^{|\pi|}$$

By doing now some combinatorics, for instance in relation with the cumulants, this gives the results. We refer here to [7] and various related papers. □

9e. Exercises

Exercises:

EXERCISE 9.33.

EXERCISE 9.34.

EXERCISE 9.35.

EXERCISE 9.36.

EXERCISE 9.37.

EXERCISE 9.38.

EXERCISE 9.39.

EXERCISE 9.40.

Bonus exercise.

CHAPTER 10

Gram determinants

10a. Gram determinants

Let us discuss now a key algebraic problem, that we already met in chapter 9, namely the linear independence of the vectors ξ_π. We first have:

DEFINITION 10.1. *Let $P(k)$ be the set of partitions of $\{1,\ldots,k\}$, and $\pi,\sigma\in P(k)$.*

(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.*

Also, we denote by $|.|$ the number of blocks of the partitions $\pi\in P(k)$.

As an illustration here, at $k=2$ we have $P(2)=\{||,\sqcap\}$, and we have:

$$||\leq\sqcap$$

Also, at $k=3$ we have $P(3)=\{|||,\sqcap|,|\sqcap,\sqcap\!\sqcap\}$, and the order relation is as follows:

$$|||\ \leq\ \sqcap|\ ,\ \sqcap\!\!|\ ,\ |\sqcap\ \leq\ \sqcap\!\sqcap$$

In relation with our linear independence questions, the idea will be that of using:

PROPOSITION 10.2. *The Gram matrix of the vectors ξ_π is given by the formula*

$$<\xi_\pi,\xi_\sigma>=N^{|\pi\vee\sigma|}$$

where $\vee$ is the superposition operation, and $|.|$ 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 $G_k(\pi,\sigma)=N^{|\pi\vee\sigma|}$, and more specifically to compute its determinant, we will use several standard facts about partitions. We have:

DEFINITION 10.3. *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, for $P(2)=\{||,\sqcap\}$, we have by definition:

$$\mu(||,||)=\mu(\sqcap,\sqcap)=1$$

Also, $||<\sqcap$, with no intermediate partition in between, so we obtain:

$$\mu(||,\sqcap)=-\mu(||,||)=-1$$

Finally, we have $\sqcap\not\leq||$, and so we have as well the following formula:

$$\mu(\sqcap,||)=0$$

Back to the general case now, the main interest in the Möbius function comes from the Möbius inversion formula, which states that the following happens:

$$f(\sigma)=\sum_{\pi\leq\sigma}g(\pi)\quad\implies\quad g(\sigma)=\sum_{\pi\leq\sigma}\mu(\pi,\sigma)f(\pi)$$

In linear algebra terms, the statement and proof of this formula are as follows:

THEOREM 10.4. *The inverse of the adjacency matrix of $P(k)$, given by*

$$A_k(\pi,\sigma)=\begin{cases}1 & \text{if } \pi\leq\sigma\\ 0 & \text{if } \pi\not\leq\sigma\end{cases}$$

is the Möbius matrix of P, given by $M_k(\pi,\sigma)=\mu(\pi,\sigma)$.

PROOF. This is well-known, coming for instance from the fact that A_k is upper triangular. Indeed, when inverting, we are led into the recurrence from Definition 10.3. □

10b. Symmetric groups

Now back to our Gram matrix considerations, we have the following key result:

PROPOSITION 10.5. *The Gram matrix of the vectors ξ_π with $\pi\in P(k)$,*

$$G_{\pi\sigma}=N^{|\pi\vee\sigma|}$$

decomposes as a product of upper/lower triangular matrices, $G_k=A_kL_k$, where

$$L_k(\pi,\sigma)=\begin{cases}N(N-1)\ldots(N-|\pi|+1) & \text{if } \sigma\leq\pi\\ 0 & \text{otherwise}\end{cases}$$

and where A_k is the adjacency matrix of $P(k)$.

PROOF. We have the following computation, based on Proposition 10.2:

$$\begin{aligned}
G_k(\pi,\sigma) &= N^{|\pi\vee\sigma|}\\
&= \#\left\{i_1,\ldots,i_k\in\{1,\ldots,N\}\Big|\ker i\geq\pi\vee\sigma\right\}\\
&= \sum_{\tau\geq\pi\vee\sigma}\#\left\{i_1,\ldots,i_k\in\{1,\ldots,N\}\Big|\ker i=\tau\right\}\\
&= \sum_{\tau\geq\pi\vee\sigma}N(N-1)\ldots(N-|\tau|+1)
\end{aligned}$$

According now to the definition of A_k, L_k, this formula reads:

$$\begin{aligned}
G_k(\pi,\sigma) &= \sum_{\tau\geq\pi}L_k(\tau,\sigma)\\
&= \sum_{\tau}A_k(\pi,\tau)L_k(\tau,\sigma)\\
&= (A_kL_k)(\pi,\sigma)
\end{aligned}$$

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

As an illustration for the above result, at $k=2$ we have $P(2)=\{||,\sqcap\}$, and the above decomposition $G_2=A_2L_2$ appears as follows:

$$\begin{pmatrix}N^2 & N\\ N & N\end{pmatrix}=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix}N^2-N & 0\\ N & N\end{pmatrix}$$

We are led in this way to the following formula, due to Lindstöm [69]:

THEOREM 10.6. *The determinant of the Gram matrix G_k is given by*

$$\det(G_k)=\prod_{\pi\in P(k)}\frac{N!}{(N-|\pi|)!}$$

with the convention that in the case $N<k$ we obtain 0.

PROOF. If we order $P(k)$ as usual, with respect to the number of blocks, and then lexicographically, A_k is upper triangular, and L_k is lower triangular. Thus, we have:

$$\begin{aligned}
\det(G_k) &= \det(A_k)\det(L_k)\\
&= \det(L_k)\\
&= \prod_{\pi}L_k(\pi,\pi)\\
&= \prod_{\pi}N(N-1)\ldots(N-|\pi|+1)
\end{aligned}$$

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

10c. Reflection groups

We discuss now the systematic computation of the Gram determinants. Let us begin with some simple observations, coming from definitions:

PROPOSITION 10.7. *Let $D_k(N) = \det(G_{kN})$, viewed as element of $\mathbb{Z}[N]$.*

(1) *D_k is monic, of degree $s_k = \sum_{\pi \in D(k)} |\pi|$.*
(2) *We have $n^{b_k} | D_k$, where $b_k = |D(k)|$.*

PROOF. Here (1) 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 $f : D(k) \to D(k)$ 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. As for (2), this is clear from the definition of D_k, and from $|\pi \vee \sigma| \geq 1$. □

We can reformulate Proposition 10.7, in the following way:

PROPOSITION 10.8. *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 a reformulation of Proposition 10.7, 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, as follows:

PROPOSITION 10.9. *We have the formula*

$$T_k(t) = \sum_{r=1}^{k} S_{kr} t^r$$

where $S_{kr} = \#\{\pi \in D(k) : |\pi| = r\}$ are the Stirling numbers.

PROOF. This is indeed clear from definitions. □

Another interpretation of the trace, analytic this time, is as follows:

PROPOSITION 10.10. *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 group.

PROOF. As explained in chapter 9, this follows from the Weingarten formula. □

Getting now to concrete computations, for the reflection groups, we have here:

THEOREM 10.11. *For S_N, H_N we have*

$$\det(G_{kN}) = \prod_{\pi\in D(k)} \frac{N!}{(N-|\pi|)!}$$

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 in [69] together with the explicit knowledge of the Möbius function on $D(k)$ as in [55]. 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:

$$G'_{kN}(\pi,\sigma) = \begin{cases} N(N-1)\ldots(N-|\sigma|+1) & \text{if } \pi\leq\sigma \\ 0 & \text{otherwise} \end{cases}$$

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 Gram determinant for the groups S_N, H_N can be computed from the trace. Indeed, the Gram matrix trace gives the Stirling numbers, which in turn give the Gram matrix determinant.

However, the connecting formula is quite complicated, so let us just record here:

THEOREM 10.12. *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 10.11 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. □

Observe that the above discussion raises the general question on whether the Gram matrix determinant can be computed or not from the Gram matrix trace.

10d. Further results

The above computations can be thought of as corresponding to the groups S_N, H_N, but we can do such things for any easy group. As a first illustration, let us discuss the case of the orthogonal group O_N. 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. We have then the following result:

THEOREM 10.13. *The determinant of the Gram matrix of O_N is given by*

$$\det(G_{kN}) = \prod_{|\lambda|=k/2} f_N(\lambda)^{f^{2\lambda}}$$

where the quantities on the right are $f_N(\lambda) = \prod_{(i,j)\in\lambda}(N + 2j - i - 1)$.

PROOF. For the group O_N the Gram matrix is diagonalizable, as follows:

$$G_{kN} = \sum_{|\lambda|=k/2} f_N(\lambda) P_{2\lambda}$$

Here $1 = \sum P_{2\lambda}$ 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 formula in the statement. □

In order to deal now with O_N^+, S_N^+, we will need the following well-known fact:

PROPOSITION 10.14. *We have a bijection $NC(k) \simeq NC_2(2k)$, 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 above two operations are indeed inverse to each other is clear, by drawing pictures, and computing the corresponding compositions. □

At the level of the associated Gram matrices, the result is as follows:

PROPOSITION 10.15. *The Gram matrices of $NC_2(2k) \simeq NC(k)$ are related by*

$$G_{2k,n}(\pi, \sigma) = n^k(\Delta_{kn}^{-1} G_{k,n^2} \Delta_{kn}^{-1})(\pi', \sigma')$$

where $\pi \to \pi'$ is the shrinking operation, and Δ_{kn} is the diagonal of G_{kn}.

PROOF. In the context of the bijection from Proposition 10.14, 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 are led to the formula in the statement. □

Now back to O_N^+, S_N^+, let us begin with some examples. We first have:

PROPOSITION 10.16. *The first Gram matrices and determinants for O_N^+ are*

$$\det\begin{pmatrix} N^2 & N \\ N & N^2 \end{pmatrix} = N^2(N^2-1)$$

$$\det\begin{pmatrix} N^3 & N^2 & N^2 & N^2 & N \\ N^2 & N^3 & N & N & N^2 \\ N^2 & N & N^3 & N & N^2 \\ N^2 & N & N & N^3 & N^2 \\ N & N^2 & N^2 & N^2 & N^3 \end{pmatrix} = N^5(N^2-1)^4(N^2-2)$$

with the matrices being written by using the lexicographic order on $NC_2(2k)$.

PROOF. The formula at $k=2$, where $NC_2(4) = \{\sqcap\sqcap, \bigcap\!\!\bigcap\}$, is clear from definitions. At $k=3$ however, things are tricky. The partitions here are as follows:

$$NC(3) = \{|||, \sqcap|, |\sqcap, \sqcap\sqcap\}$$

The Gram matrix and its determinant are, according to Theorem 10.6:

$$\det\begin{pmatrix} N^3 & N^2 & N^2 & N^2 & N \\ N^2 & N^2 & N & N & N \\ N^2 & N & N^2 & N & N \\ N^2 & N & N & N^2 & N \\ N & N & N & N & N \end{pmatrix} = N^5(N-1)^4(N-2)$$

By using now Proposition 10.15, this gives the formula in the statement. □

In general, such tricks won't work, because $NC(k)$ is strictly smaller than $P(k)$ at $k \geq 4$. However, following Di Francesco [19], we have the following result:

THEOREM 10.17. *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 P_r are the Chebycheff polynomials, given by

$$P_0 = 1 \quad , \quad P_1 = X \quad , \quad P_{r+1} = XP_r - P_{r-1}$$

and $d_{kr} = f_{kr} - f_{k,r+1}$, with f_{kr} being the following numbers, depending on $k, r \in \mathbb{Z}$,

$$f_{kr} = \binom{2k}{k-r} - \binom{2k}{k-r-1}$$

with the convention $f_{kr} = 0$ for $k \notin \mathbb{Z}$.

PROOF. This is something quite technical, obtained by using a decomposition as follows of the Gram matrix G_{kN}, with the matrix T_{kN} being lower triangular:

$$G_{kN} = T_{kN}T_{kN}^t$$

Thus, a bit as in the proof of the Lindstöm formula, we obtain the result, but the problem lies however in the construction of T_{kN}, which is non-trivial. See [19]. □

Moving ahead now, regarding S_N^+, also following Di Francesco [19], we have:

THEOREM 10.18. *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 P_r are the Chebycheff polynomials, given by

$$P_0 = 1 \quad , \quad P_1 = X \quad , \quad P_{r+1} = XP_r - P_{r-1}$$

and $d_{kr} = f_{kr} - f_{k,r+1}$, with f_{kr} being the following numbers, depending on $k, r \in \mathbb{Z}$,

$$f_{kr} = \binom{2k}{k-r} - \binom{2k}{k-r-1}$$

with the convention $f_{kr} = 0$ for $k \notin \mathbb{Z}$, and where $a_k = \sum_{\pi\in\mathcal{P}(k)}(2|\pi| - k)$.

PROOF. This follows indeed from Theorem 10.17, by using Proposition 10.15. □

10e. Exercises

Exercises:

EXERCISE 10.19.

EXERCISE 10.20.

EXERCISE 10.21.

EXERCISE 10.22.

EXERCISE 10.23.

EXERCISE 10.24.

EXERCISE 10.25.

EXERCISE 10.26.

Bonus exercise.

CHAPTER 11

De Finetti theorems

11a. Invariant sequences

Invariant sequences.

11b. De Finetti theorems

De Finetti theorems.

11c. Weak versions

Weak versions.

11d. Reflection groups

Reflection groups.

11e. Exercises

Exercises:

Exercise 11.1.

Exercise 11.2.

Exercise 11.3.

Exercise 11.4.

Exercise 11.5.

Exercise 11.6.

Exercise 11.7.

Exercise 11.8.

Bonus exercise.

CHAPTER 12

Random walks

12a. Random walks

Random walks.

12b. Basic results

Basic results.

12c. Product operations

Product operations.

12d. Further variables

Further variables.

12e. Exercises

Exercises:

Exercise 12.1.

Exercise 12.2.

Exercise 12.3.

Exercise 12.4.

Exercise 12.5.

Exercise 12.6.

Exercise 12.7.

Exercise 12.8.

Bonus exercise.

Part IV

Generalizations

Never mind
I'll find someone like you
I wish nothing but the best
For you too

CHAPTER 13

Discrete groups

13a. Discrete groups

Discrete groups.

13b. Random walks

Random walks.

13c. Group algebras

In order to talk about group algebras, at a more advanced level, we first need to know more about operator algebras. The result that we will need is as follows:

PROPOSITION 13.1. *For a subalgebra $A \subset B(H)$, the following are equivalent:*

(1) *A is closed under the weak operator topology, making each of the linear maps $T \to < Tx, y >$ continuous.*
(2) *A is closed under the strong operator topology, making each of the linear maps $T \to Tx$ continuous.*

In the case where these conditions are satisfied, A is closed under the norm topology.

PROOF. There are several statements here, the proof being as follows:

(1) It is clear that the norm topology is stronger than the strong operator topology, which is in turn stronger than the weak operator topology. At the level of the subsets $S \subset B(H)$ which are closed things get reversed, in the sense that weakly closed implies strongly closed, which in turn implies norm closed. Thus, we are left with proving that for any algebra $A \subset B(H)$, strongly closed implies weakly closed.

(2) Consider the Hilbert space obtained by summing n times H with itself:

$$K = H \oplus \ldots \oplus H$$

The operators over K can be regarded as being square matrices with entries in $B(H)$, and in particular, we have a representation $\pi : B(H) \to B(K)$, as follows:

$$\pi(T) = \begin{pmatrix} T & & \\ & \ddots & \\ & & T \end{pmatrix}$$

Assume now that we are given an operator $T \in \bar{A}$, with the bar denoting the weak closure. We have then, by using the Hahn-Banach theorem, for any $x \in K$:

$$\begin{aligned} T \in \bar{A} &\implies \pi(T) \in \overline{\pi(A)} \\ &\implies \pi(T)x \in \overline{\pi(A)x} \\ &\implies \pi(T)x \in \overline{\pi(A)x}^{||.||} \end{aligned}$$

Now observe that the last formula tells us that for any $x = (x_1, \ldots, x_n)$, and any $\varepsilon > 0$, we can find $S \in A$ such that the following holds, for any i:

$$||Sx_i - Tx_i|| < \varepsilon$$

Thus T belongs to the strong operator closure of A, as desired. □

Observe that in the above the terminology is a bit confusing, because the norm topology is stronger than the strong operator topology. As a solution, we agree to call the norm topology "strong", and the weak and strong operator topologies "weak", whenever these two topologies coincide. With this convention made, the algebras $A \subset B(H)$ in Proposition 13.1 are those which are weakly closed. Thus, we can now formulate:

DEFINITION 13.2. *A von Neumann algebra is an operator algebra*

$$A \subset B(H)$$

which is closed under the weak topology.

These algebras will be our main objects of study, in what follows. As basic examples, we have the algebra $B(H)$ itself, then the singly generated algebras, $A =< T >$ with $T \in B(H)$, and then the multiply generated algebras, $A =< T_i >$ with $T_i \in B(H)$. But for the moment, let us keep things simple, and build directly on Definition 13.2, by using basic functional analysis methods. We will need the following key result:

THEOREM 13.3. *For an operator algebra $A \subset B(H)$, we have*

$$A'' = \bar{A}$$

with A'' being the bicommutant inside $B(H)$, and $\bar{A}$ being the weak closure.

PROOF. We can prove this by double inclusion, as follows:

"$\supset$" Since any operator commutes with the operators that it commutes with, we have a trivial inclusion $S \subset S''$, valid for any set $S \subset B(H)$. In particular, we have:

$$A \subset A''$$

Our claim now is that the algebra A'' is closed, with respect to the strong operator topology. Indeed, assuming that we have $T_i \to T$ in this topology, we have:

$$\begin{aligned} T_i \in A'' &\implies ST_i = T_iS,\ \forall S \in A' \\ &\implies ST = TS,\ \forall S \in A' \\ &\implies T \in A \end{aligned}$$

Thus our claim is proved, and together with Proposition 13.1, which allows us to pass from the strong to the weak operator topology, this gives $\bar{A} \subset A''$, as desired.

"$\subset$" Here we must prove that we have the following implication, valid for any $T \in B(H)$, with the bar denoting as usual the weak operator closure:

$$T \in A'' \implies T \in \bar{A}$$

For this purpose, we use the same amplification trick as in the proof of Proposition 13.1. Consider the Hilbert space obtained by summing n times H with itself:

$$K = H \oplus \ldots \oplus H$$

The operators over K can be regarded as being square matrices with entries in $B(H)$, and in particular, we have a representation $\pi : B(H) \to B(K)$, as follows:

$$\pi(T) = \begin{pmatrix} T & & \\ & \ddots & \\ & & T \end{pmatrix}$$

The idea will be that of doing the computations in this representation. First, in this representation, the image of our algebra $A \subset B(H)$ is given by:

$$\pi(A) = \left\{ \begin{pmatrix} T & & \\ & \ddots & \\ & & T \end{pmatrix} \middle| T \in A \right\}$$

We can compute the commutant of this image, exactly as in the usual scalar matrix case, and we obtain the following formula:

$$\pi(A)' = \left\{ \begin{pmatrix} S_{11} & \ldots & S_{1n} \\ \vdots & & \vdots \\ S_{n1} & \ldots & S_{nn} \end{pmatrix} \middle| S_{ij} \in A' \right\}$$

We conclude from this that, given an operator $T \in A''$ as above, we have:

$$\begin{pmatrix} T & & \\ & \ddots & \\ & & T \end{pmatrix} \in \pi(A)''$$

In other words, the conclusion of all this is that we have:

$$T \in A'' \implies \pi(T) \in \pi(A)''$$

Now given a vector $x \in K$, consider the orthogonal projection $P \in B(K)$ on the norm closure of the vector space $\pi(A)x \subset K$. Since the subspace $\pi(A)x \subset K$ is invariant under the action of $\pi(A)$, so is its norm closure inside K, and we obtain from this:

$$P \in \pi(A)'$$

By combining this with what we found above, we conclude that we have:

$$T \in A'' \implies \pi(T)P = P\pi(T)$$

Since this holds for any $x \in K$, we conclude that any operator $T \in A''$ belongs to the strong operator closure of A. By using now Proposition 13.1, which allows us to pass from the strong to the weak operator closure, we conclude that we have:

$$A'' \subset \bar{A}$$

Thus, we have the desired reverse inclusion, and this finishes the proof. □

Now by getting back to the von Neumann algebras, from Definition 13.2, we have the following result, which is a reformulation of Theorem 13.3, by using this notion:

THEOREM 13.4. *For an operator algebra $A \subset B(H)$, the following are equivalent:*

(1) *A is weakly closed, so it is a von Neumann algebra.*
(2) *A equals its algebraic bicommutant A'', taken inside $B(H)$.*

PROOF. This follows from the formula $A'' = \bar{A}$ from Theorem 13.3, along with the trivial fact that the commutants are automatically weakly closed. □

The above statement, called bicommutant theorem, and due to von Neumann, is quite interesting, philosophically speaking. Among others, it shows that the von Neumann algebras are exactly the commutants of the self-adjoint sets of operators:

PROPOSITION 13.5. *Given a subset $S \subset B(H)$ which is closed under $*$, the commutant*

$$A = S'$$

is a von Neumann algebra. Any von Neumann algebra appears in this way.

PROOF. We have two assertions here, the idea being as follows:

(1) Given $S \subset B(H)$ satisfying $S = S^*$, the commutant $A = S'$ satisfies $A = A^*$, and is also weakly closed. Thus, A is a von Neumann algebra. Note that this follows as well from the following "tricommutant formula", which follows from Theorem 13.4:

$$S''' = S'$$

(2) Given a von Neumann algebra $A \subset B(H)$, we can take $S = A'$. Then S is closed under the involution, and we have $S' = A$, as desired. □

As an interesting consequence of Theorem 13.4, we have:

PROPOSITION 13.6. *Given a von Neumann algebra $A \subset B(H)$, its center*

$$Z(A) = A \cap A'$$

regarded as an algebra $Z(A) \subset B(H)$, is a von Neumann algebra too.

PROOF. This follows from the fact that the commutants are weakly closed, that we know from the above, which shows that $A' \subset B(H)$ is a von Neumann algebra. Thus, the intersection $Z(A) = A \cap A'$ must be a von Neumann algebra too, as claimed. □

In order to develop some general theory, let us start by investigating the finite dimensional case. Here the ambient algebra is $B(H) = M_N(\mathbb{C})$, any linear subspace $A \subset B(H)$ is automatically closed, for all 3 topologies in Proposition 13.1, and we have:

THEOREM 13.7. *The $*$-algebras $A \subset M_N(\mathbb{C})$ are exactly the algebras of the form*

$$A = M_{n_1}(\mathbb{C}) \oplus \ldots \oplus M_{n_k}(\mathbb{C})$$

depending on parameters $k \in \mathbb{N}$ and $n_1, \ldots, n_k \in \mathbb{N}$ satisfying

$$n_1 + \ldots + n_k = N$$

embedded into $M_N(\mathbb{C})$ via the obvious block embedding, twisted by a unitary $U \in U_N$.

PROOF. This is something algebraic, that we know from chapter 4, and which, retrospectively thinking, is based on the "center philosophy" from Proposition 13.6. □

In relation with the bicommutant theorem, we have the following result, which fully clarifies the situation, with a very explicit proof, in finite dimensions:

PROPOSITION 13.8. *Consider a $*$-algebra $A \subset M_N(\mathbb{C})$, written as above:*

$$A = M_{n_1}(\mathbb{C}) \oplus \ldots \oplus M_{n_k}(\mathbb{C})$$

The commutant of this algebra is then, with respect with the block decomposition used,

$$A' = \mathbb{C} \oplus \ldots \oplus \mathbb{C}$$

and by taking one more time the commutant we obtain A itself, $A = A''$.

PROOF. Let us decompose indeed our algebra A as in Theorem 13.7:

$$A = M_{n_1}(\mathbb{C}) \oplus \ldots \oplus M_{n_k}(\mathbb{C})$$

The center of each matrix algebra being reduced to the scalars, the commutant of this algebra is then as follows, with each copy of $\mathbb{C}$ corresponding to a matrix block:

$$A' = \mathbb{C} \oplus \ldots \oplus \mathbb{C}$$

By taking once again the commutant we obtain A itself, and we are done. □

As another interesting application of Theorem 13.7, clarifying this time the relation with operator theory, in finite dimensions, we have the following result:

THEOREM 13.9. *Given an operator $T \in B(H)$ in finite dimensions, $H = \mathbb{C}^N$, the von Neumann algebra $A =< T >$ that it generates inside $B(H) = M_N(\mathbb{C})$ is*

$$A = M_{n_1}(\mathbb{C}) \oplus \ldots \oplus M_{n_k}(\mathbb{C})$$

with the sizes of the blocks $n_1, \ldots, n_k \in \mathbb{N}$ coming from the spectral theory of the associated matrix $M \in M_N(\mathbb{C})$. In the normal case $TT^* = T^*T$, this decomposition comes from

$$T = UDU^*$$

with $D \in M_N(\mathbb{C})$ diagonal, and with $U \in U_N$ unitary.

PROOF. This is something which is routine, by using the standard linear algebra and spectral theory for the usual matrices $M \in M_N(\mathbb{C})$. To be more precise:

(1) The fact that $A =< T >$ decomposes into a direct sum of matrix algebras is something that we already know, coming from Theorem 13.7.

(2) By using standard linear algebra, we can compute the block sizes $n_1, \ldots, n_k \in \mathbb{N}$, from the knowledge of the spectral theory of the associated matrix $M \in M_N(\mathbb{C})$.

(3) In the normal case, $TT^* = T^*T$, we can simply invoke the spectral theorem, and by suitably changing the basis, we are led to the conclusion in the statement. □

Let us get now to infinite dimensions, with Theorem 13.9 as our main source of inspiration. The same argument applies, provided that we are in the normal case, and we have the following result, summarizing our basic knowledge here:

THEOREM 13.10. *Given a bounded operator $T \in B(H)$ which is normal, $TT^* = T^*T$, the von Neumann algebra $A =< T >$ that it generates inside $B(H)$ is*

$$< T >= L^\infty(\sigma(T))$$

with $\sigma(T) \subset \mathbb{C}$ being as usual its spectrum.

