Introduction to Lie groups

Teo Banica

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CERGY-PONTOISE, F-95000 CERGY-PONTOISE, FRANCE. teo.banica@gmail.com

2010 Mathematics Subject Classification. 22E10 Key words and phrases. Compact group, Lie group

ABSTRACT. This is an introduction to the Lie groups and algebras, with general methods, examples and applications, and with emphasis on the compact case. We first discuss the basics of group theory, notably with various results about the real and complex rotation groups, and the symplectic groups. Then we go into a study of the representation theory of Lie groups, notably with sharp results in the compact case, following Peter-Weyl, Schur, Tannaka, Brauer and others. We discuss then the theory of Lie algebras, and its applications, notably to the classification of Lie groups, and to various questions from mechanics. Finally, we discuss a number of analytic questions, of probabilistic nature, with the help of representation theory, and of Lie algebra methods too.

Preface

Transformation groups of the space surrounding us are as old as this world, as we know it, or perhaps even older, with some of the physicists' modern theories stating that, precisely, in the Far West of the first few seconds following the Big Bang, all that crazy particles were not that free to do what they want, being bound to some basic symmetry rules, involving such transformation groups. Good time that was, back then.

In more recent times, with respect to more traditional physics, transformation groups are surely present too, a bit everywhere. Various questions in mechanics, especially in fluid dynamics, involving what we mathematicians call diffeomorphisms, and in Einstein's relativity theory too, require some good knowledge of continuous group theory, for proper understanding. As for more recent disciplines like quantum mechanics, which actually bring us back to the Big Bang situation evoked above, no question about this either, transformation groups rule, over the particles there, and what they can really do.

Mathematically speaking now, and here comes our point, the theory of the continuous transformation groups is something quite recent, and this for a number of reasons. Such groups, called Lie groups in the honor of Sophus Lie, who was first to study them systematically, require indeed some substantial abstract algebra, and some substantial differential geometry too, for their understanding, and with these two ingredients being both something quite recent, so is the theory of Lie groups. In a word, quite recent theory that we have here, basically going back to no more than 100 years ago, and with the main applications being, and it is probably safe to conjecture this, still to come.

This book is an introduction to the Lie groups and algebras, with general methods, examples and applications explained, starting from zero or almost, and with emphasis on the compact Lie group case. The book is organized in four parts, as follows:

(1) We first discuss the basics of group theory, notably with various results about the real and complex rotation groups, and the symplectic groups.

(2) Then we go into the representation theory of Lie groups, notably with sharp results in the compact case, following Peter-Weyl, Schur, Tannaka, Brauer and others.

PREFACE

(3) We discuss then the theory of Lie algebras, and its applications, notably to the classification of Lie groups, and to various questions from mechanics.

(4) Finally, we discuss a number of analytic questions, of probabilistic nature, with the help of representation theory, and of Lie algebra methods too.

In the hope that you will find this book useful. As already said in the above, the theory of Lie groups is something quite recent, with the main applications probably still to come, and in view of this, it is probably safe to say that no one really knows how to properly present this material, for someone willing to learn, and then look for future applications. So, one Lie group book among others, with the presentation scheme reflecting the views of the authors, which in my personal case amount in focusing on the compact case, and also favoring representation theory and Brauer type algebras over Lie algebras. No idea if this is right or wrong, and now that you're learning, please make sure to have some other Lie group books on your desk too. The truth about Lie groups should be somewhere, there in the pile, including the present book, and up to you to discover it.

Many thanks to my quantum group colleagues and collaborators, most of the things about Lie groups that I know, I learned them from them. Thanks as well to my cats, whether they use smooth or non-smooth transformations in their daily work remains a bit of a mystery for me, but so many things to be learned from them, for sure.