PROOF. The measurable functional calculus theorem for the normal operators tells us that we have a weakly continuous morphism of $*$-algebras, as follows:

$$L^\infty(\sigma(T)) \to B(H) \quad , \quad f \to f(T)$$

Moreover, by the general properties of the measurable calculus, also established in chapter 5, this morphism is injective, and its image is the weakly closed algebra $< T >$ generated by T, T^*. Thus, we obtain the isomorphism in the statement. □

More generally now, along the same lines, we have the following result:

THEOREM 13.11. *Given operators $T_i \in B(H)$ which are normal, and which commute, the von Neumann algebra $A =< T_i >$ that these operators generates inside $B(H)$ is*

$$< T_i >= L^\infty(X)$$

with X being a certain measured space, associated to the family $\{T_i\}$.

PROOF. This is once again routine, by using the spectral theory for the families of commuting normal operators $T_i \in B(H)$. □

As a fundamental consequence now of the above results, we have:

THEOREM 13.12. *The commutative von Neumann algebras are the algebras*

$$A = L^\infty(X)$$

with X being a measured space.

PROOF. We have two assertions to be proved, the idea being as follows:

(1) In one sense, we must prove that given a measured space X, we can realize the $A = L^\infty(X)$ as a von Neumann algebra, on a certain Hilbert space H. But this is something that we know since chapter 4, the representation being as follows:

$$L^\infty(X) \subset B(L^2(X)) \quad , \quad f \to (g \to fg)$$

(2) In the other sense, given a commutative von Neumann algebra $A \subset B(H)$, we must construct a certain measured space X, and an identification $A = L^\infty(X)$. But this follows from Theorem 13.11, because we can write our algebra as follows:

$$A =< T_i >$$

To be more precise, A being commutative, any element $T \in A$ is normal, so we can pick a basis $\{T_i\} \subset A$, and then we have $A =< T_i >$ as above, with $T_i \in B(H)$ being commuting normal operators. Thus Theorem 13.11 applies, and gives the result.

(3) Alternatively, and more explicitly, we can deduce this from Theorem 13.10, applied with $T = T^*$. Indeed, by using $T = Re(T) + iIm(T)$, we conclude that any von Neumann algebra $A \subset B(H)$ is generated by its self-adjoint elements $T \in A$. Moreover, by using measurable functional calculus, we conclude that A is linearly generated by its projections. But then, assuming $A = \overline{span}\{p_i\}$, with p_i being projections, we can set:

$$T = \sum_{i=0}^{\infty} \frac{p_i}{3^i}$$

Then $T = T^*$, and by functional calculus we have $p_0 \in< T >$, then $p_1 \in< T >$, and so on. Thus $A =< T >$, and $A = L^\infty(X)$ comes now via Theorem 13.10, as claimed. □

Now forgetting about Gelfand, and taking Theorem 13.12 as such, tentative foundation for the theory that we want to develop, as a first consequence of this, we have:

THEOREM 13.13. *Given a von Neumann algebra $A \subset B(H)$, we have*

$$Z(A) = L^\infty(X)$$

with X being a certain measured space.

PROOF. We know from Proposition 13.6 that the center $Z(A) \subset B(H)$ is a von Neumann algebra. Thus Theorem 13.12 applies, and gives the result. □

It is possible to further build on this, with a powerful decomposition result as follows, over the measured space X constructed in Theorem 13.14:

$$A = \int_X A_x \, dx$$

But more on this later, after developing the appropriate tools for this program, which is something non-trivial. Among others, before getting into such things, we will have to study the von Neumann algebras A having trivial center, $Z(A) = \mathbb{C}$, called factors, which include the fibers A_x in the above decomposition result. More on this later.

13d. Amenability

Amenability.

13e. Exercises

Exercises:

EXERCISE 13.14.

EXERCISE 13.15.

EXERCISE 13.16.

EXERCISE 13.17.

EXERCISE 13.18.

EXERCISE 13.19.

EXERCISE 13.20.

EXERCISE 13.21.

Bonus exercise.

CHAPTER 14

Compact groups

14a. Compact groups

We have seen so far the foundations and basic results of classical probability. Before stepping into more complicated things, such as random matrices and free probability, we would like to clarify one important question which appeared several times, namely the computation of integrals over the compact groups of unitary matrices $G \subset U_N$, and its probabilistic consequences. The precise question that we have in mind is:

QUESTION 14.1. *Given a compact group $G \subset U_N$, how to compute the integrals*

$$I_{ij}^e = \int_G g_{i_1j_1}^{e_1} \ldots g_{i_kj_k}^{e_k} \, dg$$

depending on multi-indices i, j, and of a colored integer exponent $e = \circ \bullet \bullet \circ \ldots$? Then, how to use this formula in order to compute the laws of variables of type

$$f_P = P\Big(\{g_{ij}\}_{i,j=1,\ldots,N}\Big)$$

depending on a polynomial P? What about the $N \to \infty$ asymptotics of such laws?

All this is quite subtle, and as a basic illustration for this, we have a fundamental result from chapter 3, stating that for $G = S_N$ the law of the variable $\chi = \sum_i g_{ii}$ can be explicitly computed, and becomes Poisson (1) with $N \to \infty$. This is something truly remarkable, and it is this kind of result that we would like to systematically have.

We will discuss this in this whole chapter, and later on too. This might seem of course quite long, but believe me, it is worth the effort, because it is quite hard to do any type of advanced probability theory without knowing the answer to Question 14.1. But probably enough advertisement, let us get to work. Following Weyl, we first have:

DEFINITION 14.2. *A unitary representation of a compact group G is a continuous group morphism into a unitary group*

$$v : G \to U_N \quad , \quad g \to v_g$$

which can be faithful or not. The character of such a representation is the function

$$\chi : G \to \mathbb{C} \quad , \quad g \to Tr(v_g)$$

where Tr is the usual, unnormalized trace of the $N \times N$ matrices.

At the level of examples, most of the compact groups that we met so far, finite or continuous, naturally appear as closed subgroups $G \subset U_N$. In this case, the embedding $G \subset U_N$ is of course a representation, called fundamental representation. In general now, let us first discuss the various operations on the representations. We have here:

PROPOSITION 14.3. *The representations of a compact group G are subject to:*

(1) *Making sums. Given representations v, w, of dimensions N, M, their sum is the $N + M$-dimensional representation $v + w = diag(v, w)$.*
(2) *Making products. Given representations v, w, of dimensions N, M, their product is the NM-dimensional representation $(v \otimes w)_{ia,jb} = v_{ij}w_{ab}$.*
(3) *Taking conjugates. Given a N-dimensional representation v, its conjugate is the N-dimensional representation $(\bar{v})_{ij} = \bar{v}_{ij}$.*
(4) *Spinning by unitaries. Given a N-dimensional representation v, and a unitary $U \in U_N$, we can spin v by this unitary, $v \to UvU^*$.*

PROOF. The fact that the operations in the statement are indeed well-defined, among morphisms from G to unitary groups, is indeed clear from definitions. □

In relation now with characters, we have the following result:

PROPOSITION 14.4. *We have the following formulae, regarding characters*

$$\chi_{v+w} = \chi_v + \chi_w \quad , \quad \chi_{v\otimes w} = \chi_v\chi_w \quad , \quad \chi_{\bar{v}} = \bar{\chi}_v \quad , \quad \chi_{UvU^*} = \chi_v$$

in relation with the basic operations for the representations.

PROOF. All these assertions are elementary, by using the following well-known trace formulae, valid for any square matrices V, W, and any unitary U:

$$Tr(diag(V, W)) = Tr(V) + Tr(W) \quad , \quad Tr(V \otimes W) = Tr(V)Tr(W)$$

$$Tr(\bar{V}) = \overline{Tr(V)} \quad , \quad Tr(UVU^*) = Tr(V)$$

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

Assume now that we are given a closed subgroup $G \subset U_N$. By using the above operations, we can construct a whole family of representations of G, as follows:

DEFINITION 14.5. *Given a closed subgroup $G \subset U_N$, its Peter-Weyl representations are the various tensor products between the fundamental representation and its conjugate:*

$$v : G \subset U_N \quad , \quad \bar{v} : G \subset U_N$$

We denote these tensor products $v^{\otimes k}$, with $k = \circ \bullet \bullet \circ \ldots$ being a colored integer, with the colored tensor powers being defined according to the rules

$$v^{\otimes\circ} = v \quad , \quad v^{\otimes\bullet} = \bar{v} \quad , \quad v^{\otimes kl} = v^{\otimes k} \otimes v^{\otimes l}$$

and with the convention that $v^{\otimes\emptyset}$ is the trivial representation $1 : G \to U_1$.

Here are a few examples of such representations, namely those coming from the colored integers of length 2, which will often appear in what follows:

$$v^{\otimes\circ\circ} = v \otimes v \quad , \quad v^{\otimes\circ\bullet} = v \otimes \bar{v}$$

$$v^{\otimes\bullet\circ} = \bar{v} \otimes v \quad , \quad v^{\otimes\bullet\bullet} = \bar{v} \otimes \bar{v}$$

In relation now with characters, we have the following result:

PROPOSITION 14.6. *The characters of the Peter-Weyl representations are given by*

$$\chi_{v^{\otimes k}} = (\chi_v)^k$$

with the colored powers being given by $\chi^\circ = \chi$, $\chi^\bullet = \bar{\chi}$ and multiplicativity.

PROOF. This follows indeed from the additivity, multiplicativity and conjugation formulae from Proposition 14.4, via the conventions in Definition 14.5. □

Getting back now to our motivations, we can see the interest in the above constructions. Indeed, the joint moments of the main character $\chi = \chi_v$ and its adjoint $\bar{\chi} = \chi_{\bar{v}}$ are the expectations of the characters of various Peter-Weyl representations:

$$\int_G \chi^k = \int_G \chi_{v^{\otimes k}}$$

In order to advance, we must develop some general theory. Let us start with:

DEFINITION 14.7. *Given a compact group G, and two of its representations,*

$$v : G \to U_N \quad , \quad w : G \to U_M$$

we define the space of intertwiners between these representations as being

$$Hom(v, w) = \left\{ T \in M_{M\times N}(\mathbb{C}) \middle| Tv_g = w_g T, \forall g \in G \right\}$$

and we use the following conventions:

(1) *We use the notations $Fix(v) = Hom(1, v)$, and $End(v) = Hom(v, v)$.*
(2) *We write $v \sim w$ when $Hom(v, w)$ contains an invertible element.*
(3) *We say that v is irreducible, and write $v \in Irr(G)$, when $End(v) = \mathbb{C}1$.*

The terminology here is standard, with Fix, Hom, End standing for fixed points, homomorphisms and endomorphisms. We will see later that irreducible means indecomposable, in a suitable sense. Here are now a few basic results, regarding these spaces:

PROPOSITION 14.8. *The spaces of intertwiners have the following properties:*

(1) $T \in Hom(v, w), S \in Hom(w, z) \implies ST \in Hom(v, z)$.
(2) $S \in Hom(v, w), T \in Hom(z, t) \implies S \otimes T \in Hom(v \otimes z, w \otimes t)$.
(3) $T \in Hom(v, w) \implies T^* \in Hom(w, v)$.

In abstract terms, we say that the Hom spaces form a tensor $*$-category.

PROOF. All the formulae in the statement are indeed clear from definitions, via elementary computations. As for the last assertion, this is something coming from (1,2,3). We will be back to tensor categories later on, with more details on this latter fact. □

As a main consequence of the above result, we have:

PROPOSITION 14.9. *Given a representation $v : G \to U_N$, the linear space*

$$End(v) \subset M_N(\mathbb{C})$$

is a $*$-algebra, with respect to the usual involution of the matrices.

PROOF. By definition, $End(v)$ is a linear subspace of $M_N(\mathbb{C})$. We know from Proposition 14.8 (1) that this subspace $End(v)$ is a subalgebra of $M_N(\mathbb{C})$, and then we know as well from Proposition 14.8 (3) that this subalgebra is stable under the involution $*$. Thus, what we have here is a $*$-subalgebra of $M_N(\mathbb{C})$, as claimed. □

In order to exploit the above fact, we will need a basic result from linear algebra, stating that any $*$-algebra $A \subset M_N(\mathbb{C})$ decomposes as a direct sum, as follows:

$$A \simeq M_{N_1}(\mathbb{C}) \oplus \ldots \oplus M_{N_k}(\mathbb{C})$$

Indeed, let us write the unit $1 \in A$ as $1 = p_1 + \ldots + p_k$, with $p_i \in A$ being central minimal projections. Then each of the spaces $A_i = p_i A p_i$ is a subalgebra of A, and we have a decomposition $A = A_1 \oplus \ldots \oplus A_k$. But since each central projection $p_i \in A$ was chosen minimal, we have $A_i \simeq M_{N_i}(\mathbb{C})$, with $N_i = rank(p_i)$, as desired.

We can now formulate our first Peter-Weyl type theorem, as follows:

THEOREM 14.10 (Peter-Weyl 1). *Let $v : G \to U_N$ be a representation, consider the algebra $A = End(v)$, and write its unit $1 = p_1 + \ldots + p_k$ as above. We have then*

$$v = v_1 + \ldots + v_k$$

with each v_i being an irreducible representation, obtained by restricting v to $Im(p_i)$.

PROOF. This basically follows from Proposition 14.9, as follows:

(1) We first associate to our representation $v : G \to U_N$ the corresponding action map on $\mathbb{C}^N$. If a linear subspace $W \subset \mathbb{C}^N$ is invariant, the restriction of the action map to W is an action map too, which must come from a subrepresentation $w \subset v$.

(2) Consider now a projection $p \in End(v)$. From $pv = vp$ we obtain that the linear space $W = Im(p)$ is invariant under v, and so this space must come from a subrepresentation $w \subset v$. It is routine to check that the operation $p \to w$ maps subprojections to subrepresentations, and minimal projections to irreducible representations.

(3) With these preliminaries in hand, let us decompose the algebra $End(v)$ as above, by using the decomposition $1 = p_1 + \ldots + p_k$ into central minimal projections. If we

denote by $v_i \subset v$ the subrepresentation coming from the vector space $V_i = Im(p_i)$, then we obtain in this way a decomposition $v = v_1 + \ldots + v_k$, as in the statement. □

Here is now our second Peter-Weyl theorem, complementing Theorem 14.10:

THEOREM 14.11 (Peter-Weyl 2). *Given a closed subgroup $G \subset_v U_N$, any of its irreducible smooth representations*

$$w : G \to U_M$$

appears inside a tensor product of the fundamental representation v and its adjoint $\bar{v}$.

PROOF. Given a representation $w : G \to U_M$, we define the space of coefficients $C_w \subset C(G)$ of this representation as being the following linear space:

$$C_w = span\Big[g \to w(g)_{ij}\Big]$$

With this notion in hand, the result can be deduced as follows:

(1) The construction $w \to C_w$ is functorial, in the sense that it maps subrepresentations into linear subspaces. This is indeed something which is routine to check.

(2) A closed subgroup $G \subset_v U_N$ is a Lie group, and a representation $w : G \to U_M$ is smooth when we have an inclusion $C_w \subset < C_v >$. This is indeed well-known.

(3) By definition of the Peter-Weyl representations, as arbitrary tensor products between the fundamental representation v and its conjugate $\bar{v}$, we have:

$$< C_v > = \sum_k C_{v^{\otimes k}}$$

(4) Now by putting together the above observations (2,3) we conclude that we must have an inclusion as follows, for certain exponents $k_1, \ldots, k_p$:

$$C_w \subset C_{v^{\otimes k_1} \oplus \ldots \oplus v^{\otimes k_p}}$$

(5) By using now (1), we deduce that we have an inclusion $w \subset v^{\otimes k_1} \oplus \ldots \oplus v^{\otimes k_p}$, and by applying Theorem 14.10, this leads to the conclusion in the statement. □

14b. Haar integration

In order to further advance with Peter-Weyl theory, we need to talk about integration over G. In the finite group case the situation is trivial, as follows:

PROPOSITION 14.12. *Any finite group G has a unique probability measure which is invariant under left and right translations,*

$$\mu(E) = \mu(gE) = \mu(Eg)$$

and this is the normalized counting measure on G, given by $\mu(E) = |E|/|G|$.

PROOF. This is indeed something trivial, which follows from definitions. □

In the general, continuous case, let us begin with the following key result:

PROPOSITION 14.13. *Given a unital positive linear form $\psi : C(G) \to \mathbb{C}$, the limit*

$$\int_\varphi f = \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \psi^{*k}(f)$$

exists, and for a coefficient of a representation $f = (\tau \otimes id)w$ we have

$$\int_\varphi f = \tau(P)$$

where P is the orthogonal projection onto the 1-eigenspace of $(id \otimes \psi)w$.

PROOF. By linearity it is enough to prove the first assertion for functions of the following type, where w is a Peter-Weyl representation, and τ is a linear form:

$$f = (\tau \otimes id)w$$

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 $f = (\tau \otimes id)w$:

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \psi^{*k}(f) = \tau(P)$$

In order to prove this latter formula, observe that we have:

$$\psi^{*k}(f) = (\tau \otimes \psi^{*k})w = \tau((id \otimes \psi^{*k})w)$$

Let us set $M = (id \otimes \psi)w$. In terms of this matrix, we have:

$$((id \otimes \psi^{*k})w)_{i_0 i_{k+1}} = \sum_{i_1 \ldots i_k} M_{i_0 i_1} \ldots M_{i_k i_{k+1}} = (M^k)_{i_0 i_{k+1}}$$

Thus we have the following formula, valid for any $k \in \mathbb{N}$:

$$(id \otimes \psi^{*k})w = M^k$$

It follows that our Cesàro limit is given by the following formula:

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \psi^{*k}(f) = \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \tau(M^k) = \tau\left(\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} M^k \right)$$

Now since w is unitary we have $||w|| = 1$, and so $||M|| \leq 1$. Thus the last Cesàro limit 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 the linear form $\psi \in C(G)^*$ is faithful, we have the following finer result:

PROPOSITION 14.14. *Given a faithful unital linear form $\psi \in C(G)^*$, the limit*

$$\int_\psi f = \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \psi^{*k}(f)$$

exists, and is independent of ψ, given on coefficients of representations by

$$\left(id \otimes \int_\psi\right) w = P$$

where P is the orthogonal projection onto the space $Fix(w) = \left\{\xi \in \mathbb{C}^n \middle| w\xi = \xi\right\}$.

PROOF. In view of Proposition 14.13, it remains to prove that when ψ is faithful, the 1-eigenspace of the matrix $M = (id \otimes \psi)w$ equals the space $Fix(w)$.

"$\supset$" This is clear, and for any ψ, because we have the following implication:

$$w\xi = \xi \implies M\xi = \xi$$

"$\subset$" Here we must prove that, when ψ is faithful, we have:

$$M\xi = \xi \implies w\xi = \xi$$

For this purpose, assume that we have $M\xi = \xi$, and consider the following function:

$$f = \sum_i \left(\sum_j w_{ij}\xi_j - \xi_i\right)\left(\sum_k w_{ik}\xi_k - \xi_i\right)^*$$

We must prove that we have $f = 0$. Since v is unitary, we have:

$$\begin{aligned} f &= \sum_{ijk} w_{ij}w_{ik}^*\xi_j\bar{\xi}_k - \frac{1}{N}w_{ij}\xi_j\bar{\xi}_i - \frac{1}{N}w_{ik}^*\xi_i\bar{\xi}_k + \frac{1}{N^2}\xi_i\bar{\xi}_i \\ &= \sum_j |\xi_j|^2 - \sum_{ij} w_{ij}\xi_j\bar{\xi}_i - \sum_{ik} w_{ik}^*\xi_i\bar{\xi}_k + \sum_i |\xi_i|^2 \\ &= ||\xi||^2 - < w\xi, \xi > - \overline{< w\xi, \xi >} + ||\xi||^2 \\ &= 2(||\xi||^2 - Re(< w\xi, \xi >)) \end{aligned}$$

By using now our assumption $M\xi = \xi$, we obtain from this:

$$\begin{aligned} \psi(f) &= 2\psi(||\xi||^2 - Re(< w\xi, \xi >)) \\ &= 2(||\xi||^2 - Re(< M\xi, \xi >)) \\ &= 2(||\xi||^2 - ||\xi||^2) \\ &= 0 \end{aligned}$$

Now since ψ is faithful, this gives $f = 0$, and so $w\xi = \xi$, as claimed. □

We can now formulate a main result, as follows:

THEOREM 14.15. *Any compact group G has a unique Haar integration, which can be constructed by starting with any faithful positive unital form $\psi \in C(G)^*$, and setting:*

$$\int_G = \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \psi^{*k}$$

Moreover, for any representation w we have the formula

$$\left(id \otimes \int_G \right) w = P$$

where P is the orthogonal projection onto $Fix(w) = \left\{ \xi \in \mathbb{C}^n \middle| w\xi = \xi \right\}$.

PROOF. Let us first go back to the general context of Proposition 14.13. Since convolving one more time with ψ will not change the Cesàro limit appearing there, the functional $\int_\psi \in C(G)^*$ constructed there has the following invariance property:

$$\int_\psi * \psi = \psi * \int_\psi = \int_\psi$$

In the case where ψ is assumed to be faithful, as in Proposition 14.14, our claim is that we have the following formula, valid this time for any $\varphi \in C(G)^*$:

$$\int_\psi * \varphi = \varphi * \int_\psi = \varphi(1) \int_\psi$$

Indeed, it is enough to prove this formula on a coefficient of a corepresentation:

$$f = (\tau \otimes id)w$$

In order to do so, consider the following two matrices:

$$P = \left(id \otimes \int_\psi \right) w \quad , \quad Q = (id \otimes \varphi)w$$

We have then the following formulae, which all follow from definitions:

$$\left(\int_\psi * \varphi \right) f = \tau(PQ) \quad , \quad \left(\varphi * \int_\psi \right) f = \tau(QP) \quad , \quad \varphi(1) \int_\psi f = \varphi(1)\tau(P)$$

Thus, in order to prove our claim, it is enough to establish the following formula:

$$PQ = QP = \psi(1)P$$

But this follows from the fact, from Proposition 14.14, that $P = (id \otimes \int_\psi)w$ is the orthogonal projection onto $Fix(w)$. Thus, we proved our claim. Now observe that, with $\Delta f(g \otimes h) = f(gh)$, this formula that we proved can be written as follows:

$$\varphi \left(\int_\psi \otimes id \right) \Delta = \varphi \left(id \otimes \int_\psi \right) \Delta = \varphi \int_\psi (.)1$$

This formula being true for any $\varphi \in C(G)^*$, we can simply delete φ, and we conclude that $\int_G = \int_\psi$ has the required left and right invariance property, namely:

$$\left(\int_G \otimes id\right)\Delta = \left(id \otimes \int_G\right)\Delta = \int_G (.)1$$

Finally, the uniqueness is clear as well, because if we have two invariant integrals $\int_G, \int'_G$, then their convolution equals on one hand $\int_G$, and on the other hand, $\int'_G$. □

Summarizing, we know how to integrate over G. Before getting into probabilistic applications, let us develop however more Peter-Weyl theory. We will need:

PROPOSITION 14.16. *We have a Frobenius type isomorphism*

$$Hom(v, w) \simeq Fix(v \otimes \bar{w})$$

valid for any two representations v, w.

PROOF. According to definitions, we have the following equivalences:

$$\begin{aligned} T \in Hom(v, w) &\iff Tv = wT \\ &\iff \sum_i T_{ai} v_{ij} = \sum_b w_{ab} T_{bj}, \forall a, j \end{aligned}$$

On the other hand, we have as well the following equivalences:

$$\begin{aligned} T \in Fix(v \otimes \bar{w}) &\iff (v \otimes \bar{w})T = \xi \\ &\iff \sum_{bi} v_{ji} \bar{w}_{ab} T_{bi} = T_{aj} \forall a, j \end{aligned}$$

With these formulae in hand, both inclusions follow from the unitarity of v, w. □

We can now formulate a third Peter-Weyl theorem, as follows:

THEOREM 14.17 (Peter-Weyl 3). *The dense subalgebra $\mathcal{C}(G) \subset C(G)$ generated by the coefficients of the fundamental representation decomposes as a direct sum*

$$\mathcal{C}(G) = \bigoplus_{w \in Irr(G)} M_{\dim(w)}(\mathbb{C})$$

with the summands being pairwise orthogonal with respect to the scalar product

$$< f, g >= \int_G f\bar{g}$$

where $\int_G$ is the Haar integration over G.

PROOF. By combining the previous two Peter-Weyl results, Theorems 14.10 and 14.11, we deduce that we have a linear space decomposition as follows:

$$\mathcal{C}(G) = \sum_{w \in Irr(G)} C_w = \sum_{w \in Irr(G)} M_{\dim(w)}(\mathbb{C})$$

Thus, in order to conclude, it is enough to prove that for any two irreducible representations $v, w \in Irr(G)$, the corresponding spaces of coefficients are orthogonal:

$$v \not\sim w \implies C_v \perp C_w$$

But this follows from Theorem 14.15, via Proposition 14.16. Let us set indeed:

$$P_{ia,jb} = \int_G v_{ij}\bar{w}_{ab}$$

Then P is the orthogonal projection onto the following vector space:

$$Fix(v \otimes \bar{w}) \simeq Hom(v, w) = \{0\}$$

Thus we have $P = 0$, and this gives the result. □

Finally, we have the following result, completing the Peter-Weyl theory:

THEOREM 14.18 (Peter-Weyl 4). *The characters of irreducible representations belong to the algebra*

$$\mathcal{C}(G)_{central} = \left\{ f \in \mathcal{C}(G) \middle| f(gh) = f(hg), \forall g, h \in G \right\}$$

called algebra of central functions on G, and form an orthonormal basis of it.

PROOF. Observe first that $\mathcal{C}(G)_{central}$ is indeed an algebra, which contains all the characters. Conversely, consider a function $f \in \mathcal{C}(G)$, written as follows:

$$f = \sum_{w \in Irr(G)} f_w$$

The condition $f \in \mathcal{C}(G)_{central}$ states then that for any $w \in Irr(G)$, we must have:

$$f_w \in \mathcal{C}(G)_{central}$$

But this means that f_w must be a scalar multiple of χ_w, so the characters form a basis of $\mathcal{C}(G)_{central}$, as stated. Also, the fact that we have an orthogonal basis follows from Theorem 14.17. As for the fact that the characters have norm 1, this follows from:

$$\int_G \chi_w \bar{\chi}_w = \sum_{ij} \int_G w_{ii}\bar{w}_{jj} = \sum_i \frac{1}{M} = 1$$

Here we have used the fact, coming from Theorem 14.15 and Proposition 14.16, that the integrals $\int_G w_{ij}\bar{w}_{kl}$ form the orthogonal projection onto the following vector space:

$$Fix(w \otimes \bar{w}) \simeq End(w) = \mathbb{C}1$$

Thus, the proof of our theorem is now complete. □

14c. Diagrams, easiness

In view of the above results, no matter on what we want to do with our group, we must compute the spaces $Fix(v^{\otimes k})$. It is technically convenient to slightly enlarge the class of spaces to be computed, by talking about Tannakian categories, as follows:

DEFINITION 14.19. *The Tannakian category associated to a closed subgroup $G \subset_v U_N$ is the collection $C_G = (C_G(k,l))$ of vector spaces*

$$C_G(k,l) = Hom(v^{\otimes k}, v^{\otimes l})$$

where the representations $v^{\otimes k}$ with $k = \circ \bullet \bullet \circ \ldots$ colored integer, defined by

$$v^{\otimes \emptyset} = 1 \quad , \quad v^{\otimes \circ} = v \quad , \quad v^{\otimes \bullet} = \bar{v}$$

and multiplicativity, $v^{\otimes kl} = v^{\otimes k} \otimes v^{\otimes l}$, are the Peter-Weyl representations.

Let us make a summary of what we have so far, regarding these spaces $C_G(k,l)$. In order to formulate our result, let us start with the following definition:

DEFINITION 14.20. *Let H be a finite dimensional Hilbert space. A tensor category over H is a collection $C = (C(k,l))$ of linear spaces*

$$C(k,l) \subset \mathcal{L}(H^{\otimes k}, H^{\otimes l})$$

satisfying the following conditions:

(1) *$S, T \in C$ implies $S \otimes T \in C$.*
(2) *If $S, T \in C$ are composable, then $ST \in C$.*
(3) *$T \in C$ implies $T^* \in C$.*
(4) *$C(k,k)$ contains the identity operator.*
(5) *$C(\emptyset, k)$ with $k = \circ\bullet, \bullet\circ$ contain the operator $R : 1 \to \sum_i e_i \otimes e_i$.*
(6) *$C(kl, lk)$ with $k, l = \circ, \bullet$ contain the flip operator $\Sigma : a \otimes b \to b \otimes a$.*

Here the tensor power Hilbert spaces $H^{\otimes k}$, with $k = \circ \bullet \bullet \circ \ldots$ being a colored integer, are defined by the following formulae, and multiplicativity:

$$H^{\otimes \emptyset} = \mathbb{C} \quad , \quad H^{\otimes \circ} = H \quad , \quad H^{\otimes \bullet} = \bar{H} \simeq H$$

With these conventions, we have the following result, summarizing our knowledge on the subject, coming from the results established in the above:

THEOREM 14.21. *For a closed subgroup $G \subset_v U_N$, the associated Tannakian category*

$$C_G(k,l) = Hom(v^{\otimes k}, v^{\otimes l})$$

is a tensor category over the Hilbert space $H = \mathbb{C}^N$.

PROOF. We know that the fundamental representation v acts on the Hilbert space $H = \mathbb{C}^N$, and that its conjugate $\bar{v}$ acts on the Hilbert space $\bar{H} = \mathbb{C}^N$. Now by multiplicativity we conclude that any Peter-Weyl representation $v^{\otimes k}$ acts on the Hilbert space $H^{\otimes k}$, and so that we have embeddings as in Definition 14.20, as follows:

$$C_G(k,l) \subset \mathcal{L}(H^{\otimes k}, H^{\otimes l})$$

Regarding now the fact that the axioms (1-6) in Definition 14.20 are indeed satisfied, this is something that we basically already know. To be more precise, (1-4) are clear, and (5) follows from the fact that each element $g \in G$ is a unitary, which gives:

$$R \in Hom(1, g \otimes \bar{g}) \quad , \quad R \in Hom(1, \bar{g} \otimes g)$$

As for (6), this is something trivial, coming from the fact that the matrix coefficients $g \to g_{ij}$ and their complex conjugates $g \to \bar{g}_{ij}$ commute with each other. □

Our purpose now will be that of showing that any closed subgroup $G \subset U_N$ is uniquely determined by its Tannakian category $C_G = (C_G(k,l))$. This result, known as Tannakian duality, is something quite deep, and extremely useful. Indeed, the idea is that what we would have here is a "linearization" of G, allowing us to do combinatorics, and to ultimately reach to concrete and powerful results, regarding G itself. We first have:

THEOREM 14.22. *Given a tensor category $C = (C(k,l))$ over a finite dimensional Hilbert space $H \simeq \mathbb{C}^N$, the following construction,*

$$G_C = \left\{ g \in U_N \middle| Tg^{\otimes k} = g^{\otimes l}T \ , \ \forall k,l, \forall T \in C(k,l) \right\}$$

produces a closed subgroup $G_C \subset U_N$.

PROOF. This is something elementary, with the fact that the closed subset $G_C \subset U_N$ constructed in the statement is indeed stable under the multiplication, unit and inversion operation for the unitary matrices $g \in U_N$ being clear from definitions. □

We can now formulate the Tannakian duality result, as follows:

THEOREM 14.23. *The above Tannakian constructions*

$$G \to C_G \quad , \quad C \to G_C$$

are bijective, and inverse to each other.

PROOF. This is something quite technical, obtained by doing some abstract algebra, and for details here, we refer to the Tannakian duality literature. The whole subject is actually, in modern times, for the most part of quantum algebra, and you can consult here various quantum group papers and books, for details on the above. □

In order to reach now to more concrete things, following Brauer, we have:

DEFINITION 14.24. *Let $P(k,l)$ be the set of partitions between an upper colored integer k, and a lower colored integer l. A collection of subsets*

$$D = \bigsqcup_{k,l} D(k,l)$$

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 $(\pi,\sigma) \to \left[\begin{smallmatrix}\sigma\\ \pi\end{smallmatrix}\right]$, 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 $P(\emptyset, \bullet\circ)$ both contain the semicircle $\cap$.*
(6) *The sets $P(k,\bar{k})$ with $|k| = 2$ contain the crossing partition $\diagup\!\!\diagdown$.*

There are many examples of such categories, as for instance the category of all pairings P_2, or of all matching pairings $\mathcal{P}_2$. We will be back to examples in a moment.

Let us formulate as well the following definition:

DEFINITION 14.25. *Given a partition $\pi \in P(k,l)$ and an integer $N \in \mathbb{N}$, we can construct a linear map between tensor powers of $\mathbb{C}^N$,*

$$T_\pi : (\mathbb{C}^N)^{\otimes k} \to (\mathbb{C}^N)^{\otimes l}$$

by the following formula, with $e_1, \ldots, e_N$ being the standard basis of $\mathbb{C}^N$,

$$T_\pi(e_{i_1} \otimes \ldots \otimes e_{i_k}) = \sum_{j_1 \ldots j_l} \delta_\pi \begin{pmatrix} i_1 & \ldots & i_k \\ j_1 & \ldots & j_l \end{pmatrix} e_{j_1} \otimes \ldots \otimes e_{j_l}$$

and with the coefficients on the right being Kronecker type symbols,

$$\delta_\pi \begin{pmatrix} i_1 & \ldots & i_k \\ j_1 & \ldots & j_l \end{pmatrix} \in \{0,1\}$$

whose values depend on whether the indices fit or not.

To be more precise, we put the indices of i,j on the legs of π, in the obvious way. In case all the blocks of π contain equal indices of i,j, we set $\delta_\pi\left(\begin{smallmatrix} i\\ j\end{smallmatrix}\right) = 1$. Otherwise, we set $\delta_\pi\left(\begin{smallmatrix} i\\ j\end{smallmatrix}\right) = 0$. The relation with the Tannakian categories comes from:

PROPOSITION 14.26. *The assignement $\pi \to T_\pi$ is categorical, in the sense that*

$$T_\pi \otimes T_\nu = T_{[\pi\nu]} \quad , \quad T_\pi T_\nu = N^{c(\pi,\nu)} T_{\left[\begin{smallmatrix}\nu\\ \pi\end{smallmatrix}\right]} \quad , \quad T_\pi^* = T_{\pi^*}$$

where $c(\pi,\nu)$ are certain integers, coming from the erased components in the middle.

PROOF. This is something elementary, the computations being as follows:

(1) The concatenation axiom can be checked as follows:

$$\begin{aligned}
&(T_\pi\otimes T_\nu)(e_{i_1}\otimes\ldots\otimes e_{i_p}\otimes e_{k_1}\otimes\ldots\otimes e_{k_r})\\
=\ &\sum_{j_1\ldots j_q}\sum_{l_1\ldots l_s}\delta_\pi\begin{pmatrix}i_1&\ldots&i_p\\j_1&\ldots&j_q\end{pmatrix}\delta_\nu\begin{pmatrix}k_1&\ldots&k_r\\l_1&\ldots&l_s\end{pmatrix}e_{j_1}\otimes\ldots\otimes e_{j_q}\otimes e_{l_1}\otimes\ldots\otimes e_{l_s}\\
=\ &\sum_{j_1\ldots j_q}\sum_{l_1\ldots l_s}\delta_{[\pi\nu]}\begin{pmatrix}i_1&\ldots&i_p&k_1&\ldots&k_r\\j_1&\ldots&j_q&l_1&\ldots&l_s\end{pmatrix}e_{j_1}\otimes\ldots\otimes e_{j_q}\otimes e_{l_1}\otimes\ldots\otimes e_{l_s}\\
=\ &T_{[\pi\nu]}(e_{i_1}\otimes\ldots\otimes e_{i_p}\otimes e_{k_1}\otimes\ldots\otimes e_{k_r})
\end{aligned}$$

(2) The composition axiom can be checked as follows:

$$\begin{aligned}
&T_\pi T_\nu(e_{i_1}\otimes\ldots\otimes e_{i_p})\\
=\ &\sum_{j_1\ldots j_q}\delta_\nu\begin{pmatrix}i_1&\ldots&i_p\\j_1&\ldots&j_q\end{pmatrix}\sum_{k_1\ldots k_r}\delta_\pi\begin{pmatrix}j_1&\ldots&j_q\\k_1&\ldots&k_r\end{pmatrix}e_{k_1}\otimes\ldots\otimes e_{k_r}\\
=\ &\sum_{k_1\ldots k_r}N^{c(\pi,\nu)}\delta_{[\nu\atop\pi]}\begin{pmatrix}i_1&\ldots&i_p\\k_1&\ldots&k_r\end{pmatrix}e_{k_1}\otimes\ldots\otimes e_{k_r}\\
=\ &N^{c(\pi,\nu)}T_{[\nu\atop\pi]}(e_{i_1}\otimes\ldots\otimes e_{i_p})
\end{aligned}$$

(3) Finally, the involution axiom can be checked as follows:

$$\begin{aligned}
&T_\pi^*(e_{j_1}\otimes\ldots\otimes e_{j_q})\\
=\ &\sum_{i_1\ldots i_p}<T_\pi^*(e_{j_1}\otimes\ldots\otimes e_{j_q}),e_{i_1}\otimes\ldots\otimes e_{i_p}>e_{i_1}\otimes\ldots\otimes e_{i_p}\\
=\ &\sum_{i_1\ldots i_p}\delta_\pi\begin{pmatrix}i_1&\ldots&i_p\\j_1&\ldots&j_q\end{pmatrix}e_{i_1}\otimes\ldots\otimes e_{i_p}\\
=\ &T_{\pi^*}(e_{j_1}\otimes\ldots\otimes e_{j_q})
\end{aligned}$$

Summarizing, our correspondence is indeed categorical. □

In relation now with the groups, we have the following result:

THEOREM 14.27. *Each category of partitions $D=(D(k,l))$ produces a family of compact groups $G=(G_N)$, with $G_N\subset_v U_N$, via the formula*

$$Hom(v^{\otimes k},v^{\otimes l})=span\left(T_\pi\middle|\pi\in D(k,l)\right)$$

and the Tannakian duality correspondence.

PROOF. Given an integer $N \in \mathbb{N}$, consider the correspondence $\pi \to T_\pi$ constructed in Definition 14.25, and then the collection of linear spaces in the statement, namely:

$$C(k,l) = span\left(T_\pi \middle| \pi \in D(k,l)\right)$$

According to Proposition 14.26, and to our axioms for the categories of partitions, from Definition 14.24, this collection of spaces $C = (C(k,l))$ satisfies the axioms for the Tannakian categories, from Definition 14.20. Thus the Tannakian duality result, Theorem 14.23, applies, and provides us with a closed subgroup $G_N \subset_v U_N$ such that:

$$C(k,l) = Hom(v^{\otimes k}, v^{\otimes l})$$

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

We can now formulate a key definition, as follows:

DEFINITION 14.28. *A closed subgroup $G \subset_v U_N$ is called easy when we have*

$$Hom(v^{\otimes k}, v^{\otimes l}) = span\left(T_\pi \middle| \pi \in D(k,l)\right)$$

for any colored integers k, l, for a certain category of partitions $D \subset P$.

The notion of easiness goes back to the results of Brauer regarding the orthogonal group O_N, and the unitary group U_N, which can be formulated as follows:

THEOREM 14.29. *We have the following results:*

(1) *U_N is easy, coming from the category of matching pairings $\mathcal{P}_2$.*
(2) *O_N is easy too, coming from the category of all pairings P_2.*

PROOF. This is something very standard, the idea being as follows:

(1) The group U_N being defined via the relations $v^* = v^{-1}$, $v^t = \bar{v}^{-1}$, the associated Tannakian category is $C = span(T_\pi | \pi \in D)$, with:

$$D = <\ \cap_{\circ\bullet}\ ,\ \cap_{\bullet\circ}\ > = \mathcal{P}_2$$

(2) The group $O_N \subset U_N$ being defined by imposing the relations $v_{ij} = \bar{v}_{ij}$, the associated Tannakian category is $C = span(T_\pi | \pi \in D)$, with:

$$D = <\mathcal{P}_2, \updownarrow_\bullet, \updownarrow_\circ> = P_2$$

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

Beyond this, a first natural question is that of computing the easy group associated to the category P itself, and we have here the following Brauer type theorem:

THEOREM 14.30. *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 the easy group $G \subset O_N$ coming from the category of all partitions P. Since P is generated by the one-block partition $Y \in P(2,1)$, we have:

$$C(G) = C(O_N)\Big/\Big\langle T_Y \in Hom(v^{\otimes 2}, v)\Big\rangle$$

The linear map associated to Y is given by the following formula:

$$T_Y(e_i \otimes e_j) = \delta_{ij} e_i$$

Thus, the relation defining the above group $G \subset O_N$ reformulates as follows:

$$T_Y \in Hom(v^{\otimes 2}, v) \iff v_{ij}v_{ik} = \delta_{jk}v_{ij}, \forall i, j, k$$

In other words, the elements v_{ij} must be projections, and these projections must be pairwise orthogonal on the rows of $v = (v_{ij})$. 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 claimed. □

In fact, we have the following general easiness result, regarding the series of complex reflection groups $H_N^s \subset U_N$, that we introduced in chapter 3:

THEOREM 14.31. *The group $H_N^s = \mathbb{Z}_s \wr S_N$ is easy, the corresponding category P^s consisting of the partitions satisfying $\#\circ = \#\bullet\,(s)$ in each block. In particular:*

(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 14.30. In general, the proof is similar, based on Tannakian duality. To be more precise, in what regards the main assertion, the idea here is that the one-block partition $\pi \in P(s)$, which generates the category P^s, implements the relations producing the subgroup $H_N^s \subset U_N$. As for the last assertions, these follow from the following observations:

(1) At $s = 1$ we know that we have $H_N^1 = S_N$. Regarding now the corresponding category, here the condition $\#\circ = \#\bullet\,(1)$ is automatic, and so $P^1 = P$.

(2) At $s = 2$ we know that we have $H_N^2 = H_N$. Regarding now the corresponding category, here the condition $\#\circ = \#\bullet\,(2)$ reformulates as follows:

$$\#\circ + \#\bullet = 0(2)$$

Thus each block must have even size, and we obtain, as claimed, $P^2 = P_{even}$.

(3) At $s = \infty$ we know that we have $H_N^\infty = K_N$. Regarding now the corresponding category, here the condition $\#\circ = \#\bullet\,(\infty)$ reads:

$$\#\circ = \#\bullet$$

But this is the condition defining $\mathcal{P}_{even}$, and so $P^\infty = \mathcal{P}_{even}$, as claimed. □

Let us go back now to probability questions, with the aim of applying the above abstract theory, to questions regarding characters. The situation here is as follows:

(1) Given a closed subgroup $G \subset_v U_N$, we know from Peter-Weyl that the moments of the main character count the fixed points of the representations $v^{\otimes k}$.

(2) On the other hand, assuming that our group $G \subset_v U_N$ is easy, coming from a category of partitions $D = (D(k,l))$, the space formed by these fixed points is spanned by the following vectors, indexed by partitions π belonging to the set $D(k) = D(0,k)$:

$$\xi_\pi = \sum_{i_1 \ldots i_k} \delta_\pi \begin{pmatrix} i_1 & \ldots & i_k \end{pmatrix} e_{i_1} \otimes \ldots \otimes e_{i_k}$$

(3) Thus, we are left with investigating linear independence questions for the vectors ξ_π, and once these questions solved, to compute the moments of χ.

In order to investigate linear independence questions for the vectors ξ_π, we will use the Gram matrix of these vectors. Let us begin with some standard definitions:

DEFINITION 14.32. *Let $P(k)$ be the set of partitions of $\{1, \ldots, k\}$, and let $\pi, \nu \in P(k)$.*

(1) *We write $\pi \leq \nu$ if each block of π is contained in a block of ν.*
(2) *We let $\pi \vee \nu \in P(k)$ be the partition obtained by superposing π, ν.*

As an illustration here, at $k = 2$ we have $P(2) = \{||, \sqcap\}$, and the order is:

$$|| \leq \sqcap$$

At $k = 3$ we have $P(3) = \{|||, \sqcap|, |\sqcap, \sqcap\!\sqcap\}$, and the order relation is as follows:

$$||| \leq \sqcap|, |\sqcap, \sqcap\!\sqcap$$

Observe also that we have $\pi, \nu \leq \pi \vee \nu$. In fact, $\pi \vee \nu$ is the smallest partition with this property, called supremum of π, ν. Now back to the easy groups, we have:

PROPOSITION 14.33. *The Gram matrix $G_{kN}(\pi, \nu) = < \xi_\pi, \xi_\nu >$ is given by*

$$G_{kN}(\pi, \nu) = N^{|\pi \vee \nu|}$$

where $|.|$ is the number of blocks.

PROOF. According to our formula of the vectors ξ_π, we have:

$$\begin{aligned} < \xi_\pi, \xi_\nu > &= \sum_{i_1 \ldots i_k} \delta_\pi(i_1, \ldots, i_k) \delta_\nu(i_1, \ldots, i_k) \\ &= \sum_{i_1 \ldots i_k} \delta_{\pi \vee \nu}(i_1, \ldots, i_k) \\ &= N^{|\pi \vee \nu|} \end{aligned}$$

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 need several standard facts about the partitions. We first have:

DEFINITION 14.34. *The Möbius function of any lattice, and so of P, is given by*

$$\mu(\pi,\nu)=\begin{cases}1 & \text{if } \pi=\nu\\ -\sum_{\pi\leq\tau<\nu}\mu(\pi,\tau) & \text{if } \pi<\nu\\ 0 & \text{if } \pi\not\leq\nu\end{cases}$$

with the construction being performed by recurrence.

As an illustration here, let us go back to the set of 2-point partitions, $P(2)=\{||,\sqcap\}$. Here 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 the following formular:

$$\mu(||,\sqcap)=-\mu(||,||)=-1$$

Finally, we have $\sqcap\not\leq||$, which gives $\mu(\sqcap,||)=0$. Thus, as a conclusion, the Möbius matrix $M_{\pi\nu}=\mu(\pi,\nu)$ 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:

$$f(\nu)=\sum_{\pi\leq\nu}g(\pi)\implies g(\nu)=\sum_{\pi\leq\nu}\mu(\pi,\nu)f(\pi)$$

In linear algebra terms, the statement and proof of this formula are as follows:

THEOREM 14.35. *The inverse of the adjacency matrix of P, given by*

$$A_{\pi\nu}=\begin{cases}1 & \text{if } \pi\leq\nu\\ 0 & \text{if } \pi\not\leq\nu\end{cases}$$

is the Möbius matrix of P, given by $M_{\pi\nu}=\mu(\pi,\nu)$.

PROOF. This is well-known, coming for instance from the fact that A is upper triangular. Thus, when inverting, we are led into the recurrence from Definition 14.34. □

As an illustration here, for $P(2)$ the formula $M=A^{-1}$ appears as follows:

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

Now back to our Gram matrix considerations, we have the following result:

PROPOSITION 14.36. *The Gram matrix is given by $G_{kN} = AL$, where*

$$L(\pi,\nu) = \begin{cases} N(N-1)\ldots(N-|\pi|+1) & \text{if } \nu \leq \pi \\ 0 & \text{otherwise} \end{cases}$$

and where $A = M^{-1}$ is the adjacency matrix of $P(k)$.

PROOF. We have the following computation:

$$\begin{aligned} N^{|\pi\vee\nu|} &= \#\left\{i_1,\ldots,i_k \in \{1,\ldots,N\}\Big|\ker i \geq \pi\vee\nu\right\} \\ &= \sum_{\tau\geq\pi\vee\nu} \#\left\{i_1,\ldots,i_k \in \{1,\ldots,N\}\Big|\ker i = \tau\right\} \\ &= \sum_{\tau\geq\pi\vee\nu} N(N-1)\ldots(N-|\tau|+1) \end{aligned}$$

According to Proposition 14.33 and to the definition of A, L, this formula reads:

$$(G_{kN})_{\pi\nu} = \sum_{\tau\geq\pi} L_{\tau\nu} = \sum_{\tau} A_{\pi\tau}L_{\tau\nu} = (AL)_{\pi\nu}$$

Thus, we obtain the formula in the statement. □

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 14.37. *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 14.36, we have:

$$\det(G_{kN}) = \det(A)\det(L)$$

Now if we order $P(k)$ as usual, 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:

PROPOSITION 14.38. *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 Peter-Weyl theory, by using the linear independence result for the vectors ξ_π coming from Theorem 14.37. □

With these preliminaries in hand, we can now state and prove:

THEOREM 14.39. *In the $N \to \infty$ limit, the laws of the main character for the main easy groups, real and complex, and discrete and continuous, are as follows,*

$$\begin{array}{ccc} K_N & \longrightarrow & U_N \\ \uparrow & & \uparrow \\ H_N & \longrightarrow & O_N \end{array} \qquad : \qquad \begin{array}{ccc} B_1 & \longrightarrow & G_1 \\ \uparrow & & \uparrow \\ b_1 & \longrightarrow & g_1 \end{array}$$

with these laws, namely the real and complex Gaussian and Bessel laws, being the main limiting laws in real and complex, and discrete and continuous probability.

PROOF. This follows from the above results. To be more precise, we know that the above groups are all easy, the corresponding categories of partitions being as follows:

$$\begin{array}{ccc} \mathcal{P}_{even} & \longleftarrow & \mathcal{P}_2 \\ \downarrow & & \downarrow \\ P_{even} & \longleftarrow & P_2 \end{array}$$

Thus, we can use Proposition 14.38, are we are led into counting partitions, and then recovering the measures via their moments, and this leads to the result. □

14d. Weingarten formula

Our aim now is to go beyond what we have, with results regarding the truncated characters. Let us start with a general formula coming from Peter-Weyl, namely:

THEOREM 14.40. *The Haar integration over a closed subgroup $G \subset_v U_N$ is given on the dense subalgebra of smooth functions by the Weingarten type formula*

$$\int_G g_{i_1j_1}^{e_1} \ldots g_{i_kj_k}^{e_k}\, dg = \sum_{\pi,\nu\in D(k)} \delta_\pi(i)\delta_\sigma(j)W_k(\pi,\nu)$$

valid for any colored integer $k = e_1 \ldots e_k$ and any multi-indices i, j, where $D(k)$ is a linear basis of $Fix(v^{\otimes k})$, the associated generalized Kronecker symbols are given by

$$\delta_\pi(i) =< \pi, e_{i_1} \otimes \ldots \otimes e_{i_k} >$$

and $W_k = G_k^{-1}$ is the inverse of the Gram matrix, $G_k(\pi,\nu) =< \pi, \nu >$.

PROOF. This is something very standard, coming from the fact that the above integrals form altogether the orthogonal projection P^k onto the following space:

$$Fix(v^{\otimes k}) = span(D(k))$$

Consider now the following linear map, with $D(k) = \{\xi_k\}$ being as in the statement:

$$E(x) = \sum_{\pi\in D(k)} < x, \xi_\pi > \xi_\pi$$

By a standard linear algebra computation, it follows that we have $P = WE$, where W is the inverse of the restriction of E to the following space:

$$K = span\left(T_\pi \middle| \pi \in D(k)\right)$$

But this restriction is the linear map given by the matrix G_k, and so W is the linear map given by the inverse matrix $W_k = G_k^{-1}$, and this gives the result. □

In the easy case, we have the following more concrete result:

THEOREM 14.41. *For an easy group $G \subset U_N$, coming from a category of partitions $D = (D(k,l))$, we have the Weingarten formula*

$$\int_G g_{i_1j_1}^{e_1} \ldots g_{i_kj_k}^{e_k}\, dg = \sum_{\pi,\nu\in D(k)} \delta_\pi(i)\delta_\nu(j)W_{kN}(\pi,\nu)$$

for any $k = e_1 \ldots e_k$ and any i, j, where $D(k) = D(\emptyset, k)$, δ are usual Kronecker type symbols, checking whether the indices match, and $W_{kN} = G_{kN}^{-1}$, with

$$G_{kN}(\pi,\nu) = N^{|\pi\vee\nu|}$$

where $|.|$ is the number of blocks.