Cergy, April 2025 Teo Banica

Contents

Preface	3
Part I. Lie groups	9
Chapter 1. Group theory	11
1a. Groups, examples	11
1b. Dihedral groups	14
1c. Cayley embeddings	21
1d. Abelian groups	26
1e. Exercises	32
Chapter 2. Rotation groups	33
2a. Rotation groups	33
2b. Pauli matrices	36
2c. Euler-Rodrigues	42
2d. Higher dimensions	49
2e. Exercises	50
Chapter 3. Reflection groups	51
3a. Hyperoctahedral groups	51
3b. Complex reflections	53
3c. Reflection groups	54
3d. Further examples	55
3e. Exercises	56
Chapter 4. Symplectic groups	57
4a. Bistochastic groups	57
4b. Symplectic groups	61
4c. Reflections, again	63
4d. Generation questions	64
4e. Exercises	66

Part II. Representations	67
Chapter 5. Representations	69
5a. Basic theory	69
5b. Peter-Weyl theory	73
5c. Haar integration	78
5d. More Peter-Weyl	85
5e. Exercises	88
Chapter 6. Tannakian duality	89
6a. Generalities	89
6b. Tensor categories	96
6c. The correspondence	103
6d. Brauer theorems	107
6e. Exercises	112
Chapter 7. Diagrams, easiness	113
7a. Easy groups	113
7b. Reflection groups	120
7c. Basic operations	124
7d. Classification results	131
7e. Exercises	136
Chapter 8. Gram determinants	137
8a. Gram determinants	137
8b. Symmetric groups	138
8c. Reflection groups	140
8d. Further results	142
8e. Exercises	144
Part III. Lie algebras	145
Chapter 9. Lie algebras	147
9a. Lie algebras	147
9b.	154
9c.	154
9d.	154
9e. Exercises	154

CONTENTS

CONTENTS	7
Chapter 10.	155
10a.	155
10b.	155
10c.	155
10d.	155
10e. Exercises	155
Chapter 11.	157
11a.	157
11b.	157
11c.	157
11d.	157
11e. Exercises	157
Chapter 12.	159
12a.	159
12b.	159
12c.	159
12d.	159
12e. Exercises	159
Part IV. Analytic aspects	161
	100

Chapter 13. Haar integration	103
13a. Spherical integrals	163
13b. Complex variables	169
13c. Poisson laws	175
13d. Asymptotic characters	175
13e. Exercises	178
Chapter 14. Weingarten calculus	179
14a. Weingarten formula	179
14b. Basic estimates	181
14c. Truncated characters	189
14d. Rotation groups	192
14e. Exercises	202
Chapter 15.	203

hap	ter 1	15			

CONTENTS

15a.	203
15b.	203
15c.	203
15d.	203
15e. Exercises	203
Chapter 16.	205
16a.	205
16b.	205
16c.	205
16d.	205
16e. Exercises	205
Bibliography	207

Part I

Lie groups

We've got a mind of our own So go to hell if what you're thinking is not right Love would never leave us alone Ay, in the darkness there must come out the light

CHAPTER 1

Group theory

1a. Groups, examples

Let us begin our study with some abstract aspects. A group is something very simple, namely a set, 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:

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

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.

At the level of examples, we have for instance the symmetric group S_N . There are many other examples, with typically the basic systems of numbers that we know being abelian groups, and the basic sets of matrices being non-abelian groups. Once again, this is of course not a general rule. Here are some basic examples and counterexamples:

PROPOSITION 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. \Box

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:

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

(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 q is the inverse of q^{-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. Dihedral 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 . There are many ways of picturing \mathbb{Z}_N , both additive and multiplicative, as follows:

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.

Another interesting example of a finite group, which is more advanced, and which is non-abelian this time, is the dihedral group D_N , which appears as follows:

DEFINITION 1.6. 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:

<u>N=2</u>. 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 $D_2 = \mathbb{Z}_2$.

<u>N=3</u>. 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 $D_3 = S_3$.

<u>N = 4</u>. Here the N-gon is a square, and as symmetries we have 4 rotations, of angles $0^{\circ}, 90^{\circ}, 180^{\circ}, 270^{\circ}$, 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.

<u>N = 5</u>. 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:



<u>N = 6</u>. 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:



<u>N = 7</u>. Here the N-gon is a regular heptagon, and as symmetries we have 7 rotations, of angles $0^{\circ}, \alpha^{\circ}, \ldots, 6\alpha^{\circ}$, with $\alpha = 360/7$, as well as 7 symmetries, with respect to the 7 symmetry axes, which join the vertices to the midpoints of the 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.

1B. DIHEDRAL GROUPS

In general, we have the following result, regarding them:

PROPOSITION 1.7. 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 labelling 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, ..., N. But these are exactly the rotations $R_1, ..., R_N$ 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 1.8. 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 1.7, the various compositions between rotations and symmetries can be computed as follows:

$$\begin{aligned} R_k R_l &: i \to l+i \to k+l+i \\ R_k S_l &: i \to l-i \to k+l-i \\ S_k R_l &: i \to l+i \to k-l-i \\ S_k S_l &: i \to l-i \to k-l+i \end{aligned}$$

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.

Observe 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 1.9. 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 labelled 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. \Box

Let us compare now Theorem 1.8 and Proposition 1.9. 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 1.10. 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 as follows:

$$(g,a)(h,b) = (gh^a,ab)$$

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 1.8, into a final result on the subject, as follows:

THEOREM 1.11. 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 1.9. The elements of P_N can indeed be labelled ρ_1, \ldots, ρ_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 9.9, perturbed as in Definition 1.10. 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 1.8. 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.

As a third basic example of a finite group, we have the symmetric group S_N . This is a group that we know well from linear algebra, when talking about the determinant:

THEOREM 1.12. The permutations of $\{1, \ldots, N\}$ form a group, denoted S_N , and called symmetric group. This group has N! elements. The signature map

$$\varepsilon: S_N \to \mathbb{Z}_2$$

can be regarded as being a group morphism, with values in $\mathbb{Z}_2 = \{\pm 1\}$.

PROOF. These are things that we know from linear algebra. Indeed, the group property is clear, and the count is clear as well. As for the last assertion, recall the following formula for the signatures of the permutations, that we know too from linear algebra:

$$\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$$

But this tells us precisely that ε is a group morphism, as stated.

We will be back to S_N on many occasions, in what follows. At an even more advanced level now, we have the hyperoctahedral group H_N , which appears as follows:

DEFINITION 1.13. The hyperoctahedral group H_N is the group of symmetries of the unit cube in \mathbb{R}^N .

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 $N \in \mathbb{N}$:

<u>N = 1</u>. Here the 1-cube is the segment, whose symmetries are the identity *id* and the flip τ . Thus, we obtain the group with 2 elements, which is a very familiar object:

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

<u>N=2</u>. Here the 2-cube is the square, and so the corresponding symmetry group is the dihedral group D_4 , which is a group that we know well:

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

N = 3. Here the 3-cube is the usual cube, and the situation is considerably more complicated, because this usual cube has no less than 48 symmetries. 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 1.14. 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. Thus, we have:

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

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.

To be more precise, we have the following result, clarifying the above:

THEOREM 1.15. 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:

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

PROOF. As explained in the proof of Theorem 1.14, 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:

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

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 Definition 1.10, 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. \Box

Summarizing, we have so far many interesting examples of finite groups, and as a sequence of main examples, we have the following groups:

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

We will be back to these fundamental finite groups later on, on several occasions, with further results on them, both of algebraic and of analytic type.

1c. Cayley embeddings

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

THEOREM 1.16. Given a finite group G, we have an embedding as follows,

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

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:

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

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:

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

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:

$$g \neq h \implies \sigma_g(1) \neq \sigma_h(1)$$
$$\implies \sigma_g \neq \sigma_h$$

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 .

22

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 1.17. 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 1.18. 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 1.19. Given a finite group G, we have an embedding as follows,

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

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

PROOF. The Cayley theorem gives an embedding as follows:

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

On the other hand, Theorem 1.18 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:

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

As before, 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.

Summarizing, in order to advance, it is better to forget about the Cayley theorem, and build on Theorem 1.18 instead. In relation with the basic groups, we have:

THEOREM 1.20. 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 1.18 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 :

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

24

1C. CAYLEY EMBEDDINGS

(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 1.18 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 by Theorem 1.14 these matrices form a group, which is isomorphic to H_N .

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

DEFINITION 1.21. The complex reflection group $H_N^s \subset U_N$, depending on parameters

$$N \in \mathbb{N}$$
 , $s \in \mathbb{N} \cup \{\infty\}$

is the group of permutation-type matrices with s-th roots of unity as entries,

 $H_N^s = M_N(\mathbb{Z}_s \cup \{0\}) \cap U_N$

with the convention $\mathbb{Z}_{\infty} = \mathbb{T}$, at $s = \infty$.