PROOF. We use the abstract Weingarten formula, from Theorem 14.40. Indeed, the Kronecker type symbols there are then the usual ones, as shown by:

$$\begin{aligned}\delta_{\xi_\pi}(i) &= <\xi_\pi, e_{i_1}\otimes\ldots\otimes e_{i_k}>\\ &= \left\langle\sum_j\delta_\pi(j_1,\ldots,j_k)e_{j_1}\otimes\ldots\otimes e_{j_k}, e_{i_1}\otimes\ldots\otimes e_{i_k}\right\rangle\\ &= \delta_\pi(i_1,\ldots,i_k)\end{aligned}$$

The Gram matrix being as well the correct one, we obtain the result. □

Let us go back now to the general easy groups $G\subset U_N$, with the idea in mind of computing the laws of truncated characters. First, we have the following formula:

PROPOSITION 14.42. *The moments of truncated characters are given by the formula*

$$\int_G(g_{11}+\ldots+g_{ss})^k dg=Tr(W_{kN}G_{ks})$$

where G_{kN} and $W_{kN}=G_{kN}^{-1}$ are the associated Gram and Weingarten matrices.

PROOF. We have indeed the following computation:

$$\begin{aligned}\int_G(g_{11}+\ldots+g_{ss})^k dg &= \sum_{i_1=1}^s\ldots\sum_{i_k=1}^s\int_G g_{i_1i_1}\ldots g_{i_ki_k}\,dg\\ &= \sum_{\pi,\nu\in D(k)}W_{kN}(\pi,\nu)\sum_{i_1=1}^s\ldots\sum_{i_k=1}^s\delta_\pi(i)\delta_\nu(i)\\ &= \sum_{\pi,\nu\in D(k)}W_{kN}(\pi,\nu)G_{ks}(\nu,\pi)\\ &= Tr(W_{kN}G_{ks})\end{aligned}$$

Thus, we have reached to the formula in the statement. □

In order to process now the above formula, and reach to concrete results, we must impose on our group a uniformity condition. Let us start with:

PROPOSITION 14.43. *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. The equivalence (1) $\iff$ (2) comes from the inclusion $S_N \subset G_N$, which makes everything S_N-invariant. Regarding (1) $\iff$ (3), given a subgroup $K \subset_v U_{N-1}$, consider the matrix $u = diag(v, 1)$. Our claim is that for any $\pi \in P(k)$ we have:

$$\xi_\pi \in Fix(u^{\otimes k}) \iff \xi_{\pi'} \in Fix(u^{\otimes k'}), \forall \pi' \in P(k'), \pi' \subset \pi$$

In order to prove this claim, we must study the condition on the left. We have:

$$\begin{aligned}
\xi_\pi \in Fix(v^{\otimes k}) &\iff (u^{\otimes k}\xi_\pi)_{i_1\ldots i_k} = (\xi_\pi)_{i_1\ldots i_k}, \forall i\\
&\iff \sum_j (u^{\otimes k})_{i_1\ldots i_k, j_1\ldots j_k}(\xi_\pi)_{j_1\ldots j_k} = (\xi_\pi)_{i_1\ldots i_k}, \forall i\\
&\iff \sum_j \delta_\pi(j_1,\ldots,j_k)u_{i_1j_1}\ldots u_{i_kj_k} = \delta_\pi(i_1,\ldots,i_k), \forall i
\end{aligned}$$

Now let us recall that our representation has the special form $u = diag(v, 1)$. We conclude from this that for any index $a \in \{1, \ldots, k\}$, we 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:

$$\sum_{j'} \delta_\pi(j_1,\ldots,j_k)(u^{\otimes k'})_{i'j'} = \delta_\pi(i_1,\ldots,i_k), \forall i$$

Here the index j is by definition obtained from the index 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:

$$\sum_{j'} \delta_\pi(j'_1,\ldots,j'_{k'})(u^{\otimes k'})_{i'j'} = \delta_\pi(i'_1,\ldots,i'_{k'})$$

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 have $\xi_{\pi'} \in Fix(u^{\otimes k'})$ in both cases, for any subpartition $\pi' \subset \pi$, as desired. □

Now back to the laws of truncated characters, we have the following result:

THEOREM 14.44. *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 Proposition 14.42. With $s = [tN]$, the formula there becomes:

$$\int_{G_N} \chi_t^k = Tr(W_{kN} G_{k[tN]})$$

The point now is that in the uniform case the Gram matrix, and so the Weingarten matrix too, is asymptotically diagonal. Thus, we obtain the following estimate:

$$\begin{aligned}\int_{G_N} \chi_t^k &\simeq \sum_{\pi \in D(k)} W_{kN}(\pi,\pi) G_{k[tN]}(\pi,\pi)\\ &\simeq \sum_{\pi \in D(k)} N^{-|\pi|}(tN)^{|\pi|}\\ &= \sum_{\pi \in D(k)} t^{|\pi|}\end{aligned}$$

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

We can now enlarge our collection of truncated character results, and we have:

THEOREM 14.45. *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.*

PROOF. We already know these results at $t = 1$. In the general case, $t > 0$, these follow via some standard combinatorics, from the formula in Theorem 14.44. □

14e. Exercises

Exercises:

EXERCISE 14.46.

EXERCISE 14.47.

EXERCISE 14.48.

EXERCISE 14.49.

EXERCISE 14.50.

EXERCISE 14.51.

EXERCISE 14.52.

EXERCISE 14.53.

Bonus exercise.

CHAPTER 15

Quantum groups

15a. Quantum groups

What is a quantum space? Good question, most likely requiring a deep understanding of the nuclear reactors, and other such pieces of modern machinery.

Fortunately, the mathematical solution to our problem exists, due to Gelfand, with the starting definition here, that we already met in chapter 4, being as follows:

DEFINITION 15.1. *A C^*-algebra is a complex algebra A, having a norm $||.||$ making it a Banach algebra, and an involution $*$, related to the norm by the formula*

$$||aa^*|| = ||a||^2$$

which must hold for any $a \in A$.

As a basic example, the full operator algebra $B(H)$ is a C^*-algebra, and so is any norm closed $*$-subalgebra $A \subset B(H)$. It is possible to prove that a converse of this holds, in the sense that any C^*-algebra appears as an operator algebra, $A \subset B(H)$.

The key result about the C^*-algebras, due Gelfand, is as follows:

THEOREM 15.2. *Any commutative C^*-algebra A is of the form*

$$A = C(X)$$

with $X = Spec(A)$ being the space of Banach algebra characters $\chi : A \to \mathbb{C}$.

PROOF. This is something that we know too from chapter 4, the idea being that with X as in the statement, we have a morphism of algebras as follows:

$$ev : A \to C(X) \quad , \quad a \to ev_a = [\chi \to \chi(a)]$$

In order to prove that ev is involutive, we can argue that it is enough to prove that we have $ev_{a^*} = ev_a^*$ for the self-adjoint elements a. But this follows from:

$$ev_a(\chi) = \chi(a) \in \sigma(a) \subset \mathbb{R}$$

Next, since A is commutative, each element is normal, so ev is isometric:

$$||ev_a|| = \rho(a) = ||a||$$

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. □

In view of Theorem 15.2, we can formulate the following definition:

DEFINITION 15.3. *Given an arbitrary C^*-algebra A, we can write*

$$A = C(X)$$

and call the abstract space X a compact quantum space.

In other words, we can define the category of compact quantum spaces X as being the category of the C^*-algebras A, with the arrows reversed. A morphism $f : X \to Y$ corresponds by definition to a morphism $\Phi : C(Y) \to C(X)$, a product of spaces $X \times Y$ corresponds by definition to a product of algebras $C(X) \otimes C(Y)$, and so on.

All this is of course a bit speculative, and as a first true result, we have:

THEOREM 15.4. *The finite quantum spaces are exactly the disjoint unions of type*

$$X = M_{N_1} \sqcup \ldots \sqcup M_{N_k}$$

where M_N is the finite quantum space given by $C(M_N) = M_N(\mathbb{C})$.

PROOF. For a compact quantum space X, coming from a C^*-algebra A via the formula $A = C(X)$, being finite can only mean that the following number is finite:

$$|X| = \dim_{\mathbb{C}} A < \infty$$

Thus, we are led to the conclusion that we must have:

$$C(X) = M_{N_1}(\mathbb{C}) \oplus \ldots \oplus M_{N_k}(\mathbb{C})$$

But since direct sums of algebras A correspond to disjoint unions of quantum spaces X, via the correspondence $A = C(X)$, this leads to the conclusion in the statement. □

Finally, at the general level, we have as well the following key result:

THEOREM 15.5. *Any C^*-algebra appears as an operator algebra:*

$$A \subset B(H)$$

Moreover, when A is separable, which is usually the case, H can be taken separable.

PROOF. Let us first prove that the result holds in the commutative case, $A = C(X)$. Here, we can pick a positive measure on X, and construct our embedding as follows:

$$C(X) \subset B(L^2(X)) \quad , \quad f \to [g \to fg]$$

In general the proof is similar, the idea being that given a C^*-algebra A we can construct a Hilbert space $H = L^2(A)$, and then an embedding as above:

$$A \subset B(L^2(A)) \quad , \quad a \to [b \to ab]$$

Finally, the last assertion is clear, because when A is separable, meaning that it has a countable algebraic basis, so does the associated Hilbert space $H = L^2(A)$. □

We are ready now to introduce the quantum groups. The axioms here, due to Woronowicz [100], and slightly modified for our purposes, are as follows:

DEFINITION 15.6. *A Woronowicz algebra is a C^*-algebra A, given with a unitary matrix $u \in M_N(A)$ whose coefficients generate A, such that the formulae*

$$\Delta(u_{ij}) = \sum_k u_{ik} \otimes u_{kj} \quad , \quad \varepsilon(u_{ij}) = \delta_{ij} \quad , \quad S(u_{ij}) = u_{ji}^*$$

define morphisms of C^*-algebras $\Delta : A \to A \otimes A$, $\varepsilon : A \to \mathbb{C}$ and $S : A \to A^{opp}$, called comultiplication, counit and antipode.

Here the tensor product needed for Δ can be any C^*-algebra tensor product, and more on this later. In order to get rid of redundancies, coming from this and from amenability issues, we will divide everything by an equivalence relation, as follows:

DEFINITION 15.7. *We agree to identify two Woronowicz algebras, $(A, u) = (B, v)$, when we have an isomorphism of $*$-algebras*

$$< u_{ij} > \simeq < v_{ij} >$$

mapping standard coordinates to standard coordinates, $u_{ij} \to v_{ij}$.

We say that A is cocommutative when $\Sigma\Delta = \Delta$, where $\Sigma(a \otimes b) = b \otimes a$ is the flip. We have then the following key result, from [100], providing us with examples:

THEOREM 15.8. *The following are Woronowicz algebras, which are commutative, respectively cocommutative:*

(1) *$C(G)$, with $G \subset U_N$ compact Lie group. Here the structural maps are:*

$$\Delta(\varphi) = \big[(g, h) \to \varphi(gh)\big] \quad , \quad \varepsilon(\varphi) = \varphi(1) \quad , \quad S(\varphi) = \big[g \to \varphi(g^{-1})\big]$$

(2) *$C^*(\Gamma)$, with $F_N \to \Gamma$ finitely generated group. Here the structural maps are:*

$$\Delta(g) = g \otimes g \quad , \quad \varepsilon(g) = 1 \quad , \quad S(g) = g^{-1}$$

Moreover, we obtain in this way all the commutative/cocommutative algebras.

PROOF. In both cases, we first have to exhibit a certain matrix u, and then prove that we have indeed a Woronowicz algebra. The constructions are as follows:

(1) For the first assertion, we can use the matrix $u = (u_{ij})$ formed by the standard matrix coordinates of G, which is by definition given by:

$$g = \begin{pmatrix} u_{11}(g) & \ldots & u_{1N}(g) \\ \vdots & & \vdots \\ u_{N1}(g) & \ldots & u_{NN}(g) \end{pmatrix}$$

(2) For the second assertion, we can use the diagonal matrix formed by generators:

$$u = \begin{pmatrix} g_1 & & 0 \\ & \ddots & \\ 0 & & g_N \end{pmatrix}$$

Finally, regarding the last assertion, in the commutative case this follows from the Gelfand theorem, and in the cocommutative case, we will be back to this. □

In order to get now to quantum groups, we will need as well:

PROPOSITION 15.9. *Assuming that $G \subset U_N$ is abelian, we have an identification of Woronowicz algebras $C(G) = C^*(\Gamma)$, with Γ being the Pontrjagin dual of G:*

$$\Gamma = \left\{\chi : G \to \mathbb{T}\right\}$$

Conversely, assuming that $F_N \to \Gamma$ is abelian, we have an identification of Woronowicz algebras $C^*(\Gamma) = C(G)$, with G being the Pontrjagin dual of Γ:

$$G = \left\{\chi : \Gamma \to \mathbb{T}\right\}$$

Thus, the Woronowicz algebras which are both commutative and cocommutative are exactly those of type $A = C(G) = C^*(\Gamma)$, with G, Γ being abelian, in Pontrjagin duality.

PROOF. This follows from the Gelfand theorem applied to $C^*(\Gamma)$, and from the fact that the characters of a group algebra come from the characters of the group. □

In view of this result, and of the findings from Theorem 15.8 too, we have the following definition, complementing Definition 15.6 and Definition 15.7:

DEFINITION 15.10. *Given a Woronowicz algebra, we write it as follows, and call G a compact quantum Lie group, and Γ a finitely generated discrete quantum group:*

$$A = C(G) = C^*(\Gamma)$$

Also, we say that G, Γ are dual to each other, and write $G = \widehat{\Gamma}, \Gamma = \widehat{G}$.

Let us discuss now some tools for studying the Woronowicz algebras, and the underlying quantum groups. First, we have the following result:

PROPOSITION 15.11. *Let (A, u) be a Woronowicz algebra.*

(1) *Δ, ε satisfy the usual axioms for a comultiplication and a counit, namely:*

$$(\Delta \otimes id)\Delta = (id \otimes \Delta)\Delta$$

$$(\varepsilon \otimes id)\Delta = (id \otimes \varepsilon)\Delta = id$$

(2) *S satisfies the antipode axiom, on the $*$-algebra generated by entries of u:*

$$m(S \otimes id)\Delta = m(id \otimes S)\Delta = \varepsilon(.)1$$

(3) *In addition, the square of the antipode is the identity, $S^2 = id$.*

PROOF. As a first observation, the result holds in the commutative case, $A = C(G)$ with $G \subset U_N$. Indeed, here we know from Theorem 15.8 that Δ, ε, S appear as functional analytic transposes of the multiplication, unit and inverse maps m, u, i:

$$\Delta = m^t \quad , \quad \varepsilon = u^t \quad , \quad S = i^t$$

Thus, the various conditions in the statement on Δ, ε, S simply come from the group axioms satisfied by m, u, i. Observe also that the result holds as well in the cocommutative case, $A = C^*(\Gamma)$ with $F_N \to \Gamma$. In general now, the first axiom follows from:

$$(\Delta \otimes id)\Delta(u_{ij}) = (id \otimes \Delta)\Delta(u_{ij}) = \sum_{kl} u_{ik} \otimes u_{kl} \otimes u_{lj}$$

As for the other axioms, the verifications here are similar. □

In order to reach now to more advanced results, the idea will be that of doing representation theory. Following Woronowicz [100], let us start with the following definition:

DEFINITION 15.12. *Given (A, u), we call corepresentation of it any unitary matrix $v \in M_n(\mathcal{A})$, with $\mathcal{A} =< u_{ij} >$, satisfying the same conditions as u, namely:*

$$\Delta(v_{ij}) = \sum_k v_{ik} \otimes v_{kj} \quad , \quad \varepsilon(v_{ij}) = \delta_{ij} \quad , \quad S(v_{ij}) = v_{ji}^*$$

We also say that v is a representation of the underlying compact quantum group G.

In the commutative case, $A = C(G)$ with $G \subset U_N$, we obtain in this way the finite dimensional unitary smooth representations $v : G \to U_n$, via the following formula:

$$v(g) = \begin{pmatrix} v_{11}(g) & \ldots & v_{1n}(g) \\ \vdots & & \vdots \\ v_{n1}(g) & \ldots & v_{nn}(g) \end{pmatrix}$$

With this convention, we have the following fundamental result, from [100]:

THEOREM 15.13. *Any Woronowicz algebra has a unique Haar integration functional,*

$$\left(\int_G \otimes id\right)\Delta = \left(id \otimes \int_G\right)\Delta = \int_G (.)1$$

which can be constructed by starting with any faithful positive form $\varphi \in A^*$, 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 corepresentation $v \in M_n(\mathbb{C}) \otimes A$ 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. Following [100], this can be done in 3 steps, as follows:

(1) Given $\varphi \in A^*$, our claim is that the following limit converges, for any $a \in A$:

$$\int_\varphi a = \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \varphi^{*k}(a)$$

Indeed, by linearity we can assume that $a \in A$ is the coefficient of certain corepresentation, $a = (\tau \otimes id)v$. But in this case, an elementary computation gives the following formula, with P_φ being the orthogonal projection onto the 1-eigenspace of $(id \otimes \varphi)v$:

$$\left(id \otimes \int_\varphi\right) v = P_\varphi$$

(2) Since $v\xi = \xi$ implies $[(id \otimes \varphi)v]\xi = \xi$, we have $P_\varphi \geq P$, where P is the orthogonal projection onto the fixed point space in the statement, namely:

$$Fix(v) = \left\{\xi \in \mathbb{C}^n \middle| v\xi = \xi\right\}$$

The point now is that when $\varphi \in A^*$ is faithful, by using a standard positivity trick, we can prove that we have $P_\varphi = P$, exactly as in the classical case.

(3) With the above formula in hand, the left and right invariance of $\int_G = \int_\varphi$ is clear on coefficients, and so in general, and this gives all the assertions. See [100]. □

We can now develop, again following [100], the Peter-Weyl theory for the corepresentations of A. Consider the dense subalgebra $\mathcal{A} \subset A$ generated by the coefficients of the fundamental corepresentation u, and endow it with the following scalar product:

$$< a, b >= \int_G ab^*$$

With this convention, we have the following result, also from [100]:

THEOREM 15.14. *We have the following Peter-Weyl type results:*

(1) *Any corepresentation decomposes as a sum of irreducible corepresentations.*
(2) *Each irreducible corepresentation appears inside a certain $u^{\otimes k}$.*
(3) $\mathcal{A} = \bigoplus_{v\in Irr(A)} M_{\dim(v)}(\mathbb{C})$, *the summands being pairwise orthogonal.*
(4) *The characters of irreducible corepresentations form an orthonormal system.*

PROOF. This is something that we met in chapters 5 and 14, in the case where $G \subset U_N$ is a finite group, or more generally a compact group. In general, when G is a compact quantum group, the proof is quite similar, by using Theorem 15.13. □

Finally, no discussion about compact and discrete quantum groups would be complete without a word on amenability. The result here, again from [100], is as follows:

THEOREM 15.15. *Let A_{full} be the enveloping C^*-algebra of $\mathcal{A}$, and A_{red} be the quotient of A by the null ideal of the Haar integration. The following are then equivalent:*

(1) *The Haar functional of A_{full} is faithful.*
(2) *The projection map $A_{full} \to A_{red}$ is an isomorphism.*
(3) *The counit map $\varepsilon : A_{full} \to \mathbb{C}$ factorizes through A_{red}.*
(4) *We have $N \in \sigma(Re(\chi_u))$, the spectrum being taken inside A_{red}.*

If this is the case, we say that the underlying discrete quantum group Γ is amenable.

PROOF. This is well-known in the group dual case, $A = C^*(\Gamma)$, with Γ being a usual discrete group. In general, the result follows by adapting the group dual case proof:

(1) $\iff$ (2) This simply follows from the fact that the GNS construction for the algebra A_{full} with respect to the Haar functional produces the algebra A_{red}.

(2) $\iff$ (3) Here $\implies$ is trivial, and conversely, a counit $\varepsilon : A_{red} \to \mathbb{C}$ produces an isomorphism $\Phi : A_{red} \to A_{full}$, by slicing the map $\widetilde{\Delta} : A_{red} \to A_{red} \otimes A_{full}$.

(3) $\iff$ (4) Here $\implies$ is clear, coming from $\varepsilon(N - Re(\chi(u))) = 0$, and the converse can be proved by doing some functional analysis. See [100]. □

This was for the basic theory of the quantum groups in the sense of Woronowicz, quickly explained. For more on all this, we have for instance my book [8].

15b. Quantum permutations

Following Wang, let us discuss now the construction and basic properties of the quantum permutation group S_N^+. Let us first look at S_N. We have here:

THEOREM 15.16. *The algebra of functions on S_N has the following presentation,*

$$C(S_N) = C^*_{comm}\left((u_{ij})_{i,j=1,\ldots,N}\middle| u = \text{magic}\right)$$

and the multiplication, unit and inversion map of S_N appear from the maps

$$\Delta(u_{ij}) = \sum_k u_{ik} \otimes u_{kj} \quad , \quad \varepsilon(u_{ij}) = \delta_{ij} \quad , \quad S(u_{ij}) = u_{ji}$$

defined at the algebraic level, of functions on S_N, by transposing.

PROOF. This is something that we know from chapter 4, coming from the Gelfand theorem, applied to the universal algebra in the statement. Indeed, that algebra follows to be of the form $A = C(X)$, with X being a certain compact space. Now since we have coordinates $u_{ij} : X \to \mathbb{R}$, we have an embedding $X \subset M_N(\mathbb{R})$. Also, since we know that these coordinates form a magic matrix, the elements $g \in X$ must be 0-1 matrices, having exactly one 1 entry on each row and each column, and so $X = S_N$, as desired. □

Following now Wang, we can liberate S_N, as follows:

THEOREM 15.17. *The following universal C^*-algebra, with magic meaning as usual formed by projections ($p^2 = p^* = p$), summing up to 1 on each row and each column,*

$$C(S_N^+) = C^*\left((u_{ij})_{i,j=1,\ldots,N}\middle| u = \text{magic}\right)$$

is a Woronowicz algebra, with comultiplication, counit and antipode given by:

$$\Delta(u_{ij}) = \sum_k u_{ik} \otimes u_{kj} \quad , \quad \varepsilon(u_{ij}) = \delta_{ij} \quad , \quad S(u_{ij}) = u_{ji}$$

Thus the space S_N^+ is a compact quantum group, called quantum permutation group.

PROOF. As a first observation, the universal C^*-algebra in the statement is indeed well-defined, because the conditions $p^2 = p^* = p$ satisfied by the coordinates give:

$$||u_{ij}|| \leq 1$$

In order to prove now that we have a Woronowicz algebra, we must construct maps Δ, ε, S given by the formulae in the statement. Consider the following matrices:

$$u_{ij}^{\Delta} = \sum_k u_{ik} \otimes u_{kj} \quad , \quad u_{ij}^{\varepsilon} = \delta_{ij} \quad , \quad u_{ij}^{S} = u_{ji}$$

Our claim is that, since u is magic, so are these three matrices. Indeed, regarding u^{Δ}, its entries are idempotents, as shown by the following computation:

$$(u_{ij}^{\Delta})^2 = \sum_{kl} u_{ik}u_{il} \otimes u_{kj}u_{lj} = \sum_{kl} \delta_{kl}u_{ik} \otimes \delta_{kl}u_{kj} = u_{ij}^{\Delta}$$

These elements are self-adjoint as well, as shown by the following computation:

$$(u_{ij}^{\Delta})^* = \sum_k u_{ik}^* \otimes u_{kj}^* = \sum_k u_{ik} \otimes u_{kj} = u_{ij}^{\Delta}$$

The row and column sums for the matrix u^{Δ} can be computed as follows:

$$\sum_j u_{ij}^{\Delta} = \sum_{jk} u_{ik} \otimes u_{kj} = \sum_k u_{ik} \otimes 1 = 1$$

$$\sum_i u_{ij}^{\Delta} = \sum_{ik} u_{ik} \otimes u_{kj} = \sum_k 1 \otimes u_{kj} = 1$$

Thus, u^{Δ} is magic. Regarding now u^{ε}, u^S, these matrices are magic too, and this for obvious reasons. Thus, all our three matrices $u^{\Delta}, u^{\varepsilon}, u^S$ are magic, so we can define Δ, ε, S by the formulae in the statement, by using the universality property of $C(S_N^+)$. □

Our first task now is to make sure that Theorem 15.17 produces indeed a new quantum group, which does not collapse to S_N. Following Wang, we have:

THEOREM 15.18. *We have an embedding $S_N \subset S_N^+$, given at the algebra level by:*

$$u_{ij} \to \chi\left(\sigma \in S_N \middle| \sigma(j) = i\right)$$

This is an isomorphism at $N \leq 3$, but not at $N \geq 4$, where S_N^+ is not classical, nor finite.

PROOF. The fact that we have indeed an embedding as above follows from Theorem 15.16. Observe that in fact more is true, because Theorems 15.16 and 15.17 give:

$$C(S_N) = C(S_N^+) \Big/ \Big\langle ab = ba \Big\rangle$$

Regarding now the second assertion, we can prove this in four steps, as follows:

Case $N = 2$. The fact that S_2^+ is indeed classical, and hence collapses to S_2, is trivial, because the 2×2 magic matrices are as follows, with p being a projection:

$$U = \begin{pmatrix} p & 1-p \\ 1-p & p \end{pmatrix}$$

Thus $C(S_2^+)$ is commutative, and equals its biggest commutative quotient, $C(S_2)$.

Case $N = 3$. It is enough to check that u_{11}, u_{22} commute. But this follows from:

$$\begin{aligned} u_{11}u_{22} &= u_{11}u_{22}(u_{11} + u_{12} + u_{13}) \\ &= u_{11}u_{22}u_{11} + u_{11}u_{22}u_{13} \\ &= u_{11}u_{22}u_{11} + u_{11}(1 - u_{21} - u_{23})u_{13} \\ &= u_{11}u_{22}u_{11} \end{aligned}$$

Indeed, by conjugating, $u_{22}u_{11} = u_{11}u_{22}u_{11}$, so $u_{11}u_{22} = u_{22}u_{11}$, as desired.

Case $N = 4$. Consider the following matrix, with p, q being projections:

$$U = \begin{pmatrix} p & 1-p & 0 & 0 \\ 1-p & p & 0 & 0 \\ 0 & 0 & q & 1-q \\ 0 & 0 & 1-q & q \end{pmatrix}$$

This matrix is magic, and we can choose $p, q \in B(H)$ as for the algebra $< p, q >$ to be noncommutative and infinite dimensional. We conclude that $C(S_4^+)$ is noncommutative and infinite dimensional as well, and so S_4^+ is non-classical and infinite, as claimed.

Case $N \geq 5$. Here we can use the standard embedding $S_4^+ \subset S_N^+$, obtained at the level of the corresponding magic matrices in the following way:

$$u \to \begin{pmatrix} u & 0 \\ 0 & 1_{N-4} \end{pmatrix}$$

Indeed, with this in hand, the fact that S_4^+ is a non-classical, infinite compact quantum group implies that S_N^+ with $N \geq 5$ has these two properties as well. □

As a first observation, as a matter of doublechecking our findings, we are not wrong with our formalism, because as discovered once again by Wang, we have as well:

THEOREM 15.19. *The quantum permutation group S_N^+ acts on the set $X = \{1, \ldots, N\}$, the corresponding coaction map $\Phi : C(X) \to C(X) \otimes C(S_N^+)$ being given by:*

$$\Phi(e_i) = \sum_j e_j \otimes u_{ji}$$

In fact, S_N^+ is the biggest compact quantum group acting on X, by leaving the counting measure invariant, in the sense that $(tr \otimes id)\Phi = tr(.)1$, where $tr(e_i) = \frac{1}{N}, \forall i$.

PROOF. Our claim is that given a compact matrix quantum group G, the following formula defines a morphism of algebras, which is a coaction map, leaving the trace invariant, precisely when the matrix $u = (u_{ij})$ is a magic corepresentation of $C(G)$:

$$\Phi(e_i) = \sum_j e_j \otimes u_{ji}$$

Indeed, let us first determine when Φ is multiplicative. We have:

$$\Phi(e_i)\Phi(e_k) = \sum_{jl} e_j e_l \otimes u_{ji} u_{lk} = \sum_j e_j \otimes u_{ji} u_{jk}$$

$$\Phi(e_i e_k) = \delta_{ik}\Phi(e_i) = \delta_{ik} \sum_j e_j \otimes u_{ji}$$

We conclude that the multiplicativity of Φ is equivalent to the following conditions:

$$u_{ji} u_{jk} = \delta_{ik} u_{ji} \quad , \quad \forall i, j, k$$

Similarly, Φ is unital when $\sum_i u_{ji} = 1$, $\forall j$. Finally, the fact that Φ is a $*$-morphism translates into $u_{ij} = u_{ij}^*$, $\forall i, j$. Summing up, in order for $\Phi(e_i) = \sum_j e_j \otimes u_{ji}$ to be a morphism of C^*-algebras, the elements u_{ij} must be projections, summing up to 1 on each row of u. Regarding now the preservation of the trace, observe that we have:

$$(tr \otimes id)\Phi(e_i) = \frac{1}{N} \sum_j u_{ji}$$

Thus the trace is preserved precisely when the elements u_{ij} sum up to 1 on each of the columns of u. We conclude from this that $\Phi(e_i) = \sum_j e_j \otimes u_{ji}$ is a morphism of C^*-algebras preserving the trace precisely when u is magic, and this gives the result. □

Many other things can be said about S_N^+. We will be back to this.

15c. Liberation theory

In order to study S_N^+, and better understand the liberation operation $S_N \to S_N^+$, we can use representation theory. We have the following version of Tannakian duality:

THEOREM 15.20. *The following operations are inverse to each other:*

(1) *The construction $A \to C$, which associates to any Woronowicz algebra A the tensor category formed by the intertwiner spaces $C_{kl} = Hom(u^{\otimes k}, u^{\otimes l})$.*
(2) *The construction $C \to A$, which associates to a tensor category C the Woronowicz algebra A presented by the relations $T \in Hom(u^{\otimes k}, u^{\otimes l})$, with $T \in C_{kl}$.*

PROOF. This is something quite deep, with the idea being as follows:

– We have indeed a construction $A \to C$ as above, whose output is a tensor C^*-subcategory with duals of the tensor C^*-category of Hilbert spaces.

– We have as well a construction $C \to A$ as above, simply by dividing the free $*$-algebra on N^2 variables by the relations in the statement.

Some elementary algebra shows then that $C = C_{A_C}$ implies $A = A_{C_A}$, and also that $C \subset C_{A_C}$ is automatic. Thus we are left with proving $C_{A_C} \subset C$, and this can be done by doing some algebra, and using von Neumann's bicommutant theorem. See [8]. □

We will need as well the notion of "easiness". Let us start with the following definition:

DEFINITION 15.21. *Let $P(k,l)$ be the set of partitions between an upper row of k points, and a lower row of l points. A set $D = \bigsqcup_{k,l} D(k,l)$ 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 the vertical concatenation, $(\pi, \sigma) \to \left[\begin{smallmatrix}\sigma\\ \pi\end{smallmatrix}\right]$.*
(3) *Stability under the upside-down turning, $\pi \to \pi^*$.*
(4) *Each set $P(k,k)$ contains the identity partition $|| \ldots ||$.*
(5) *The set $P(0,2)$ contains the semicircle partition $\cap$.*

Observe that this is precisely the definition that we used in chapter 7, with the condition there on the basic crossing $\diagdown\!\!\diagup$, which produces commutativity via Tannakian duality, removed. In relation with the quantum groups, we have the following notion:

DEFINITION 15.22. *A compact quantum matrix group G is called easy when*

$$Hom(u^{\otimes k}, u^{\otimes l}) = span\left(T_\pi \middle| \pi \in D(k,l)\right)$$

for any colored integers k, l, for certain sets of partitions $D(k,l) \subset P(k,l)$, where

$$T_\pi(e_{i_1} \otimes \ldots \otimes e_{i_k}) = \sum_{j_1 \ldots j_l} \delta_\pi \begin{pmatrix} i_1 & \ldots & i_k \\ j_1 & \ldots & j_l \end{pmatrix} e_{j_1} \otimes \ldots \otimes e_{j_l}$$

with the Kronecker type symbols $\delta_\pi \in \{0,1\}$ depending on whether the indices fit or not.

Again, this is something coming as a continuation of the material from chapter 7, and for more on this definition, and its meaning, we refer to the material there.

Many things can be said here, but getting now straight to the point, we have:

THEOREM 15.23. *We have the following results:*

(1) S_N *is easy, coming from the category of all partitions* P.
(2) S_N^+ *is easy, coming from the category of all noncrossing partitions* NC.

PROOF. This is something quite fundamental, with the proof, using the above Tannakian results and subsequent easiness theory, being as follows:

(1) S_N^+. We know that this quantum group comes from the magic condition. In order to interpret this magic condition, consider the fork partition:

$$Y \in P(2,1)$$

By arguing as in chapter 7, we conclude that we have the following equivalence:

$$T_Y \in Hom(u^{\otimes 2}, u) \iff u_{ij}u_{ik} = \delta_{jk}u_{ij}, \forall i,j,k$$

The condition on the right being equivalent to the magic condition, we conclude that S_N^+ is indeed easy, the corresponding category of partitions being, as desired:

$$D = < Y > = NC$$

(2) S_N. Here there is no need for new computations, because we have:

$$S_N = S_N^+ \cap O_N$$

At the categorical level means that S_N is easy, coming from:

$$< NC, \diagdown\!\!\diagdown > = P$$

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

Summarizing, we have now a good understanding of the liberation operation $S_N \to S_N^+$, the idea being that this comes, via Tannakian duality, from $P \to NC$:

THEOREM 15.24. *The operation* $S_N \to S_N^+$ *is an easy liberation, in the sense that it appears, at the level of the corresponding categories of partitions, from* $P \to NC$.

PROOF. This follows indeed from Theorem 15.23. □

Many other things can be said here, with results for the reflection groups too.

In order to go further in this direction, we will need the following result, with $*$ being the classical convolution, and $\boxplus$ being Voiculescu's free convolution operation [91]:

THEOREM 15.25. *The following Poisson type limits converge, for any $t > 0$,*

$$p_t = \lim_{n\to\infty} \left(\left(1 - \frac{1}{n} \right) \delta_0 + \frac{1}{n} \delta_t \right)^{*n}$$

$$\pi_t = \lim_{n\to\infty} \left(\left(1 - \frac{1}{n} \right) \delta_0 + \frac{1}{n} \delta_t \right)^{\boxplus n}$$

the limiting measures being the Poisson law p_t, and the Marchenko-Pastur law π_t,

$$p_t = \frac{1}{e^t} \sum_{k=0}^{\infty} \frac{t^k \delta_k}{k!}$$

$$\pi_t = \max(1-t, 0)\delta_0 + \frac{\sqrt{4t - (x-1-t)^2}}{2\pi x}\, dx$$

whose moments are given by the following formulae:

$$M_k(p_t) = \sum_{\pi \in P(k)} t^{|\pi|} \quad , \quad M_k(\pi_t) = \sum_{\pi \in NC(k)} t^{|\pi|}$$

The Marchenko-Pastur measure π_t is also called free Poisson law.

PROOF. This is something quite advanced, related to probability theory, free probability theory, and random matrices, the idea being as follows:

(1) The first step is that of finding suitable functional transforms, which linearize the convolution operations in the statement. In the classical case this is the logarithm of the Fourier transform $\log F$, and in the free case this is Voiculescu's R-transform.

(2) With these tools in hand, the above limiting theorems can be proved in a standard way, a bit as when proving the Central Limit Theorem. The computations give the moment formulae in the statement, and the density computations are standard as well.

(3) Finally, in order for the discussion to be complete, what still remains to be explained is the precise nature of the "liberation" operation $p_t \to \pi_t$, as well as the random matrix occurrence of π_t. This is more technical, and we refer here to [74], [91]. □

Getting back now to quantum permutations, the results here are as follows:

THEOREM 15.26. *The law of the main character, given by*

$$\chi = \sum_i u_{ii}$$

for S_N/S_N^+ becomes p_1/π_1 with $N \to \infty$. As for the truncated character

$$\chi_t = \sum_{i=1}^{[tN]} u_{ii}$$

for S_N/S_N^+, with $t \in (0, 1]$, this becomes p_t/π_t with $N \to \infty$.

PROOF. This is again something quite technical, the idea being as follows:

(1) In the classical case this is well-known, and follows by using the inclusion-exclusion principle, and then letting $N \to \infty$, as explained in chapter 2.

(2) In the free case there is no such simple argument, and we must use what we know about S_N^+, namely its easiness property. We know from easiness that we have:

$$Fix(u^{\otimes k}) = span(NC(k))$$

On the other hand, a direct computation shows that the partitions in $P(k)$, and in particular those in $NC(k)$, implemented as linear maps via the operation $\pi \to T_\pi$ from Definition 15.22, become linearly independent with $N \geq k$. Thus we have, as desired:

$$\begin{aligned}\int_{S_N^+} \chi^k &= \dim\left(Fix(u^{\otimes k})\right)\\ &= \dim\left(span\left(T_\pi\middle|\pi \in NC(k)\right)\right)\\ &\simeq |NC(k)|\\ &= \sum_{\pi\in NC(k)} 1^{|\pi|}\end{aligned}$$

(3) In the general case now, where our parameter is an arbitrary number $t \in (0, 1]$, the above computation does not apply, but we can still get away with Peter-Weyl theory. Indeed, we know from Theorem 15.13 how to compute the Haar integration of S_N^+, out of the knowledge of the fixed point spaces $Fix(u^{\otimes k})$, and in practice, by using easiness, this leads to the following formula, called Weingarten integration formula:

$$\int_{S_N^+} u_{i_1j_1} \ldots u_{i_kj_k} = \sum_{\pi,\sigma\in NC(k)} \delta_\pi(i)\delta_\sigma(j)W_{kN}(\pi, \sigma)$$

Here the δ symbols are Kronecker type symbols, checking whether the indices fit or not with the partitions, and $W_{kN} = G_{kN}^{-1}$, with $G_{kN}(\pi, \sigma) = N^{|\pi\vee\sigma|}$, where $|.|$ is the number of blocks. Now by using this formula for computing the moments of χ_t, we obtain:

$$\begin{aligned}\int_{S_N^+} \chi_t^k &= \sum_{i_1=1}^{[tN]} \ldots \sum_{i_k=1}^{[tN]} \int u_{i_1i_1} \ldots u_{i_ki_k}\\ &= \sum_{\pi,\sigma\in NC(k)} W_{kN}(\pi, \sigma) \sum_{i_1=1}^{[tN]} \ldots \sum_{i_k=1}^{[tN]} \delta_\pi(i)\delta_\sigma(i)\\ &= \sum_{\pi,\sigma\in NC(k)} W_{kN}(\pi, \sigma)G_{k[tN]}(\sigma, \pi)\\ &= Tr(W_{kN}G_{k[tN]})\end{aligned}$$

(4) The point now is that with $N \to \infty$ the Gram matrix G_{kN}, and so the Weingarten matrix W_{kN} too, becomes asymptotically diagonal. We therefore obtain:

$$\int_{S_N^+} \chi_t^k \simeq \sum_{\pi \in NC(k)} t^{|\pi|}$$

Thus, we are led to the conclusion in the statement. For details, see [9]. □

15d. Quantum reflections

Getting now to quantum reflections, whose construction and properties we would like to explain now, we first have the following result, which is something very standard:

THEOREM 15.27. *Consider the graph consisting of N segments.*

(1) *Its symmetry group is the hyperoctahedral group $H_N = \mathbb{Z}_2 \wr S_N$.*
(2) *Its quantum symmetry group is the quantum group $H_N^+ = \mathbb{Z}_2 \wr_* S_N^+$.*

PROOF. This is something very standard, the idea being as follows:

(1) This is clear indeed from definitions, and with the remark that the group H_N appears as well as the symmetry group of the hypercube, $G(\square_N) = H_N$.

(2) This is something which is standard too, a bit like in the classical case, and with the remark that for the hypercube we obtain something different, $G(\square_N) = O_N^{-1}$. □

In order to further study H_N^+, we first have the following result:

PROPOSITION 15.28. *The algebra $C(H_N^+)$ can be presented in two ways, as follows:*

(1) *As the universal algebra generated by the entries of a $2N \times 2N$ magic unitary having the "sudoku" pattern $w = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$, with a, b being square matrices.*
(2) *As the universal algebra generated by the entries of a $N \times N$ orthogonal matrix which is "cubic", in the sense that $u_{ij}u_{ik} = u_{ji}u_{ki} = 0$, for any $j \neq k$.*

As for $C(H_N)$, this has similar presentations, among the commutative algebras.

PROOF. We must prove that the algebras A_s, A_c coming from (1,2) coincide. We can define a morphism $A_c \to A_s$ by the following formula:

$$\varphi(u_{ij}) = a_{ij} - b_{ij}$$

We construct now the inverse morphism. Consider the following elements:

$$\alpha_{ij} = \frac{u_{ij}^2 + u_{ij}}{2} \quad , \quad \beta_{ij} = \frac{u_{ij}^2 - u_{ij}}{2}$$

These are projections, and the following matrix is a sudoku unitary:

$$M = \begin{pmatrix} (\alpha_{ij}) & (\beta_{ij}) \\ (\beta_{ij}) & (\alpha_{ij}) \end{pmatrix}$$

Thus we can define a morphism $A_s \to A_c$ by the following formula:

$$\psi(a_{ij}) = \frac{u_{ij}^2 + u_{ij}}{2} \quad , \quad \psi(b_{ij}) = \frac{u_{ij}^2 - u_{ij}}{2}$$

We check now the fact that ψ, φ are indeed inverse morphisms:

$$\psi\varphi(u_{ij}) = \psi(a_{ij} - b_{ij}) = \frac{u_{ij}^2 + u_{ij}}{2} - \frac{u_{ij}^2 - u_{ij}}{2} = u_{ij}$$

As for the other composition, we have the following computation:

$$\varphi\psi(a_{ij}) = \varphi\left(\frac{u_{ij}^2 + u_{ij}}{2}\right) = \frac{(a_{ij} - b_{ij})^2 + (a_{ij} - b_{ij})}{2} = a_{ij}$$

A similar computation gives $\varphi\psi(b_{ij}) = b_{ij}$, as desired. As for the final assertion, regarding $C(H_N)$, this follows from the above results, by taking classical versions. □

We can now work out the easiness property of H_N, H_N^+, with respect to the cubic representations, and we are led to the following result:

THEOREM 15.29. *The quantum groups H_N, H_N^+ are both easy, as follows:*

(1) *H_N corresponds to the category P_{even}.*
(2) *H_N^+ corresponds to the category NC_{even}.*

PROOF. This is something quite routine, the idea being as follows:

(1) We know that $H_N^+ \subset O_N^+$ appears via the cubic relations, namely:

$$u_{ij}u_{ik} = u_{ji}u_{ki} = 0 \quad , \quad \forall j \neq k$$

Our claim is that, in Tannakian terms, these relations reformulate as follows, with $H \in P(2,2)$ being the 1-block partition, joining all 4 points:

$$T_H \in End(u^{\otimes 2})$$

(2) In order to prove our claim, observe first that we have, by definition of T_H:

$$T_H(e_i \otimes e_j) = \delta_{ij} e_i \otimes e_i$$

With this formula in hand, we have the following computation:

$$\begin{aligned} T_H u^{\otimes 2}(e_i \otimes e_j \otimes 1) &= T_H\left(\sum_{abij} e_{ai} \otimes e_{bj} \otimes u_{ai}u_{bj}\right)(e_i \otimes e_j \otimes 1) \\ &= T_H \sum_{ab} e_a \otimes e_b \otimes u_{ai}u_{bj} \\ &= \sum_a e_a \otimes e_a \otimes u_{ai}u_{aj} \end{aligned}$$

On the other hand, we have as well the following computation:

$$\begin{aligned} u^{\otimes 2}T_H(e_i\otimes e_j\otimes 1) &= \delta_{ij}u^{\otimes 2}(e_i\otimes e_j\otimes 1)\\ &= \delta_{ij}\left(\sum_{abij}e_{ai}\otimes e_{bj}\otimes u_{ai}u_{bj}\right)(e_i\otimes e_j\otimes 1)\\ &= \delta_{ij}\sum_{ab}e_a\otimes e_b\otimes u_{ai}u_{bi} \end{aligned}$$

We conclude that $T_Hu^{\otimes 2}=u^{\otimes 2}T_H$ means that u is cubic, as desired.

(3) With our claim proved, we can go back to H_N^+. Indeed, it follows from Tannakian duality that this quantum group is easy, coming from the following category:

$$D=<H>=NC_{even}$$

(4) But this proves as well the result for H_N. Indeed, since this group is the classical version of H_N^+, we have as desired easiness, the corresponding category being:

$$E=<NC_{even},\diagdown\!\!\diagdown>=P_{even}$$

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

As an immediate consequence of the above result, we have:

THEOREM 15.30. *The operation $H_N\to H_N^+$ is a liberation in the sense of easy quantum groups, in the sense that the category of partitions for H_N^+ appears as*

$$D^+=D\cap NC$$

with D being the category of partitions for H_N.

PROOF. We already know, from definitions, that $H_N\to H_N^+$ is a liberation, in the sense that the classical version of H_N^+ is H_N. However, by using Theorem 15.29, we can see that much more is true, in the sense that $H_N\to H_N^+$ is an easy quantum group liberation, as stated, and with this coming from $NC_{even}=P_{even}\cap NC$. □

The free analogues of the reflection groups H_N^s can be constructed as follows:

DEFINITION 15.31. *The algebra $C(H_N^{s+})$ is the universal C^*-algebra generated by N^2 normal elements u_{ij}, subject to the following relations,*

(1) *$u=(u_{ij})$ is unitary,*
(2) *$u^t=(u_{ji})$ is unitary,*
(3) *$p_{ij}=u_{ij}u_{ij}^*$ is a projection,*
(4) *$u_{ij}^s=p_{ij}$,*

with Woronowicz algebra maps Δ,ε,S constructed by universality.

Here we allow the value $s = \infty$, with the convention that the last axiom simply disappears in this case. Observe that at $s < \infty$ the normality condition is actually redundant. This is because a partial isometry a subject to the relation $aa^* = a^s$ is normal. As a first result now, making the connection with H_N^s, we have:

THEOREM 15.32. *We have an inclusion of quantum groups*

$$H_N^s \subset H_N^{s+}$$

which is a liberation, in the sense that the classical version of H_N^{s+}, obtained by dividing by the commutator ideal, is the group H_N^s.

PROOF. This follows as before for $O_N \subset O_N^+$ or for $S_N \subset S_N^+$, by using the Gelfand theorem, applied to the quotient of $C(H_N^{s+})$ by its commutator ideal. □

In analogy with the results from the real case, we have the following result:

PROPOSITION 15.33. *The algebras $C(H_N^{s+})$ with $s = 1, 2, \infty$, and their presentation relations in terms of the entries of the matrix $u = (u_{ij})$, are as follows:*

(1) *For $C(H_N^{1+}) = C(S_N^+)$, the matrix u is magic: all its entries are projections, summing up to 1 on each row and column.*
(2) *For $C(H_N^{2+}) = C(H_N^+)$ the matrix u is cubic: it is orthogonal, and the products of pairs of distinct entries on the same row or the same column vanish.*
(3) *For $C(H_N^{\infty+}) = C(K_N^+)$ the matrix u is unitary, its transpose is unitary, and all its entries are normal partial isometries.*

PROOF. This is something elementary, the idea being as follows:

(1) This follows from definitions and from standard operator algebra tricks.

(2) This follows as well from definitions and standard operator algebra tricks.

(3) This is just a translation of the definition of $C(H_N^{s+})$, at $s = \infty$. □

Let us prove now that H_N^{s+} with $s < \infty$ is a quantum permutation group. For this purpose, we must change the fundamental representation. Let us start with:

DEFINITION 15.34. *A (s, N)-sudoku matrix is a magic unitary of size sN, of the form*

$$m = \begin{pmatrix} a^0 & a^1 & \ldots & a^{s-1} \\ a^{s-1} & a^0 & \ldots & a^{s-2} \\ \vdots & \vdots & & \vdots \\ a^1 & a^2 & \ldots & a^0 \end{pmatrix}$$

where $a^0, \ldots, a^{s-1}$ are $N \times N$ matrices.

The basic examples of such matrices come from the group H_n^s. Indeed, with $w = e^{2\pi i/s}$, each of the N^2 matrix coordinates $u_{ij} : H_N^s \to \mathbb{C}$ takes values in the following set:

$$S = \{0\} \cup \{1, w, \ldots, w^{s-1}\}$$

Thus, this coordinate function $u_{ij} : H_N^s \to \mathbb{C}$ decomposes as follows:

$$u_{ij} = \sum_{r=0}^{s-1} w^r a_{ij}^r$$

Here each function a_{ij}^r is a function taking values in $\{0, 1\}$, and so is a projection in the C^*-algebra sense, and it follows from definitions that these projections form indeed a sudoku matrix. Now with this notion in hand, we have the following result:

THEOREM 15.35. *The following happen:*

(1) *The algebra $C(H_N^s)$ is isomorphic to the universal commutative C^*-algebra generated by the entries of a (s, N)-sudoku matrix.*
(2) *The algebra $C(H_N^{s+})$ is isomorphic to the universal C^*-algebra generated by the entries of a (s, N)-sudoku matrix.*

PROOF. The first assertion follows from the second one, via Theorem 15.32. In order to prove the second assertion, consider the universal algebra in the statement, namely:

$$A = C^* \left(a_{ij}^p \;\middle|\; \left(a_{ij}^{q-p}\right)_{pi,qj} = (s, N) - \text{sudoku} \right)$$

Consider also the algebra $C(H_N^{s+})$. According to Definition 15.31, this is presented by certain relations R, that we will call here level s cubic conditions:

$$C(H_N^{s+}) = C^* \left(u_{ij} \;\middle|\; u = N \times N \text{ level } s \text{ cubic} \right)$$

We will construct a pair of inverse morphisms between these algebras.

(1) Our first claim is that $U_{ij} = \sum_p w^{-p} a_{ij}^p$ is a level s cubic unitary. Indeed, by using the sudoku condition, the verification of (1-4) in Definition 15.31 is routine.

(2) Our second claim is that the elements $A_{ij}^p = \frac{1}{s} \sum_r w^{rp} u_{ij}^r$, with the convention $u_{ij}^0 = p_{ij}$, form a level s sudoku unitary. Once again, the proof here is routine.

(3) According to the above, we can define a morphism $\Phi : C(H_N^{s+}) \to A$ by the formula $\Phi(u_{ij}) = U_{ij}$, and a morphism $\Psi : A \to C(H_N^{s+})$ by the formula $\Psi(a_{ij}^p) = A_{ij}^p$.