Observe that at s = 1, 2 we obtain the following groups:

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

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

$$K_N \subset U_N$$

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

PROPOSITION 1.22. 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 1.23. We have a wreath product decomposition $H_N^s = \mathbb{Z}_s \wr S_N$, which means by definition that we have a crossed product decomposition

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

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

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

PROOF. As explained in the proof of Proposition 1.22, 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 Definition 1.10, 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.

Summarizing, and by focusing now on the cases $s = 1, 2, \infty$, which are the most important, we have extended our series of basic unitary groups, as follows:

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

In addition to this, we have the groups H_N^s with $s \in \{3, 4, ..., \}$. However, these will not fit well into the above series of inclusions, because we only have:

$$s|t \implies H_N^s \subset H_N^t$$

Thus, we can only extend our series of inclusions as follows:

$$\mathbb{Z}_N \subset D_N \subset S_N \subset H_N \subset H_N^4 \subset H_N^8 \subset \ldots \subset K_N$$

We will be back later to H_N^s , with more theory, and some generalizations as well.

1d. Abelian groups

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 this chapter, 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, and coming somewhat as a surprise, this leads us again into linear algebra, due to the following fact:

1D. ABELIAN GROUPS

THEOREM 1.24. 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 1.25. 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:

$$\chi(g,h) = \chi[(g,1)(1,h)] = \chi(g,1)\chi(1,h)$$

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.

We can get some further insight into duality by using the some standard spectral theory methods, and we have the following result:

THEOREM 1.26. 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 $G = \widehat{G}$.

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 $X = \hat{G}$, 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. \Box

All the above is very nice, but remains something rather abstract, based on all sorts of clever algebraic manipulations, and no computations at all. So, now that we are done with this, time to get into some serious computations. For this purpose, we will need some basic abstract results, which are good to know. Let us start with:

THEOREM 1.27. Given a finite group G and a subgroup $H \subset G$, the sets

$$G/H = \{gH \mid g \in G\} \quad , \quad H \setminus G = \{Hg \mid g \in G\}$$

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

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

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

 $|H| \mid |G|$

When $H \subset G$ is normal, gH = Hg for any $g \in G$, the space $G/H = H \setminus G$ 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 $G/H = H \setminus G$ is a indeed group, with multiplication (gH)(sH) = gsH.

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

THEOREM 1.28. Given a finite group G, any $g \in G$ generates a cyclic subgroup

$$\langle g \rangle = \{1, g, g^2, \dots, g^{k-1}\}$$

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

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

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

PROOF. As before with Theorem 1.27, 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 $\langle g \rangle \subset G$ formed by the sequence of powers of g:

$$\langle g \rangle = \{1, g, g^2, g^3, \ldots\} \subset G$$

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:

$$\langle g \rangle = \{1, g, g^2, \dots, g^{k-1}\}$$

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 $\langle g \rangle \subset G$ is indeed a group, and more specifically a cyclic group, of order k = ord(g). Finally, ord(g) | |G| follows from Theorem 1.27. \Box

With these 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 1.29. 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, $G = \hat{G}$.

1D. ABELIAN GROUPS

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, $G = \hat{G}$, follows from the structure result that we just proved, and from Theorem 1.25 (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 1.29, 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 will be back to the finite groups, which are quite fascinating objects, on a regular basis, in what follows. In fact, one of the main questions that we will investigate in this book will be the classification of the finite subgroups $H \subset G$ of a continuous group G. But more on this later, once we will know more about such continuous groups G.

1e. Exercises

Exercises:

EXERCISE 1.30.

EXERCISE 1.31.

EXERCISE 1.32.

Exercise 1.33.

Exercise 1.34.

EXERCISE 1.35.

Exercise 1.36.

Exercise 1.37.

Bonus exercise.

CHAPTER 2

Rotation groups

2a. Rotation groups

In the continuous group case, that we will be mainly interested in, in this book, we first have, as basic examples, the unitary group U_N itself, then its real version, which is the orthogonal group O_N , and various technical versions of these basic groups O_N, U_N .