(4) We check now the fact that Φ, Ψ are indeed inverse morphisms:

$$\begin{aligned}\Psi\Phi(u_{ij}) &= \sum_p w^{-p} A_{ij}^p \\ &= \frac{1}{s}\sum_p w^{-p} \sum_r w^{rp} u_{ij}^r \\ &= \frac{1}{s}\sum_{pr} w^{(r-1)p} u_{ij}^r \\ &= u_{ij}\end{aligned}$$

As for the other composition, we have the following computation:

$$\begin{aligned}\Phi\Psi(a_{ij}^p) &= \frac{1}{s}\sum_r w^{rp} U_{ij}^r \\ &= \frac{1}{s}\sum_r w^{rp} \sum_q w^{-rq} a_{ij}^q \\ &= \frac{1}{s}\sum_q a_{ij}^q \sum_r w^{r(p-q)} \\ &= a_{ij}^p\end{aligned}$$

Thus we have an isomorphism $C(H_N^{s+}) = A$, as claimed. □

In order to further advance, we will need the following simple fact:

PROPOSITION 15.36. *A $sN \times sN$ magic unitary commutes with the matrix*

$$\Sigma = \begin{pmatrix} 0 & I_N & 0 & \ldots & 0 \\ 0 & 0 & I_N & \ldots & 0 \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & 0 & \ldots & I_N \\ I_N & 0 & 0 & \ldots & 0 \end{pmatrix}$$

if and only if it is a sudoku matrix in the sense of Definition 15.34.

PROOF. This follows from the fact that commutation with Σ means that the matrix is circulant. Thus, we obtain the sudoku relations from Definition 15.34. □

Now let Z_s be the oriented cycle with s vertices, and consider the graph NZ_s consisting of N disjoint copies of it. Observe that, with a suitable labeling of the vertices, the adjacency matrix of this graph is the above matrix Σ. We obtain from this:

THEOREM 15.37. *We have the following results:*

(1) *H_N^s is the symmetry group of NZ_s.*
(2) *H_N^{s+} is the quantum symmetry group of NZ_s.*

PROOF. This is something elementary, the idea being as follows:

(1) This follows from definitions.

(2) This follows from Theorem 15.35 and Proposition 15.36, because the algebra $C(H_N^{s+})$ is the quotient of the algebra $C(S_{sN}^+)$ by the relations making the fundamental corepresentation commute with the adjacency matrix of NZ_s. □

Next in line, we must talk about wreath products. We have here:

THEOREM 15.38. *We have the following results:*

(1) $H_N^s = \mathbb{Z}_s \wr S_N$.
(2) $H_N^{s+} = \mathbb{Z}_s \wr_* S_N^+$.

PROOF. This follows from the following formulae, valid for any connected graph X, and explained before, in chapter 5, applied to the graph Z_s:

$$G(NX) = G(X) \wr S_N \quad , \quad G^+(NX) = G^+(X) \wr_* S_N^+$$

Alternatively, (1) follows from definitions, and (2) can be proved directly, by constructing a pair of inverse morphisms. For details here, we refer to [9]. □

Regarding now the easiness property of H_N^s, H_N^{s+}, we already know that this happens at $s = 1, 2$. The point is that this happens at $s = \infty$ too, the result being as follows:

THEOREM 15.39. *The quantum groups K_N, K_N^+ are easy, the corresponding categories*

$$\mathcal{P}_{even} \subset P \quad , \quad \mathcal{NC}_{even} \subset NC$$

consisting of the partitions satisfying $\#\circ = \#\bullet$, as a weighted equality, in each block.

PROOF. This is something which is routine, along the lines of the proof of Theorem 15.29, and for details here, we refer for instancd to [9]. □

More generally now, we have the following result:

THEOREM 15.40. *The quantum groups H_N^s, H_N^{s+} are easy, the corresponding categories*

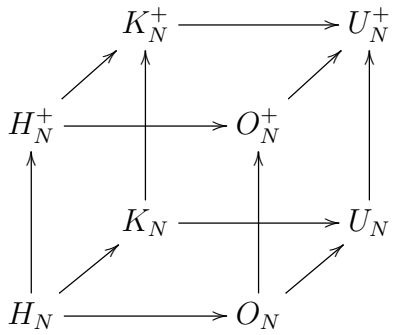
$$P^s \subset P \quad , \quad NC^s \subset NC$$

consisting of partitions satisfying $\#\circ = \#\bullet\,(s)$, as a weighted sum, in each block.

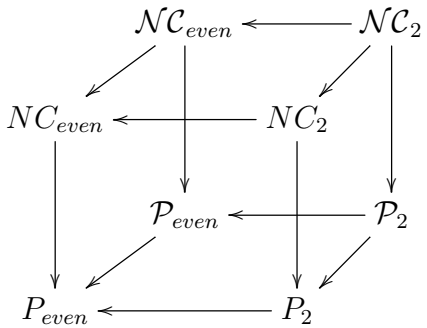
PROOF. Observe that the result holds at $s = 1$, trivially, then at $s = 2$ as well, where our condition is equivalent to $\#\circ = \#\bullet\,(2)$ in each block, as found in Theorem 15.29, and finally at $s = \infty$ too, as explained in Theorem 15.39. In general, this follows as in the case of H_N, H_N^+, by using the one-block partition in $P(s, s)$. □

Good news, we can now formulate a nice and conceptual result, as follows:

THEOREM 15.41. *We have quantum rotation and reflection groups, as follows,*



which are all easy, the corresponding categories of partitions being as follows,



with on top, the symbol NC standing everywhere for noncrossing partitions.

PROOF. This follows indeed by putting together all the above results. □

In order to discuss now probabilistic aspects, we will need:

DEFINITION 15.42. *The Bessel and free Bessel laws, depending on parameters $s \in \mathbb{N} \cup \{\infty\}$ and $t > 0$, are the following compound Poisson and free Poisson laws,*

$$b_t^s = p_{t\varepsilon_s} \quad , \quad \beta_t^s = \pi_{t\varepsilon_s}$$

with ε_s being the uniform measure on the s-th roots of unity. In particular:

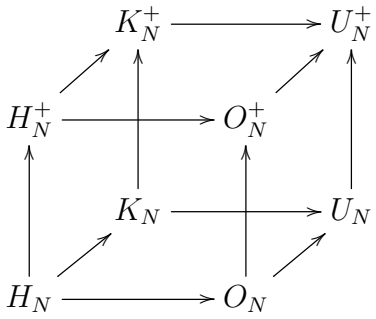
(1) *At $s = 1$ we recover the Poisson laws p_t, π_t.*
(2) *At $s = 2$ we have the real Bessel laws b_t, β_t.*
(3) *At $s = \infty$ we have the complex Bessel laws $B_t, \mathfrak{B}_t$.*

Here the terminology comes from the fact that the density of the measure b_t from (2) is a Bessel function of the first kind, the formula being as follows:

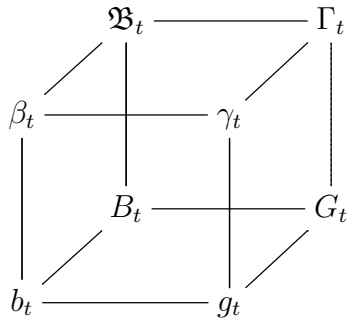
$$b_t = e^{-t} \sum_{r=-\infty}^{\infty} \delta_r \sum_{p=0}^{\infty} \frac{(t/2)^{|r|+2p}}{(|r|+p)!p!}$$

Good news, with the above general theory in hand, we can now formulate our truncated character results for the main examples of easy quantum groups, as follows:

THEOREM 15.43. *For the main quantum rotation and reflection groups,*

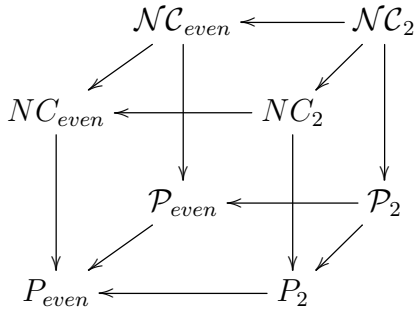


the corresponding truncated characters follow with $N \to \infty$ the laws



which are the main limiting laws in classical and free probability.

PROOF. We know from Theorem 15.41 that the above quantum groups are all easy, coming from the following categories of partitions:



(1) At $t = 1$, we can use the following general formula, coming from Peter-Weyl:

$$\lim_{N\to\infty} \int_{G_N} \chi^k = |D(k)|$$

But this gives the laws in the statement, via some standard calculus.

(2) In order to compute now the asymptotic laws of truncated characters, at any $t > 0$, we can use the following general moment formula, as in the classical case:

$$\int_G (u_{11} + \ldots + u_{ss})^k = Tr(W_{kN} G_{ks})$$

To be more precise, what happens is that in each of the cases under consideration, the Gram matrix is asymptotically diagonal, and so the Weingarten matrix is asymptotically diagonal too. Thus, in the limit we obtain the following moment formula:

$$\lim_{N\to\infty} \int_{G_N} \chi_t^k = \sum_{\pi \in D(k)} t^{|\pi|}$$

But this gives the laws in the statement, via some standard calculus. □

15e. Exercises

Exercises:

Exercise 15.44.

Exercise 15.45.

Exercise 15.46.

Exercise 15.47.

Exercise 15.48.

Exercise 15.49.

Exercise 15.50.

Exercise 15.51.

Bonus exercise.

CHAPTER 16

Planar algebras

16a. Planar algebras

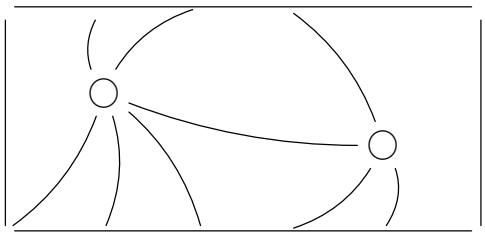
The Temperley-Lieb category that we met before is more than a category, it is a planar algebra. In order to explain this fact, which will be of key importance in what follows, following Jones [60], let us start with the following general definition:

DEFINITION 16.1. *The planar algebras are defined as follows:*

(1) *We consider rectangles in the plane, with the sides parallel to the coordinate axes, and taken up to planar isotopy, and we call such rectangles boxes.*
(2) *A labeled box is a box with $2n$ marked points on its boundary, n on its upper side, and n on its lower side, for some integer $n \in \mathbb{N}$.*
(3) *A tangle is labeled box, containing a number of labeled boxes, with all marked points, on the big and small boxes, being connected by noncrossing strings.*
(4) *A planar algebra is a sequence of finite dimensional vector spaces $P = (P_n)$, together with linear maps $P_{n_1} \otimes \ldots \otimes P_{n_k} \to P_n$, one for each tangle, such that the gluing of tangles corresponds to the composition of linear maps.*

In this definition we are using rectangles, but everything being up to isotopy, we could have used instead circles with marked points, as in [60]. Our choice for using rectangles comes from the main examples that we have in mind, to be discussed below, where the planar algebra structure is best viewed by using rectangles, as above.

This being said, when convenient, we agree to use circles with marked points for the outer box, or for the inner boxes, or for both, with the convention that the marked point is the lower left corner of the rectangle. Here is a planar tangle, drawn in this way, with the marked points on both circles being by definition those at South-West:



And, exercise for you to see what this tangle becomes, in rectangular notation.

Getting back now to what Definition 16.1 says, in relation with the tangle pictured above, that tangle has two inner boxes, having respectively $2 \times 2 = 4$ and $2 \times 3 = 6$ marked points on their boundaries, and the outer box has $2 \times 4 = 8$ marked points on its boundary. Thus, that tangle π must produce a linear map as follows:

$$T_\pi : P_2 \otimes P_3 \to P_4$$

You get the point, I hope, Definition 16.1 is something very useful in the context of algebra, in order to index various possible operations on a sequence of finite dimensional vector spaces $P = (P_n)$, by diagrams as above. Of course, all this remains very vague for the moment, but we will see many examples and illustrations, in what follows.

Getting now to the essence of Definition 16.1, that lies in the axiom (4) there, compatibility of the gluing of the tangles with the composition of the multilinear maps. We will comment on this later, once we will have some examples of planar algebras. In the meantime, let us mention that it is possible to be more abstract here, by talking about the planar operad, and planar algebras as modules over this operad. But again, we will comment on this later, once we will have some examples of planar algebras.

Finally, let us mention now that Definition 16.1 is something quite simplified. As explained in [60], in order for subfactors to produce planar algebras and vice versa, there are quite a number of supplementary axioms that must be added. More on this later.

But probably too much talking, let us see some illustrations for this. As a first, very basic example of a planar algebra, we have the Temperley-Lieb algebra:

THEOREM 16.2. *The Temperley-Lieb algebra TL_N, viewed as graded algebra*

$$TL_N = (TL_N(n))_{n\in\mathbb{N}}$$

is a planar algebra, with the corresponding linear maps associated to the planar tangles

$$TL_N(n_1) \otimes \ldots \otimes TL_N(n_k) \to TL_N(n)$$

appearing by putting the various $TL_N(n_i)$ diagrams into the small boxes of the given tangle, which produces a $TL_N(n)$ diagram.

PROOF. This is something trivial, which follows from definitions:

(1) Assume indeed that we are given a planar tangle π, as in Definition 16.1, consisting of a box having $2n$ marked points on its boundary, and containing k small boxes, having respectively $2n_1, \ldots, 2n_k$ marked points on their boundaries, and then a total of $n + \Sigma n_i$ noncrossing strings, connecting the various $2n + \Sigma 2n_i$ marked points.

(2) We want to associate to this tangle π a linear map as follows:

$$T_\pi : TL_N(n_1) \otimes \ldots \otimes TL_N(n_k) \to TL_N(n)$$

For this purpose, by linearity, it is enough to construct elements as follows, for any choice of Temperley-Lieb diagrams $\sigma_i \in TL_N(n_i)$, with $i = 1, \ldots, k$:

$$T_\pi(\sigma_1 \otimes \ldots \otimes \sigma_k) \in TL_N(n)$$

(3) But constructing such an element is obvious, just by putting the various diagrams $\sigma_i \in TL_N(n_i)$ into the small boxes the given tangle π. Indeed, this procedure produces a certain diagram in $TL_N(n)$, that we can call $T_\pi(\sigma_1 \otimes \ldots \otimes \sigma_k)$, as above.

(4) Finally, we have to check that everything is well-defined up to planar isotopy, and that the gluing of tangles corresponds to the composition of linear maps. But both these checks are trivial, coming from the definition of TL_N, and we are done. □

As a conclusion to all this, $P = TL_N$ is indeed a planar algebra, but of somewhat "trivial" type, with the triviality coming from the fact that, in this case, the elements of P are planar diagrams themselves, and so the planar structure appears trivially.

The Temperley-Lieb planar algebra TL_N is however an important planar algebra, because it is the "smallest" one, appearing inside the planar algebra of any subfactor. But more on this later, when talking about planar algebras and subfactors.

Moving ahead now, here is our second basic example of a planar algebra, which is also "trivial" in the above sense, with the elements of the planar algebra being planar diagrams themselves, but which appears in a bit more complicated way:

THEOREM 16.3. *The Fuss-Catalan algebra $FC_{N,M}$, obtained by coloring the Temperley-Lieb diagrams with black and white colors, clockwise, as follows,*

$$\circ\bullet\bullet\circ\circ\bullet\bullet\circ \ldots\ldots\ldots \circ\bullet\bullet\circ$$

and keeping those diagrams whose strings connect either $\circ - \circ$ or $\bullet - \bullet$, is a planar algebra, with again the corresponding linear maps associated to the planar tangles

$$FC_{N,M}(n_1) \otimes \ldots \otimes FC_{N,M}(n_k) \to FC_{N,M}(n)$$

appearing by putting the various $FC_{N,M}(n_i)$ diagrams into the small boxes of the given tangle, which produces a $FC_{N,M}(n)$ diagram.

PROOF. The proof here is nearly identical to the proof of Theorem 16.2, with the only change appearing at the level of the colors. To be more precise:

(1) Forgetting about upper and lower sequences of points, which must be joined by strings, a Temperley-Lieb diagram can be thought of as being a collection of strings, say black strings, which compose in the obvious way, with the rule that the value of the circle, which is now a black circle, is N. And it is this obvious composition rule that gives the planar algebra structure, as explained in the proof of Theorem 16.2.

(2) Similarly, forgetting about points, a Fuss-Catalan diagram can be thought of as being a collection of strings, which come now in two colors, black and white. These Fuss-Catalan diagrams compose then in the obvious way, with the rule that the value of the black circle is N, and the value of the white circle is M. And it is this obvious composition rule that gives the planar algebra structure, as before for TL_N. □

Even more generally now, we can talk about the multicolored Fuss-Catalan algebra, generalizing both the Temperley-Lieb and Fuss-Catalan algebras, as follows:

THEOREM 16.4. *The multicolored Fuss-Catalan algebra $FC_{N_1,\ldots,N_s}$, obtained by coloring the Temperley-Lieb diagrams with s colors, clockwise, as follows,*

$$1\ldots ss\ldots 11\ldots ss\ldots 1\ldots\ldots\ldots 1\ldots ss\ldots 1$$

and keeping those diagrams whose strings connect $i-i$, is a planar algebra, with again the corresponding linear maps associated to the planar tangles

$$FC_{N_1,\ldots,N_s}(n_1)\otimes\ldots\otimes FC_{N_1,\ldots,N_s}(n_k)\to FC_{N_1,\ldots,N_s}(n)$$

appearing by putting the various $FC_{N_1,\ldots,N_s}(n_i)$ diagrams into the small boxes of the given tangle, which produces a $FC_{N_1,\ldots,N_s}(n)$ diagram.

PROOF. This is a straightforward remake of Theorems 16.2 and 16.3, which correspond respectively to the cases $s=1,2$, with the only thing that must be added being the fact that the values of the circles of colors $1,\ldots,s$ are respectively the numbers $N_1,\ldots,N_s$. And with this we are led, as before, to the conclusions in the statement. □

Getting back now to generalities, and to Definition 16.1 as stated, that of a general planar algebra, we have so far a few illustrations for it, which, while all important, are all "trivial", with the planar structure simply coming from the fact that, in all the above cases, the elements of the planar algebra are planar diagrams themselves.

In general, the planar algebras can be more complicated than this, and we will see some further examples in a moment. However, the idea is very simple, namely:

PRINCIPLE 16.5. *The elements of a planar algebra are not necessarily diagrams, but they behave like diagrams.*

And important principle this is. If there is something to be known, in order to understand planar algebras, and the whole quantum algebra theory based on them, it is this principle. But, do we really understand this principle? Not yet, because as already mentioned, our examples so far of planar algebras, namely Temperley-Lieb and Fuss-Catalan, are both "trivial", with the elements of the planar algebra being themselves diagrams.

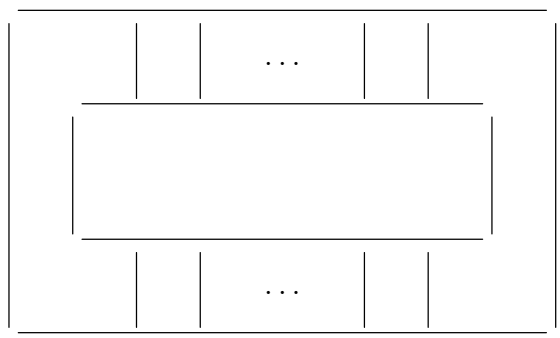
Nevermind. We will get to understand this principle, via more examples, and via some theory too. And, once this chapter read, Principle 16.5 will be understood.

16b. Basic tangles

What is next? Instead of looking right away for further examples, which can be substantially more complicated than Temperley-Lieb and Fuss-Catalan, let us enjoy what we have. To be more precise, with these two basic examples in hand, Temperley-Lieb and Fuss-Catalan, let us try to say more about the arbitrary planar algebras, as in Definition 16.1, with a bit of inspiration from what happens for these examples.

To start with, we have a number of remarkable planar tangles, whose algebraic action must be well understood, before anything. The first basic tangle is as follows:

EXAMPLE 16.6. *The identity tangle is the following tangle, with $2n$ outer legs,*

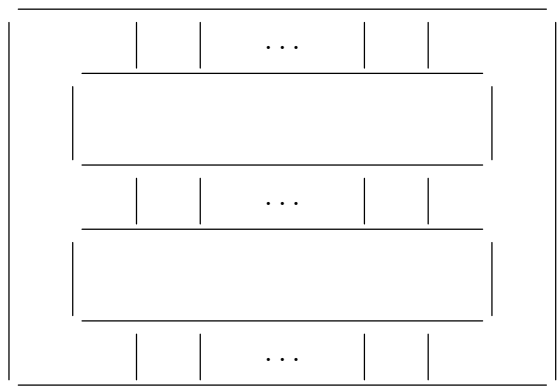


and this tangle must act via the identity, $T_\pi(x) = x$, for any $x \in P_n$.

To be more precise here, consider the tangle in the statement, π. Since applying this tangle obviously does nothing, this tangle must act via the identity map, as stated.

As a more interesting example now, bringing an associative algebra structure to each of the vector spaces P_n that our planar algebra is made of, we have:

EXAMPLE 16.7. *The multiplication tangle is as follows, with $2n$ outer legs,*



and this must implement a multiplication map, $T_\pi(x \otimes y) = xy$, for any $x, y \in P_n$.

Again, this is something quite self-explanatory, the idea being that the tangle in the statement, or rather its action on P_n, must be an associative multiplication.

Along the same lines, bringing more basic structure to our sequence of vector spaces $P = (P_n)$, which are now a sequence of associative algebras $P = (P_n)$, we have:

EXAMPLE 16.8. *The inclusion tangle is as follows, with $2n + 2$ outer legs,*

and this tangle must act via an inclusion, $T_\pi(x) = x$, for any $x \in P_n$.

Again, this is something quite self-explanatory, the idea being that the tangle in the statement, or rather its action $P_n \to P_{n+1}$, must be an inclusion of algebras.

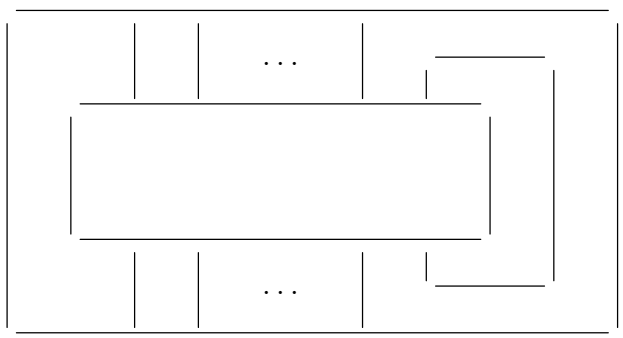
As a conclusion to all this, we already have some interesting structure on our planar algebras, getting well beyond what is totally obvious from Definition 16.1, as follows:

CONCLUSION 16.9. *Any planar algebra $P = (P_n)$ is naturally a graded associative algebra over the complex numbers, with multiplication and inclusion maps coming from the action of the multiplication and inclusion tangles, pictured above.*

Which looks quite interesting, especially in view of the fact that, due to this coming from the study of some trivial tangles, this can only be the tip of the iceberg. So, let us explore some more what the basic tangles are, and what can be done with them.

Coming first in our second batch of examples, we have:

EXAMPLE 16.10. *The expectation tangle is as follows, with $2n$ outer legs,*

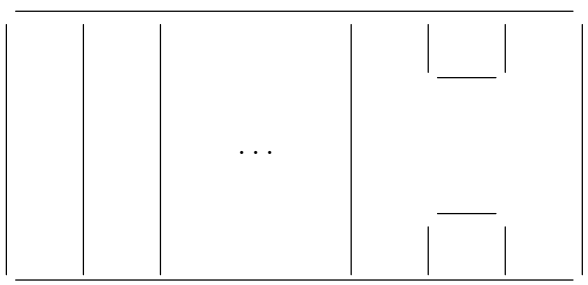


and this tangle must act via an expectation, $T_\pi : P_{n+1} \to P_n$.

To be more precise, this is something a bit more advanced, the idea here being that the linear map $T_\pi : P_{n+1} \to P_n$ associated to the above expectation tangle must be a section, and bimodule map, with respect to the canonical inclusion of algebras $P_n \subset P_{n+1}$, that we constructed before. We will be back to this, with more details, later.

Along the same lines, again at the level of more specialized tangles, we have:

EXAMPLE 16.11. *The Jones projection tangle is as follows, with $2n$ outer legs,*



and this tangle corresponds to a rescaled projection $T_\pi \in P_n$.

Again, this is something quite self-explanatory, the idea being that, with no inner box present, the Jones projection tangle must simply correspond to a certain element $T_\pi \in P_n$. But this element must be an idempotent, up to a N factor, as said above.

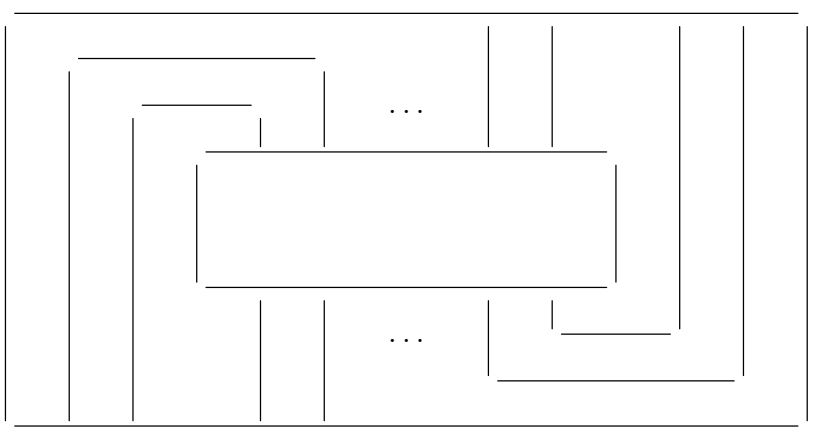
Very good all this, so let us upgrade Conclusion 16.9, as follows:

CONCLUSION 16.12 (upgrade). *Any planar algebra $P = (P_n)$ is naturally a graded associative algebra, via the action of the multiplication and inclusion tangles, and in addition we have, a bit as for the Temperley-Lieb algebra, expectations and Jones projections.*

As already mentioned in the above, in what concerns the last part, regarding the expectations and the Jones projections, this is something a bit more specialized, and definitely in need of more discussion. We will come back to this, a bit later.

Moving ahead, let us discuss now a third batch of basic planar tangles, that we will heavily use as well in what follows. First we have the rotation, which is as follows:

EXAMPLE 16.13. *The rotation tangle is as follows, with* $2n$ *outer legs,*

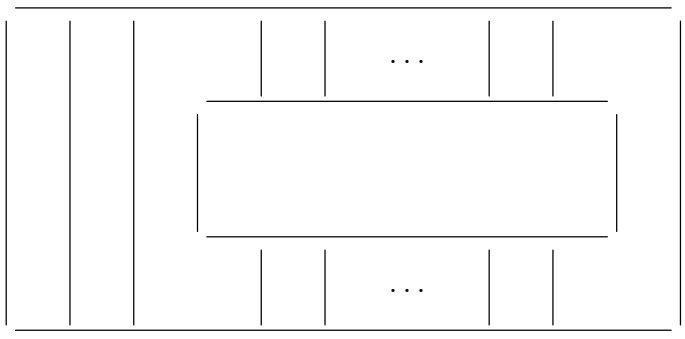


and this tangle must act via a rotation $T_\pi : P_n \to P_n$.

Again, this is something quite self-explanatory, the idea being that the linear map $T_\pi : P_n \to P_n$ associated to the above rotation tangle must produce the identity, when raised to the power n, a bit like the usual rotation in the plane, of angle $2\pi/n$, does.

As a last basic tangle, we have the shift, which is constructed as follows:

EXAMPLE 16.14. *The shift tangle is as follows, with* $2n + 2$ *outer legs,*



and this tangle must act via a shift, $T_\pi : P_n \to P_{n+2}$.

Again, this is something quite self-explanatory, and with the remark of course that the shift is not to be confused with the double inclusion map $P_n \to P_{n+2}$. We will get back to this, shift and its properties, with more details, later in this chapter.

As a grand conclusion now to what we did so far, we have:

CONCLUSION 16.15 (final upgrade). *Any planar algebra $P = (P_n)$ is naturally a graded associative algebra, and in addition we have, a bit as for the Temperley-Lieb algebra, or for the Fuss-Catalan one, expectations, Jones projections, rotations and shifts.*

Which is good knowledge, and we will be back to this, with further details, later on. In any case, we can see here some good evidence for what we said in Principle 16.5, namely that the elements of a planar algebra are not necessarily diagrams, but behave like diagrams. And, more on this on several occassions, in what follows.

Getting back now to theory, we have the following remarkable result, which is something that we will heavily use, in what follows, for all sorts of purposes:

THEOREM 16.16. *The following tangles generate the set of all tangles, via gluing:*

(1) *Multiplications.*
(2) *Inclusions.*
(3) *Expectations.*
(4) *Jones projections.*
(5) *Rotations, or shifts.*

PROOF. This is something well-known and elementary, obtained by "chopping" the various planar tangles into small pieces, as in the above list:

(1) To start with, in what regards the list itself, this is the one coming from the above examples, with the identities, which bring nothing to our generation problem, removed.

(2) As a subtlety now, at the end we have a choice, between the rotation and the shift. This is something quite important for the applications, which come in two flavors.

(3) As for the proof, as indicated above, both the results, the one with rotations, and the one with shifts, follow by chopping the tangles, in the obvious way. See [60]. □

There are many more things that can be said, along these lines, that is, generalities and basic algebra, in relation with Definition 16.1. We will be back to this later.

16c. Tensor and spin

Let us discuss now some further examples of planar algebras, which are of less trivial nature than TL_N and $FC_{N,M}$, and are of particular interest in relation with algebra and topology. These are the tensor and spin planar algebras $\mathcal{T}_N, \mathcal{S}_N$. Let us start with:

DEFINITION 16.17. *The tensor planar algebra $\mathcal{T}_N$ is the sequence of vector spaces*

$$P_k = M_N(\mathbb{C})^{\otimes k}$$

with the multilinear maps $T_\pi : P_{k_1} \otimes \ldots \otimes P_{k_r} \to P_k$ being given by the formula

$$T_\pi(e_{i_1} \otimes \ldots \otimes e_{i_r}) = \sum_j \delta_\pi(i_1, \ldots, i_r : j) e_j$$

with the Kronecker symbols δ_π being 1 if the indices fit, and being 0 otherwise.

In other words, we put the indices of the basic tensors on the marked points of the small boxes, in the obvious way, and the coefficients of the output tensor are then given by Kronecker symbols, $\delta_\pi \in \{0, 1\}$, which are themselves defined as follows:

– $\delta_\pi = 1$ when all strings join pairs of equal indices.

– $\delta_\pi = 0$ otherwise.

The fact that we have indeed a planar algebra is something elementary, and for full details here, we refer to Jones' paper [60]. As illustrations for all this, we have:

EXAMPLE 16.18. *Identity.*

We recall that the identity 1_k is the (k, k)-tangle having vertical strings only. The solutions of $\delta_{1_k}(x, y) = 1$ being the pairs of the form (x, x), this tangle acts as follows:

$$1_k \begin{pmatrix} j_1 & \ldots & j_k \\ i_1 & \ldots & i_k \end{pmatrix} = \begin{pmatrix} j_1 & \ldots & j_k \\ i_1 & \ldots & i_k \end{pmatrix}$$

But this action is the identity, as it should.

EXAMPLE 16.19. *Multiplication.*

The multiplication M_k is the (k, k, k)-tangle having 2 input boxes, one on top of the other, and vertical strings only. This tangle acts in the following way:

$$M_k\left(\begin{pmatrix} j_1 & \ldots & j_k \\ i_1 & \ldots & i_k \end{pmatrix} \otimes \begin{pmatrix} l_1 & \ldots & l_k \\ m_1 & \ldots & m_k \end{pmatrix}\right) = \delta_{j_1 m_1} \ldots \delta_{j_k m_k} \begin{pmatrix} l_1 & \ldots & l_k \\ i_1 & \ldots & i_k \end{pmatrix}$$

Again, this action is the multiplication, as it should.

EXAMPLE 16.20. *Inclusion.*

The inclusion I_k is the $(k, k+1)$-tangle which looks like 1_k, but has one more vertical string, at right of the input box. Given x, the solutions of $\delta_{I_k}(x, y) = 1$ are the elements y obtained from x by adding to the right a vector of the form $\binom{l}{l}$, and so:

$$I_k \begin{pmatrix} j_1 & \ldots & j_k \\ i_1 & \ldots & i_k \end{pmatrix} = \sum_l \begin{pmatrix} j_1 & \ldots & j_k & l \\ i_1 & \ldots & i_k & l \end{pmatrix}$$

Once again, what we have here is what we can expect from an inclusion.

EXAMPLE 16.21. *Expectation.*

The expectation U_k is the $(k+1,k)$-tangle which looks like 1_k, but has one more string, connecting the extra 2 input points, both at right of the input box:

$$U_k\begin{pmatrix} j_1 & \ldots & j_k & j_{k+1}\\ i_1 & \ldots & i_k & i_{k+1}\end{pmatrix}=\delta_{i_{k+1}j_{k+1}}\begin{pmatrix} j_1 & \ldots & j_k\\ i_1 & \ldots & i_k\end{pmatrix}$$

This map satisfies then the usual requirements for an expectation.

EXAMPLE 16.22. *Jones projection.*

The Jones projection E_k is a $(0,k+2)$-tangle, having no input box. There are k vertical strings joining the first k upper points to the first k lower points, counting from left to right. The remaining upper 2 points are connected by a semicircle, and the remaining lower 2 points are also connected by a semicircle. We have:

$$E_k(1)=\sum_{ijl}\begin{pmatrix} i_1 & \ldots & i_k & j & j\\ i_1 & \ldots & i_k & l & l\end{pmatrix}$$

The elements $e_k=N^{-1}E_k(1)$ are then projections, and define a representation of the infinite Temperley-Lieb algebra of index N inside the inductive limit algebra $\mathcal{S}_N$.

EXAMPLE 16.23. *Rotation.*

The rotation R_k is the (k,k)-tangle which looks like 1_k, but the first 2 input points are connected to the last 2 output points, and the same happens at right:

$$R_k=\begin{array}{c}\Cap\,|\,|\,|\,\|\\ \|\qquad\quad\|\\ \|\,|\,|\,|\,\Cup\end{array}$$

The action of R_k on the standard basis is by rotation of the indices, as follows:

$$R_k(e_{i_1i_2\ldots i_k})=e_{i_2\ldots i_ki_1}$$

Thus, what we have indeed is a rotation map.

EXAMPLE 16.24. *Shift.*

As for the shift S_k, this is the $(k,k+2)$-tangle which looks like 1_k, but has two more vertical strings, at left of the input box. This tangle acts as follows:

$$S_k\begin{pmatrix} j_1 & \ldots & j_k\\ i_1 & \ldots & i_k\end{pmatrix}=\sum_{lm}\begin{pmatrix} l & m & j_1 & \ldots & j_k\\ l & m & i_1 & \ldots & i_k\end{pmatrix}$$

Observe that S_k is an inclusion of algebras, which is different from $I_{k+1}I_k$.

Finally, in order for our discussion to be complete, we must talk as well about the $*$-structure of the spin planar algebra. Once again this is constructed as in the easy quantum group calculus, by turning upside-down the diagrams, as follows:

$$\begin{pmatrix} j_1 & \ldots & j_k \\ i_1 & \ldots & i_k \end{pmatrix}^* = \begin{pmatrix} i_1 & \ldots & i_k \\ j_1 & \ldots & j_k \end{pmatrix}$$

As before, we refer to Jones' paper [60] for more on all this.

Let us discuss now a second planar algebra of the same type, which is important as well for various reasons, namely the spin planar algebra $\mathcal{S}_N$. This planar algebra appears somewhat as a "square root" of the tensor planar algebra $\mathcal{T}_N$, and its construction is quite similar, but by using this time the algebra $\mathbb{C}^N$ instead of the algebra $M_N(\mathbb{C})$.

There is one subtlety, however, coming from the fact that the general planar algebra formalism, from Definition 16.1, requires the tensors to have even length. Note that this was automatic for the tensor planar $\mathcal{T}_N$, where the tensors of $M_N(\mathbb{C})$ have length 2. In the case of the spin planar algebra $\mathcal{S}_N$, we want the vector spaces to be:

$$P_k = (\mathbb{C}^N)^{\otimes k}$$

Thus, we must double the indices of the tensors, in the following way:

DEFINITION 16.25. *We write the standard basis of $(\mathbb{C}^N)^{\otimes k}$ in $2 \times k$ matrix form,*

$$e_{i_1 \ldots i_k} = \begin{pmatrix} i_1 & i_1 & i_2 & i_2 & i_3 & \ldots & \ldots \\ i_k & i_k & i_{k-1} & \ldots & \ldots & \ldots & \ldots \end{pmatrix}$$

by duplicating the indices, and then writing them clockwise, starting from top left.

Now with this convention in hand for the tensors, we can formulate the construction of the spin planar algebra $\mathcal{S}_N$, also from [60], as follows:

DEFINITION 16.26. *The spin planar algebra $\mathcal{S}_N$ is the sequence of vector spaces*

$$P_k = (\mathbb{C}^N)^{\otimes k}$$

written as above, with the multiplinear maps $T_\pi : P_{k_1} \otimes \ldots \otimes P_{k_r} \to P_k$ being given by

$$T_\pi(e_{i_1} \otimes \ldots \otimes e_{i_r}) = \sum_j \delta_\pi(i_1, \ldots, i_r : j) e_j$$

with the Kronecker symbols δ_π being 1 if the indices fit, and being 0 otherwise.

In other words, we are using exactly the same construction as for the tensor planar algebra $\mathcal{T}_N$, but with $M_N(\mathbb{C})$ replaced by $\mathbb{C}^N$, with the indices doubled, as in Definition 16.25. As before with the tensor planar algebra $\mathcal{T}_N$, the fact that the spin planar algebra $\mathcal{S}_N$ is indeed a planar algebra is something rather trivial, coming from definitions.

Observe however that, unlike our previous planar algebras TL_N and $FC_{N,M}$, which were "trivial" planar algebras, their elements being planar diagrams themselves, the planar algebras $\mathcal{T}_N$ and $\mathcal{S}_N$ are not trivial, their elements being not exactly planar diagrams.

Let us also mention that the tensor and spin planar algebras $\mathcal{T}_N$ and $\mathcal{S}_N$ are important for a number of reasons, in the context of group theory, algebra and topology, to be discussed later, at the end of the present chapter, and later on too.

Getting back now to the planar algebra structure of $\mathcal{T}_N$ and $\mathcal{S}_N$, which is something quite fundamental, worth being well understood, let us have here some more discussion. Generally speaking, the planar calculus for tensors is quite simple, and does not really require diagrams. Indeed, it suffices to imagine that the way various indices appear, travel around and dissapear is by following some obvious strings connecting them.

Here are some illustrations for this general principle, for the spin planar algebra $\mathcal{S}_N$, in relation with the various basic planar tangles, that we know well:

EXAMPLE 16.27. *Identity.*

The identity 1_k is the (k,k)-tangle having vertical strings only. The solutions of $\delta_{1_k}(x,y)=1$ being the pairs of the form (x,x), this tangle 1_k acts as follows:

$$1_k\begin{pmatrix}j_1&\cdots&j_k\\ i_1&\cdots&i_k\end{pmatrix}=\begin{pmatrix}j_1&\cdots&j_k\\ i_1&\cdots&i_k\end{pmatrix}$$

But this action is the identity, as it should.

EXAMPLE 16.28. *Multiplication.*

The multiplication M_k is the (k,k,k)-tangle having 2 input boxes, one on top of the other, and vertical strings only. This tangle acts in the following way:

$$M_k\left(\begin{pmatrix}j_1&\cdots&j_k\\ i_1&\cdots&i_k\end{pmatrix}\otimes\begin{pmatrix}l_1&\cdots&l_k\\ m_1&\cdots&m_k\end{pmatrix}\right)=\delta_{j_1m_1}\ldots\delta_{j_km_k}\begin{pmatrix}l_1&\cdots&l_k\\ i_1&\cdots&i_k\end{pmatrix}$$

Again, this action is the multiplication, as it should. Observe that, in the present context of the spin planar algebra, this multiplication is commutative.

EXAMPLE 16.29. *Inclusion.*

The inclusion I_k is the $(k,k+1)$-tangle which looks like 1_k, but has one more vertical string, at right of the input box. Given x, the solutions of $\delta_{I_k}(x,y)=1$ are the elements y obtained from x by adding to the right a vector of the form $\binom{l}{l}$, and so:

$$I_k\begin{pmatrix}j_1&\cdots&j_k\\ i_1&\cdots&i_k\end{pmatrix}=\sum_l\begin{pmatrix}j_1&\cdots&j_k&l\\ i_1&\cdots&i_k&l\end{pmatrix}$$

Once again, what we have here is what we can expect from an inclusion.

EXAMPLE 16.30. *Expectation.*

The expectation U_k is the $(k+1,k)$-tangle which looks like 1_k, but has one more string, connecting the extra 2 input points, both at right of the input box:

$$U_k\begin{pmatrix} j_1 & \ldots & j_k & j_{k+1}\\ i_1 & \ldots & i_k & i_{k+1}\end{pmatrix}=\delta_{i_{k+1}j_{k+1}}\begin{pmatrix} j_1 & \ldots & j_k\\ i_1 & \ldots & i_k\end{pmatrix}$$

This map satisfies then the usual requirements for an expectation.

EXAMPLE 16.31. *Jones projection.*

The Jones projection E_k is a $(0,k+2)$-tangle, having no input box. There are k vertical strings joining the first k upper points to the first k lower points, counting from left to right. The remaining upper 2 points are connected by a semicircle, and the remaining lower 2 points are also connected by a semicircle. We have:

$$E_k(1)=\sum_{ijl}\begin{pmatrix} i_1 & \ldots & i_k & j & j\\ i_1 & \ldots & i_k & l & l\end{pmatrix}$$

The elements $e_k=N^{-1}E_k(1)$ are then projections, and define a representation of the infinite Temperley-Lieb algebra of index N inside the inductive limit algebra $\mathcal{S}_N$.

EXAMPLE 16.32. *Rotation.*

The rotation R_k is the (k,k)-tangle which looks like 1_k, but the first 2 input points are connected to the last 2 output points, and the same happens at right:

$$R_k=\begin{array}{c}\cap\,|\,|\,|\,\|\\ \|\qquad\quad\|\\ \|\,|\,|\,|\,\cup\end{array}$$

The action of R_k on the standard basis is by rotation of the indices, as follows:

$$R_k(e_{i_1i_2\ldots i_k})=e_{i_2\ldots i_ki_1}$$

Thus, what we have indeed is a rotation map.

EXAMPLE 16.33. *Shift.*

As for the shift S_k, this is the $(k,k+2)$-tangle which looks like 1_k, but has two more vertical strings, at left of the input box. This tangle acts as follows:

$$S_k\begin{pmatrix} j_1 & \ldots & j_k\\ i_1 & \ldots & i_k\end{pmatrix}=\sum_{lm}\begin{pmatrix} l & m & j_1 & \ldots & j_k\\ l & m & i_1 & \ldots & i_k\end{pmatrix}$$

Observe that S_k is an inclusion of algebras, which is different from $I_{k+1}I_k$.

Finally, in order for our discussion to be complete, we must talk as well about the $*$-structure of the spin planar algebra. Once again this is constructed as in the easy quantum group calculus, by turning upside-down the diagrams, as follows:

$$\begin{pmatrix} j_1 & \ldots & j_k \\ i_1 & \ldots & i_k \end{pmatrix}^* = \begin{pmatrix} i_1 & \ldots & i_k \\ j_1 & \ldots & j_k \end{pmatrix}$$

As before, we refer to Jones' paper [60] for more on all this.

Getting back now to quantum groups, following [9], we have the following result:

THEOREM 16.34. *Given $G \subset S_N^+$, consider the tensor powers of the associated coaction map on $C(X)$, where $X = \{1, \ldots, N\}$, which are the folowing linear maps:*

$$\Phi^k : C(X^k) \to C(X^k) \otimes C(G)$$

$$e_{i_1 \ldots i_k} \to \sum_{j_1 \ldots j_k} e_{j_1 \ldots j_k} \otimes u_{j_1 i_1} \ldots u_{j_k i_k}$$

The fixed point spaces of these coactions, which are by definition the spaces

$$P_k = \left\{ x \in C(X^k) \middle| \Phi^k(x) = 1 \otimes x \right\}$$

are given by $P_k = Fix(u^{\otimes k})$, and form a subalgebra of the spin planar algebra $\mathcal{S}_N$.

PROOF. Since the map Φ is a coaction, its tensor powers Φ^k are coactions too, and at the level of fixed point algebras we have the following formula:

$$P_k = Fix(u^{\otimes k})$$

In order to prove now the planar algebra assertion, we will use Theorem 16.16. Consider the rotation R_k. Rotating, then applying Φ^k, and rotating backwards by R_k^{-1} is the same as applying Φ^k, then rotating each k-fold product of coefficients of Φ. Thus the elements obtained by rotating, then applying Φ^k, or by applying Φ^k, then rotating, differ by a sum of Dirac masses tensored with commutators in $A = C(G)$:

$$\Phi^k R_k(x) - (R_k \otimes id)\Phi^k(x) \in C(X^k) \otimes [A, A]$$

Now let $\int_A$ be the Haar functional of A, and consider the conditional expectation onto the fixed point algebra P_k, which is given by the following formula:

$$\phi_k = \left(id \otimes \int_A \right) \Phi^k$$

Since $\int_A$ is a trace, it vanishes on commutators. Thus R_k commutes with ϕ_k:

$$\phi_k R_k = R_k \phi_k$$

The commutation relation $\phi_k T = T\phi_l$ holds in fact for any (l,k)-tangle T. These tangles are called annular, and the proof is by verification on generators of the annular category. In particular we obtain, for any annular tangle T:

$$\phi_k T \phi_l = T\phi_l$$

We conclude from this that the annular category is contained in the suboperad $\mathcal{P}' \subset \mathcal{P}$ of the planar operad consisting of tangles T satisfying the following condition, where $\phi = (\phi_k)$, and where $i(.)$ is the number of input boxes:

$$\phi T \phi^{\otimes i(T)} = T\phi^{\otimes i(T)}$$

On the other hand the multiplicativity of Φ^k gives $M_k \in \mathcal{P}'$. Now since the planar operad $\mathcal{P}$ is generated by multiplications and annular tangles, it follows that we have $\mathcal{P}' = P$. Thus for any tangle T the corresponding multilinear map between spaces $P_k(X)$ restricts to a multilinear map between spaces P_k. In other words, the action of the planar operad $\mathcal{P}$ restricts to P, and makes it a subalgebra of $\mathcal{S}_N$, as claimed. □

As a second result now, also from [9], completing our study, we have:

THEOREM 16.35. *We have a bijection between quantum permutation groups and subalgebras of the spin planar algebra,*

$$(G \subset S_N^+) \quad \longleftrightarrow \quad (Q \subset \mathcal{S}_N)$$

given in one sense by the construction in Theorem 16.34, and in the other sense by a suitable modification of Tannakian duality.

PROOF. The idea is that this will follow by applying Tannakian duality to the annular category over Q. Let n, m be positive integers. To any element $T_{n+m} \in Q_{n+m}$ we associate a linear map $L_{nm}(T_{n+m}) : P_n(X) \to P_m(X)$ in the following way:

$$L_{nm}\begin{pmatrix} | & | & | \\ & T_{n+m} & \\ | & | & | \end{pmatrix} : \begin{pmatrix} | \\ a_n \\ | \end{pmatrix} \to \begin{pmatrix} | & | & \cap \\ & T_{n+m} & | \\ | & | & | & | \\ a_n & | & | & | \\ \cup & & | & | \end{pmatrix}$$

That is, we consider the planar $(n, n+m, m)$-tangle having an small input n-box, a big input $n+m$-box and an output m-box, with strings as on the picture of the right. This defines a certain multilinear map, as follows:

$$P_n(X) \otimes P_{n+m}(X) \to P_m(X)$$

If we put the element T_{n+m} in the big input box, we obtain in this way a certain linear map $P_n(X) \to P_m(X)$, that we call L_{nm}. With this convention, let us set:

$$Q_{nm} = \left\{ L_{nm}(T_{n+m}) : P_n(X) \to P_m(X) \middle| T_{n+m} \in Q_{n+m} \right\}$$

These spaces form a Tannakian category, so by [100] we obtain a Woronowicz algebra (A, u), such that the following equalities hold, for any m, n:

$$Hom(u^{\otimes m}, u^{\otimes n}) = Q_{mn}$$

We prove that u is a magic unitary. We have $Hom(1, u^{\otimes 2}) = Q_{02} = Q_2$, so the unit of Q_2 must be a fixed vector of $u^{\otimes 2}$. But $u^{\otimes 2}$ acts on the unit of Q_2 as follows:

$$\begin{aligned} u^{\otimes 2}(1) &= u^{\otimes 2}\left(\sum_i \begin{pmatrix} i & i \\ i & i \end{pmatrix}\right) \\ &= \sum_{ikl} \begin{pmatrix} k & k \\ l & l \end{pmatrix} \otimes u_{ki}u_{li} \\ &= \sum_{kl} \begin{pmatrix} k & k \\ l & l \end{pmatrix} \otimes (uu^t)_{kl} \end{aligned}$$

From $u^{\otimes 2}(1) = 1 \otimes 1$ ve get that uu^t is the identity matrix. Together with the unitarity of u, this gives the following formulae:

$$u^t = u^* = u^{-1}$$

Consider the Jones projection $E_1 \in Q_3$. After isotoping, $L_{21}(E_1)$ looks as follows:

$$L_{21}\left(\begin{smallmatrix} \cup \\ \cap \end{smallmatrix}\right) : \begin{pmatrix} | & | \\ i & i \\ j & j \\ | & | \end{pmatrix} \to \begin{pmatrix} | \\ i \ i \\ j \ j \ \supset \\ | \end{pmatrix} = \delta_{ij} \begin{pmatrix} | \\ i \\ i \\ | \end{pmatrix}$$

In other words, the linear map $M = L_{21}(E_1)$ is the multiplication $\delta_i \otimes \delta_j \to \delta_{ij}\delta_i$:

$$M \begin{pmatrix} i & i \\ j & j \end{pmatrix} = \delta_{ij} \begin{pmatrix} i \\ i \end{pmatrix}$$

In order to finish, consider the following element of $C(X) \otimes A$:

$$(M \otimes id)u^{\otimes 2}\left(\begin{pmatrix} i & i \\ j & j \end{pmatrix} \otimes 1\right) = \sum_k \begin{pmatrix} k \\ k \end{pmatrix} \delta_k \otimes u_{ki}u_{kj}$$

Since $M \in Q_{21} = Hom(u^{\otimes 2}, u)$, this equals the following element of $C(X) \otimes A$:

$$u(M \otimes id)\left(\begin{pmatrix} i & i \\ j & j \end{pmatrix} \otimes 1\right) = \sum_k \begin{pmatrix} k \\ k \end{pmatrix} \delta_k \otimes \delta_{ij}u_{ki}$$

Thus we have $u_{ki}u_{kj} = \delta_{ij}u_{ki}$ for any i, j, k, which shows that u is a magic unitary. Now if P is the planar algebra associated to u, we have $Hom(1, v^{\otimes n}) = P_n = Q_n$, as desired. As for the uniqueness, this is clear from the Peter-Weyl theory. □

Back now to our favorite business, graph symmetries, we have the following result:

THEOREM 16.36. *The planar algebra associated to $G^+(X)$ is equal to the planar algebra generated by d, viewed as a 2-box in the spin planar algebra $\mathcal{S}_N$, with $N = |X|$.*

PROOF. We recall from the above that any quantum permutation group $G \subset S_N^+$ produces a subalgebra $P \subset \mathcal{S}_N$ of the spin planar algebra, given by:

$$P_k = Fix(u^{\otimes k})$$

In our case, the idea is that $G = G^+(X)$ comes via the relation $d \in End(u)$, but we can view this relation, via Frobenius duality, as a relation of the following type:

$$\xi_d \in Fix(u^{\otimes 2})$$

Indeed, let us view the adjacency matrix $d \in M_N(0,1)$ as a 2-box in $\mathcal{S}_N$, by using the canonical identification between $M_N(\mathbb{C})$ and the algebra of 2-boxes $\mathcal{S}_N(2)$:

$$(d_{ij}) \leftrightarrow \sum_{ij} d_{ij} \begin{pmatrix} i & i \\ j & j \end{pmatrix}$$

Let P be the planar algebra associated to $G^+(X)$ and let Q be the planar algebra generated by d. The action of $u^{\otimes 2}$ on d viewed as a 2-box is given by:

$$u^{\otimes 2}\left(\sum_{ij} d_{ij} \begin{pmatrix} i & i \\ j & j \end{pmatrix}\right) = \sum_{ijkl} d_{ij} \begin{pmatrix} k & k \\ l & l \end{pmatrix} \otimes u_{ki}u_{lj} = \sum_{kl} \begin{pmatrix} k & k \\ l & l \end{pmatrix} \otimes (udu^t)_{kl}$$

Since v is a magic unitary commuting with d we have:

$$udu^t = duu^t = d$$

But this means that d, viewed as a 2-box, is in the algebra P_2 of fixed points of $u^{\otimes 2}$. Thus $Q \subset P$. As for $P \subset Q$, this follows from the duality found above. □

Generally speaking, the above material, when coupled with what we did in this book about graphs, leads us into the classification of the subalgebras of the spin planar algebra generated by a 2-box. But this can be regarded as a particular case of the Bisch-Jones question of classifying, in general, the planar algebras generated by a 2-box.