So, let us start with some basic reminders, regarding O_N, U_N :

THEOREM 2.1. 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 also know 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:

2. ROTATION GROUPS

PROPOSITION 2.2. 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:

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

(2) We have indeed the following implications:

$$U \in U_N \implies U^* = U^{-1}$$
$$\implies \det U^* = \det U^{-1}$$
$$\implies \det U = (\det U)^{-1}$$
$$\implies \det U \in \mathbb{T}$$

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 2.3. The following are groups of matrices,

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

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. \Box

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



As an illustration, let us work out what happens at N = 1, 2. At N = 1 the situation is quite trivial, and we obtain very simple groups, as follows:

PROPOSITION 2.4. The basic continuous groups at N = 1, namely



are the following groups of complex numbers,



or, equivalently, are the following cyclic groups,



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 $\overline{U} = U^{-1}$, 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 2.5. 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:

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

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

2. ROTATION GROUPS

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 already know, from chapter 1, obtained by computing $R_t \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $R_t \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

(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 basically know too, obtained by computing $S_t \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $S_t \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

(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. \Box

In general, the structure of O_N and SO_N , and the relation between them, is far more complicated than what happens at N = 1, 2. We will be back to this later.

2b. Pauli matrices

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 2.6. We have the following formula,

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

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:

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

$$S_{\mathbb{C}}^{1} = \left\{ (a, b) \mid |a|^{2} + |b|^{2} = 1 \right\}$$

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 2.7. We have the following formula,

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

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 2.6, 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:

$$|\det(U)|^2 = \det(U)\overline{\det(U)}$$

= $\det(U)\det(U^*)$
= $\det(UU^*)$
= $\det(1)$
= 1

Consider now the following complex number, defined up to a sign choice:

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

2. ROTATION GROUPS

We know from Proposition 2.2 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:

$$det(V) = det(U/d)$$

= $det(U)/d^2$
= $det(U)/det(U)$
= 1

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 .

Let us record now a few more results regarding SU_2, U_2 , which are key groups in mathematics and physics. First, we have the following reformulation of Theorem 2.6:

THEOREM 2.8. We have the formula

$$SU_{2} = \left\{ \begin{pmatrix} x + iy & z + it \\ -z + it & x - iy \end{pmatrix} \mid x^{2} + y^{2} + z^{2} + t^{2} = 1 \right\}$$

which makes SU_2 isomorphic to the unit real sphere $S^3_{\mathbb{R}} \subset \mathbb{R}^3$.

PROOF. We recall from Theorem 2.6 that we have:

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

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:

$$a = x + iy$$
 , $b = z + it$

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:

$$S_{\mathbb{R}}^{3} = \left\{ (x, y, z, t) \mid x^{2} + y^{2} + z^{2} + t^{2} = 1 \right\}$$

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

$$SU_2 \simeq S^3_{\mathbb{R}}$$
, $\begin{pmatrix} x+iy & z+it \\ -z+it & x-iy \end{pmatrix} \rightarrow (x,y,z,t)$

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 2.9. We have the following formula,

$$U_2 = \left\{ (p+iq) \begin{pmatrix} x+iy & z+it \\ -z+it & x-iy \end{pmatrix} \mid x^2 + y^2 + z^2 + t^2 = 1, \ p^2 + q^2 = 1 \right\}$$

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 Theorem 2.7 that we have:

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

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 , b = z + it , 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:

$$x^{2} + y^{2} + z^{2} + t^{2} = 1$$
 , $p^{2} + q^{2} = 1$

2. ROTATION GROUPS

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:

$$S_{\mathbb{R}}^{3} = \left\{ (x, y, z, t) \mid x^{2} + y^{2} + z^{2} + t^{2} = 1 \right\}$$
$$S_{\mathbb{R}}^{1} = \left\{ (p, q) \mid p^{2} + q^{2} = 1 \right\}$$

Thus, we have quotient map of compact spaces, as follows:

$$S^{3}_{\mathbb{R}} \times S^{1}_{\mathbb{R}} \to U_{2}$$
$$((x, y, z, t), (p, q)) \to (p + iq) \begin{pmatrix} x + iy & z + it \\ -z + it & x - iy \end{pmatrix}$$

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 2.8:

THEOREM 2.10. We have the following formula,

$$SU_2 = \left\{ xc_1 + yc_2 + zc_3 + tc_4 \mid x^2 + y^2 + z^2 + t^2 = 1 \right\}$$

where c_1, c_2, c_3, c_4 are the Pauli matrices, given by:

$$c_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} , \quad c_2 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$
$$c_3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} , \quad c_4 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

PROOF. We recall from Theorem 2.8 that the group SU_2 can be parametrized by the real sphere $S^3_{\mathbb{R}} \subset \mathbb{R}^4$, in the following way:

$$SU_{2} = \left\{ \begin{pmatrix} x + iy & z + it \\ -z + it & x - iy \end{pmatrix} \mid x^{2} + y^{2} + z^{2} + t^{2} = 1 \right\}$$

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:

40

THEOREM 2.11. 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

 $\langle a, b \rangle = tr(ab^*)$

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 $i \neq j$:

$$\langle c_i, c_j \rangle = tr(c_i c_j^*) = tr(\pm c_i c_j) = tr(\pm c_k) = 0$$

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. Remember indeed the basic discussion from foundational quantum mechanics, involving the wave functions $\psi : \mathbb{R}^3 \to \mathbb{C}$ of these electrons, and of the Hilbert space $H = L^2(\mathbb{R}^3)$ needed for understanding their quantum mechanics. Well, that was only half of the story, with the other half coming from the fact that, 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 wave function space $H = L^2(\mathbb{R}^3)$ has to be enlarged with a copy of $K = \mathbb{C}^2$, 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.

2. ROTATION GROUPS

2c. 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 2.12. 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 2.11. 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 2.11, 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:

$$T_U T_V(M) = UVMV^*U^* = T_{UV}(M)$$

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 2.12 can be improved as follows:

THEOREM 2.13. 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 $SU_2 \rightarrow SO_3$.

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 10.12 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 2.12:

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

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:

$$\langle T_{U^*}(M), N \rangle = \langle U^*MU, N \rangle$$

= $tr(U^*MUN)$
= $tr(MUNU^*)$

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

$$\langle (T_U)^t(M), N \rangle = \langle M, T_U(N) \rangle$$

= $\langle M, UNU^* \rangle$
= $tr(MUNU^*)$

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:

$$T_U(c_1) = Uc_1U^* = UU^* = 1 = c_1$$

43

2. ROTATION GROUPS

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:

$$SU_2 \rightarrow O_3$$

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 $SU_2 \rightarrow SO_3$ 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 as follows:

$$(x, y, z, t) \in S^3_{\mathbb{R}}$$

In order to work out all this, let us start with the following result, coming as a continuation of Proposition 2.12, independently of Theorem 2.13:

PROPOSITION 2.14. 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 $SU_2 \rightarrow O_4$, what we have in fact is a group morphism $SU_2 \rightarrow O_3$, and even $SU_2 \rightarrow SO_3$.

PROOF. With notations from Proposition 2.12 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:

$$U = xc_1 + yc_2 + zc_3 + tc_4$$
$$M = ac_1 + bc_2 + cc_3 + dc_4$$

2C. EULER-RODRIGUES

By using the multiplication formulae in Theorem 2.11, we obtain:

$$UM = (xc_1 + yc_2 + zc_3 + tc_4)(ac_1 + bc_2 + cc_3 + dc_4)$$

= $(xa - yb - zc - td)c_1$
+ $(xb + ya + zd - tc)c_2$
+ $(xc - yd + za + tb)c_3$
+ $(xd + yc - zb + ta)c_4$

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 2.11, we obtain:

$$MU^* = (ac_1 + bc_2 + cc_3 + dc_4)(xc_1 - yc_2 - zc_3 - tc_4)$$

= $(ax + by + cz + dt)c_1$
+ $(-ay + bx - ct + dz)c_2$
+ $(-az + bt + cx - dy)c_3$
+ $(-at - bz + cy + dx)c_4$

We conclude that the matrix of the right action considered above is:

$$R_{U} = \begin{pmatrix} x & y & z & t \\ -y & x & -t & z \\ -z & t & x & -y \\ -t & -z & y & x \end{pmatrix}$$