16d. Finite depth

Following Jones [57], let us discuss now the relation with subfactor theory. We have already met II_1 factors in chapter 13, but what about morphisms, between such factors. And here, a natural idea is that of looking at the inclusions of such factors:

DEFINITION 16.37. *A subfactor is an inclusion of II_1 factors $A_0 \subset A_1$.*

So, these will be the objects that we will be interested in, in what follows. Now given a subfactor $A_0 \subset A_1$, a first question is that of defining its index, measuring how big A_1 is, when compared to A_0. But this can be done as follows:

PROPOSITION 16.38. *Given an inclusion of* II_1 *factors* $A_0 \subset A_1$*, the number*

$$N = \frac{\dim_{A_0} H}{\dim_{A_1} H}$$

is independent of the ambient Hilbert space H*, and is called index.*

PROOF. This is standard, with the fact that the index as defined by the above formula is indeed independent of the ambient Hilbert space H coming from the various properties of the coupling constant, coming from the work of Murray and von Neumann. □

Following Jones [57], let us start with the following standard result:

PROPOSITION 16.39. *Associated to any subfactor* $A_0 \subset A_1$ *is the orthogonal projection*

$$e : L^2(A_1) \to L^2(A_0)$$

producing the conditional expectation $E : A_1 \to A_0$ *via the following formula:*

$$exe = E(x)e$$

This projection is called Jones projection for the subfactor $A_0 \subset A_1$*.*

PROOF. This is indeed somehing quite routine. □

Quite remarkably, the subfactor $A_0 \subset A_1$, as well as its commutant, can be recovered from the knowledge of this projection, in the following way:

PROPOSITION 16.40. *Given a subfactor* $A_0 \subset A_1$*, with Jones projection* e*, we have*

$$A_0 = A_1 \cap \{e\}' \quad , \quad A_0' = (A_1' \cap \{e\})''$$

as equalities of von Neumann algebras, acting on the space $L^2(A_1)$*.*

PROOF. The above two formulae both follow from $exe = E(x)e$, via some elementary computations, and for details here, we refer to Jones' paper [57]. □

We are now ready to formulate a key definition, as follows:

DEFINITION 16.41. *Associated to any subfactor* $A_0 \subset A_1$ *is the basic construction*

$$A_0 \subset_e A_1 \subset A_2$$

with $A_2 =< A_1, e >$ *being the algebra generated by* A_1 *and by the Jones projection*

$$e : L^2(A_1) \to L^2(A_0)$$

acting on the Hilbert space $L^2(A_1)$*.*

The idea now, following [57], will be that $A_1 \subset A_2$ appears as a kind of "reflection" of $A_0 \subset A_1$, and also that the basic construction can be iterated, and with all this leading to non-trivial results. To be more precise, following [57], we have:

THEOREM 16.42. *Associated to any subfactor $A_0 \subset A_1$ is the Jones tower*

$$A_0 \subset_{e_1} A_1 \subset_{e_2} A_2 \subset_{e_3} A_3 \subset \ldots\ldots$$

with the Jones projections having the following properties:

(1) $e_i^2 = e_i = e_i^*$.
(2) $e_i e_j = e_j e_i$ *for* $|i - j| \geq 2$.
(3) $e_i e_{i\pm 1} e_i = [A_1 : A_0]^{-1} e_i$.
(4) $tr(we_{n+1}) = [A_1 : A_0]^{-1} tr(w)$, *for any word* $w \in < e_1, \ldots, e_n >$.

PROOF. This follows indeed by doing some computations. See [57]. □

The relations found in Theorem 16.42 are in fact well-known, from the standard theory of the Temperley-Lieb algebra. This algebra, discovered by Temperley and Lieb in the context of statistical mechanics, has a very simple definition, as follows:

DEFINITION 16.43. *The Temperley-Lieb algebra of index $N \in [1, \infty)$ is defined as*

$$TL_N(k) = span(NC_2(k, k))$$

with product given by vertical concatenation, with the rule

$$\bigcirc = N$$

for the closed circles that might appear when concatenating.

As already mentioned, this algebra was discovered by Temperley and Lieb in the context of general statistical mechanics, and we refer here to the physics literature. In what concerns us, still following Jones' paper [57], we have the following result:

THEOREM 16.44. *Given a subfactor $A_0 \subset A_1$, construct its the Jones tower:*

$$A_0 \subset_{e_1} A_1 \subset_{e_2} A_2 \subset_{e_3} A_3 \subset \ldots\ldots$$

The rescaled sequence of projections $e_1, e_2, e_3, \ldots \in B(H)$ produces then a representation

$$TL_N \subset B(H)$$

of the Temperley-Lieb algebra of index $N = [A_1 : A_0]$.

PROOF. We know from Theorem 16.42 that the rescaled sequence of Jones projections $e_1, e_2, e_3, \ldots \in B(H)$ behaves algebrically exactly as the following TL_N diagrams:

$$\varepsilon_1 = \begin{smallmatrix} \cup \\ \cap \end{smallmatrix} \quad , \quad \varepsilon_2 = | \begin{smallmatrix} \cup \\ \cap \end{smallmatrix} \quad , \quad \varepsilon_3 = || \begin{smallmatrix} \cup \\ \cap \end{smallmatrix} \quad , \quad \ldots$$

But these diagrams generate TL_N, and so we have an embedding $TL_N \subset B(H)$, where H is the Hilbert space where our subfactor $A_0 \subset A_1$ lives, as claimed. □

As an interesting consequence of Theorem 16.44, somehow contradicting the "continuous geometry" philosophy that has being going on so far, in relation with the II_1 factors, we have the following surprising result, also from Jones' original paper [57]:

THEOREM 16.45. *The index of subfactors $A_0 \subset A_1$ is "quantized" in the $[1,4]$ range,*

$$N \in \left\{4\cos^2\left(\frac{\pi}{n}\right)\Big|n \geq 3\right\} \cup [4,\infty]$$

with the obstruction coming from the existence of the representation $TL_N \subset B(H)$.

PROOF. This comes from the basic construction, and more specifically from the combinatorics of the Jones projections $e_1, e_2, e_3, \ldots$, the idea being as folows:

(1) When performing a basic construction, we obtain, by trace manipulations on e_1:

$$N \notin (1,2)$$

With a double basic construction, we obtain, by trace manipulations on $< e_1, e_2 >$:

$$N \notin \left(2, \frac{3+\sqrt{5}}{2}\right)$$

With a triple basic construction, we obtain, by trace manipulations on $< e_1, e_2, e_3 >$:

$$N \notin \left(\frac{3+\sqrt{5}}{2}, 3\right)$$

Thus, we are led to the conclusion in the statement, by a kind of recurrence, involving a certain family of orthogonal polynomials.

(2) In practice now, the most elegant way of proving the result is by using the fundamental fact, explained in Theorem 16.44, that that sequence of Jones projections $e_1, e_2, e_3, \ldots \subset B(H)$ generate a copy of the Temperley-Lieb algebra of index N:

$$TL_N \subset B(H)$$

With this result in hand, we must prove that such a representation cannot exist in index $N < 4$, unless we are in the following special situation:

$$N = 4\cos^2\left(\frac{\pi}{n}\right)$$

But this can be proved by using some suitable trace and positivity manipulations on TL_N, as in (2) above. For full details here, we refer to [57]. □

In relation now with subfactors, the result, which extends Theorem 16.44, and which was found by Jones in [60], almost 20 years after [57], is as follows:

THEOREM 16.46. *Given a subfactor $A_0 \subset A_1$, the collection $P = (P_n)$ of linear spaces*

$$P_n = A_0' \cap A_n$$

has a planar algebra structure, extending the planar algebra structure of TL_N.

PROOF. We know from Theorem 16.44 that we have an inclusion as follows, coming from the basic construction, and with TL_N itself being a planar algebra:

$$TL_N \subset P$$

Thus, the whole point is that of proving that the trivial planar algebra structure of TL_N extends into a planar algebra structure of P. But this can be done via a long algebraic study, and for the full computation here, we refer to Jones' paper [60]. □

As a first illustration for the above result, we have:

THEOREM 16.47. *We have the following universality results:*

(1) *The Temperley-Lieb algebra TL_N appears inside the planar algebra of any subfactor $A_0 \subset A_1$ having index N.*
(2) *The Fuss-Catalan algebra $FC_{N,M}$ appears inside the planar algebra of any subfactor $A_0 \subset A_1$, in the presence of an intermediate subfactor $A_0 \subset B \subset A_1$.*

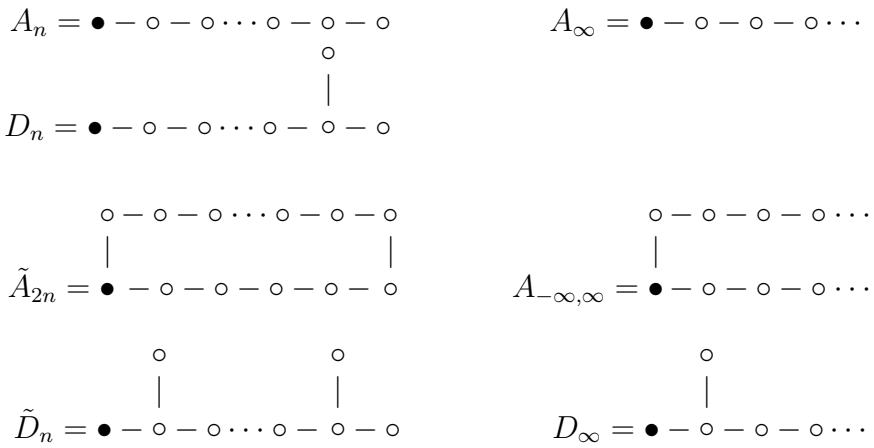
PROOF. Here the first assertion is something that we already know, from Theorem 16.46, and the second assertion is something quite standard as well, by carefully working out the basic construction for $A_0 \subset A_1$, in the presence of an intermediate subfactor $A_0 \subset B \subset A_1$. For details here, we refer to the papers of Bisch and Jones. □

As a consequence of the above, in relation with classification questions, we have:

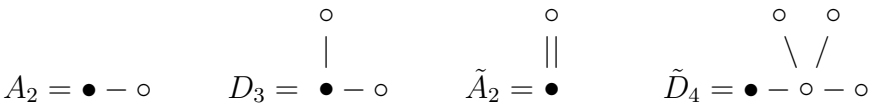
THEOREM 16.48. *The principal graph of a subfactor having index $N \leq 4$ must be one of the Coxeter-Dynkin graphs of type ADE.*

PROOF. This follows indeed from the well-known formula $N = ||X||^2$, and from the considerations from the proof of the Jones index restriction theorem. □

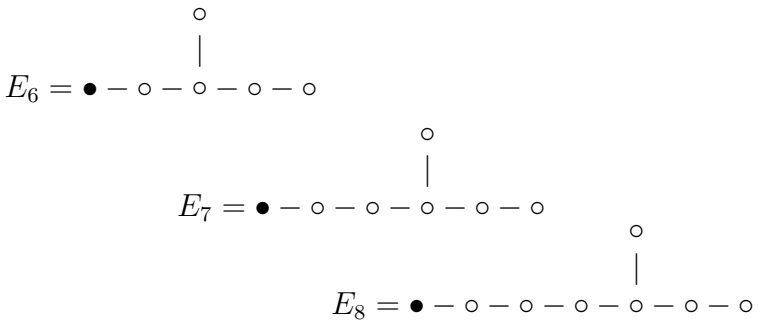
More in detail now, the usual Coxeter-Dynkin graphs are as follows:



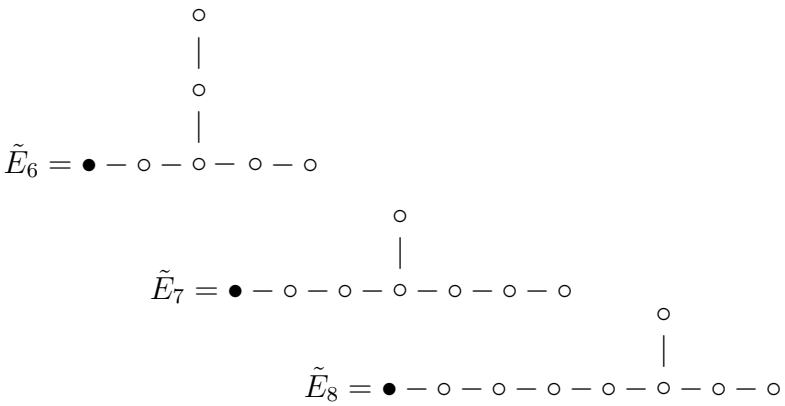
Here the graphs A_n with $n \geq 2$ and D_n with $n \geq 3$ have by definition n vertices each, $\tilde{A}_{2n}$ with $n \geq 1$ has $2n$ vertices, and $\tilde{D}_n$ with $n \geq 4$ has $n+1$ vertices. Thus, the first graph in each series is by definition as follows:



There are also a number of exceptional Coxeter-Dynkin graphs. First we have:



Also, we have as well index 4 versions of the above exceptional graphs, as follows:



Getting back now to Theorem 16.48, with this list in hand, the story is not over here, because we still have to understand which of these graphs can really appear as principal graphs of subfactors. The result here, in a simplified version, is as follows:

THEOREM 16.49. *The principal graphs of subfactors of index ≤ 4 are:*

(1) *Index < 4 graphs: A_n, D_{even}, E_6, E_8.*
(2) *Index 4 finite graphs: $\tilde{A}_{2n}$, $\tilde{D}_n$, $\tilde{E}_6$, $\tilde{E}_7$, $\tilde{E}_8$.*
(3) *Index 4 infinite graphs: A_∞, $A_{-\infty,\infty}$, D_∞.*

PROOF. As already mentioned, this is something quite heavy, with contributions by many authors. Observe that the graphs D_{odd} and E_7 don't appear in the above list. This is one of the subtle points of subfactor theory. For a discussion here, see [57]. □

Regarding now the subfactors of index $N \in (4, 5]$, and also of small index above 5, these can be classified, but this is a long and complicated story. Let us just record here the result in index 5, which is something quite easy to formulate, as follows:

THEOREM 16.50. *The principal graphs of the irreducible index* 5 *subfactors are:*

(1) A_∞*, and a non-extremal perturbation of* $A_\infty^{(1)}$*.*
(2) *The McKay graphs of* $\mathbb{Z}_5, D_5, GA_1(5), A_5, S_5$*.*
(3) *The twists of the McKay graphs of* A_5, S_5*.*

PROOF. This is a heavy result, and there is a long story with this. □

As a comment here, the above $N = 5$ result was much harder to obtain than the classification in index $N = 4$, obtained as a consequence of Theorem 16.48. However, at the level of the explicit construction of such subfactors, things are quite similar at $N = 4$ and $N = 5$, with the fixed point subfactors associated to quantum permutation groups $G \subset S_N^+$ providing most of the examples. We refer here to the literature.

In index $N = 6$ now, the subfactors cannot be classified, at least in general, due to several uncountable families, coming from groups, group duals, and more generally compact quantum groups. The exact assumption to be added is not known yet.

16e. Exercises

Congratulations for having read this book, and no exercises for this final chapter.

Bibliography

[1] E. Abe, Hopf algebras, Cambridge Univ. Press (1980).

[2] V.I. Arnold, Mathematical methods of classical mechanics, Springer (1974).

[3] V.I. Arnold, Lectures on partial differential equations, Springer (1997).

[4] V.I. Arnold and B.A. Khesin, Topological methods in hydrodynamics, Springer (1998).

[5] M.F. Atiyah, The geometry and physics of knots, Cambridge Univ. Press (1990).

[6] M.F. Atiyah and I.G. MacDonald, Introduction to commutative algebra, Addison-Wesley (1969).

[7] T. Banica, Linear algebra and group theory (2024).

[8] T. Banica, Advanced linear algebra (2025).

[9] T. Banica, Basic quantum algebra (2025).

[10] R.J. Baxter, Exactly solved models in statistical mechanics, Academic Press (1982).

[11] I. Bengtsson and K. Życzkowski, Geometry of quantum states, Cambridge Univ. Press (2006).

[12] S.J. Blundell and K.M. Blundell, Concepts in thermal physics, Oxford Univ. Press (2006).

[13] R. Brauer, On algebras which are connected with the semisimple continuous groups, *Ann. of Math.* **38** (1937), 857–872.

[14] S.M. Carroll, Spacetime and geometry, Cambridge Univ. Press (2004).

[15] V. Chari and A. Pressley, A guide to quantum groups, Cambridge Univ. Press (1994).

[16] 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.

[17] A. Connes, Noncommutative geometry, Academic Press (1994).

[18] P. Deligne, Catégories tannakiennes, in "Grothendieck Festchrift", Birkhauser (1990), 111–195.

[19] P. Di Francesco, Meander determinants, *Comm. Math. Phys.* **191** (1998), 543–583.

[20] P. Diaconis and M. Shahshahani, On the eigenvalues of random matrices, *J. Applied Probab.* **31** (1994), 49–62.

[21] P.A.M. Dirac, Principles of quantum mechanics, Oxford Univ. Press (1930).

[22] M.P. do Carmo, Differential geometry of curves and surfaces, Dover (1976).

[23] S. Doplicher and J. Roberts, A new duality theory for compact groups, *Invent. Math.* **98** (1989), 157–218.

[24] V.G. Drinfeld, Quantum groups, Proc. ICM Berkeley (1986), 798–820.

[25] R. Durrett, Probability: theory and examples, Cambridge Univ. Press (1990).

[26] A. Einstein, Relativity: the special and the general theory, Dover (1916).

[27] M. Enock and J.M. Schwartz, Kac algebras and duality of locally compact groups, Springer (1992).

[28] P. Etingof, S. Gelaki, D. Nikshych and V. Ostrik, Tensor categories, AMS (2016).

[29] L.C. Evans, Partial differential equations, AMS (1998).

[30] L. Faddeev, N. Reshetikhin and L. Takhtadzhyan, Quantization of Lie groups and Lie algebras, *Leningrad Math. J.* **1** (1990), 193–225.

[31] W. Feller, An introduction to probability theory and its applications, Wiley (1950).

[32] E. Fermi, Thermodynamics, Dover (1937).

[33] R.P. Feynman, R.B. Leighton and M. Sands, The Feynman lectures on physics, Caltech (1963).

[34] P. Flajolet and R. Sedgewick, Analytic combinatorics, Cambridge Univ. Press (2009).

[35] W. Fulton, Algebraic topology, Springer (1995).

[36] W. Fulton and J. Harris, Representation theory, Springer (1991).

[37] C. Godsil and G. Royle, Algebraic graph theory, Springer (2001).

[38] H. Goldstein, C. Safko and J. Poole, Classical mechanics, Addison-Wesley (1980).

[39] J.M. Gracia-Bondía, J.C. Várilly and H. Figueroa, Elements of noncommutative geometry, Birkhäuser (2001).

[40] D.J. Griffiths, Introduction to electrodynamics, Cambridge Univ. Press (2017).

[41] D.J. Griffiths and D.F. Schroeter, Introduction to quantum mechanics, Cambridge Univ. Press (2018).

[42] D.J. Griffiths, Introduction to elementary particles, Wiley (2020).

[43] P. Griffiths and J. Harris, Principles of algebraic geometry, Wiley (1994).

[44] L.C. Grove, Classical groups and geometric algebra, AMS (2002).

[45] G.H. Hardy and E.M. Wright, An introduction to the theory of numbers, Oxford Univ. Press (1938).

[46] J. Harris, Algebraic geometry, Springer (1992).

[47] R. Hartshorne, Algebraic geometry, Springer (1977).

[48] A. Hatcher, Algebraic topology, Cambridge Univ. Press (2002).

[49] R.A. Horn and C.R. Johnson, Matrix analysis, Cambridge Univ. Press (1985).

[50] K. Huang, Introduction to statistical physics, CRC Press (2001).

[51] J.E. Humphreys, Introduction to Lie algebras and representation theory, Springer (1972).

[52] J.E. Humphreys, Linear algebraic groups, Springer (1975).

[53] M. Idel and M.M. Wolf, Sinkhorn normal form for unitary matrices, *Linear Algebra Appl.* **471** (2015), 76–84.

[54] K. Ireland and M. Rosen, A classical introduction to modern number theory, Springer (1982).

[55] N. Jacobson, Basic algebra, Dover (1974).

[56] M. Jimbo, A q-difference analog of $U(\mathfrak{g})$ and the Yang-Baxter equation, *Lett. Math. Phys.* **10** (1985), 63–69.

[57] V.F.R. Jones, Index for subfactors, *Invent. Math.* **72** (1983), 1–25.

[58] V.F.R. Jones, On knot invariants related to some statistical mechanical models, *Pacific J. Math.* **137** (1989), 311–334.

[59] V.F.R. Jones, Subfactors and knots, AMS (1991).

[60] V.F.R. Jones, Planar algebras I (1999).

[61] C. Kassel, Quantum groups, Springer (1995).

[62] T. Kibble and F.H. Berkshire, Classical mechanics, Imperial College Press (1966).

[63] M. Kumar, Quantum: Einstein, Bohr, and the great debate about the nature of reality, Norton (2009).

[64] G. Landi, An introduction to noncommutative spaces and their geometry, Springer (1997).

[65] S. Lang, Algebra, Addison-Wesley (1993).

[66] S. Lang, Abelian varieties, Dover (1959).

[67] P. Lax, Linear algebra and its applications, Wiley (2007).

[68] P. Lax, Functional analysis, Wiley (2002).

[69] B. Lindstöm, Determinants on semilattices, *Proc. Amer. Math. Soc.* **20** (1969), 207–208.

[70] F. Lusztig, Introduction to quantum groups, Birkhäuser (1993).

[71] S. Majid, Foundations of quantum group theory, Cambridge Univ. Press (1995).

[72] S. Malacarne, Woronowicz's Tannaka-Krein duality and free orthogonal quantum groups, *Math. Scand.* **122** (2018), 151–160.

[73] Y.I. Manin, Quantum groups and noncommutative geometry, Springer (2018).

[74] V.A. Marchenko and L.A. Pastur, Distribution of eigenvalues in certain sets of random matrices, *Mat. Sb.* **72** (1967), 507–536.

[75] M.L. Mehta, Random matrices, Elsevier (2004).

[76] S. Montgomery, Hopf algebras and their actions on rings, AMS (1993).

[77] M.A. Nielsen and I.L. Chuang, Quantum computation and quantum information, Cambridge Univ. Press (2000).

[78] P. Petersen, Linear algebra, Springer (2012).

[79] D.E. Radford, Hopf algebras, World Scientific (2011).

[80] W. Rudin, Principles of mathematical analysis, McGraw-Hill (1964).

[81] W. Rudin, Real and complex analysis, McGraw-Hill (1966).

[82] W. Rudin, Fourier analysis on groups, Dover (1972).

[83] D.V. Schroeder, An introduction to thermal physics, Oxford Univ. Press (1999).

[84] J.P. Serre, A course in arithmetic, Springer (1973).

[85] J.P. Serre, Linear representations of finite groups, Springer (1977).

[86] I.R. Shafarevich, Basic algebraic geometry, Springer (1974).

[87] G.C. Shephard and J.A. Todd, Finite unitary reflection groups, *Canad. J. Math.* **6** (1954), 274–304.

[88] M.E. Sweedler, Hopf algebras, W.A. Benjamin (1969).

[89] P. Tarrago and M. Weber, Unitary easy quantum groups: the free case and the group case, *Int. Math. Res. Not.* **18** (2017), 5710–5750.

[90] J.R. Taylor, Classical mechanics, Univ. Science Books (2003).

[91] D.V. Voiculescu, K.J. Dykema and A. Nica, Free random variables, AMS (1992).

[92] J. von Neumann, Mathematical foundations of quantum mechanics, Princeton Univ. Press (1955).

[93] S. Weinberg, Foundations of modern physics, Cambridge Univ. Press (2011).

[94] S. Weinberg, Lectures on quantum mechanics, Cambridge Univ. Press (2012).

[95] D. Weingarten, Asymptotic behavior of group integrals in the limit of infinite rank, *J. Math. Phys.* **19** (1978), 999–1001.

[96] H. Weyl, The theory of groups and quantum mechanics, Princeton Univ. Press (1931).

[97] H. Weyl, The classical groups: their invariants and representations, Princeton Univ. Press (1939).

[98] H. Weyl, Space, time, matter, Princeton Univ. Press (1918).

[99] E. Wigner, Characteristic vectors of bordered matrices with infinite dimensions, *Ann. of Math.* **62** (1955), 548–564.

[100] S.L. Woronowicz, Compact matrix pseudogroups, *Comm. Math. Phys.* **111** (1987), 613–665.

Index