2. ROTATION GROUPS

Now by composing, the matrix of the adjoint matrix in the statement is:

$$\begin{aligned} T_U &= R_U L_U \\ &= \begin{pmatrix} x & y & z & t \\ -y & x & -t & z \\ -z & t & x & -y \\ -t & -z & y & x \end{pmatrix} \begin{pmatrix} x & -y & -z & -t \\ y & x & -t & z \\ z & t & x & -y \\ t & -z & y & x \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & x^2 + y^2 - z^2 - t^2 & 2(yz - xt) & 2(xz + yt) \\ 0 & 2(xt + yz) & x^2 + z^2 - y^2 - t^2 & 2(zt - xy) \\ 0 & 2(yt - xz) & 2(xy + zt) & x^2 + t^2 - y^2 - z^2 \end{pmatrix} \end{aligned}$$

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 2.13. $\hfill \Box$

We can now formulate the Euler-Rodrigues result, as follows:

THEOREM 2.15. We have a double cover map, obtained via the adjoint representation,

$$SU_2 \rightarrow SO_3$$

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 $SU_2 \rightarrow SO_3$, 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:

$$\ker(SU_2 \to SO_3) = \left\{ U \in SU_2 \middle| T_U(M) = M, \forall M \in E \right\}$$
$$= \left\{ U \in SU_2 \middle| UM = MU, \forall M \in E \right\}$$
$$= \left\{ U \in SU_2 \middle| Uc_i = c_i U, \forall i \right\}$$
$$= \{ \pm 1 \}$$

(2) Thus, we are done with this, and as a side remark here, this result shows that our morphism $SU_2 \rightarrow SO_3$ is ultimately a morphism as follows:

$$PU_2 \subset SO_3$$
 , $PU_2 = SU_2/\{\pm 1\}$

2C. EULER-RODRIGUES

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 $SU_2 \rightarrow SO_3$ 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 $SU_2 \rightarrow SO_3$ follows to be surjective around 1, and then globally.

– Another proof is via representation theory. Indeed, the representations of SU_2 and SO_3 are subject to very similar formulae, called Clebsch-Gordan rules, and this shows that $SU_2 \rightarrow SO_3$ is surjective. We will discuss this later in this book.

– 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:

$$b\bar{q} = bq$$
 , $b(p - \bar{p}) = (a - \bar{a})q$

2. ROTATION GROUPS

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:

$$q = \lambda b$$
 , $p = \lambda \cdot \frac{a - \bar{a}}{2}$

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:

$$|p|^{2} + |q|^{2} = |\lambda b|^{2} + \left|\lambda \cdot \frac{a - \bar{a}}{2}\right|^{2}$$
$$= \lambda^{2}(|b|^{2} + Im(a)^{2})$$
$$= \lambda^{2}(1 - Re(a)^{2})$$

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. In what concerns us, we will be back to this later, when doing representation theory, with some further comments on all this.

Regarding now O_3 , the extension from SO_3 is very simple, as follows:

2D. HIGHER DIMENSIONS

THEOREM 2.16. 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 2.15, because the determinant of an orthogonal matrix $U \in O_3$ must satisfy det $U = \pm 1$, 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.

2d. Higher dimensions

With the above small N examples worked out, let us discuss now the general theory, at arbitrary values of $N \in \mathbb{N}$. In the real case, we have the following result:

PROPOSITION 2.17. 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, and we have seen this already at N = 3, in the proof of Theorem 2.16. Finally, when N is even the situation is more complicated, and requires complex numbers. We will be back to this.

In the complex case now, the result is simpler, as follows:

PROPOSITION 2.18. 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. \Box

It is possible to use the decomposition in Proposition 2.18 in order to say more about what happens in the real case, in the context of Proposition 2.17, 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:

2. ROTATION GROUPS

THEOREM 2.19. 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. \Box

2e. Exercises

Exercises:

EXERCISE 2.20.

EXERCISE 2.21.

EXERCISE 2.22.

EXERCISE 2.23.

EXERCISE 2.24.

EXERCISE 2.25.

EXERCISE 2.26.

EXERCISE 2.27.

Bonus exercise.

CHAPTER 3

Reflection groups

3a. Hyperoctahedral groups

Back to the finite 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 3.1. The hyperoctahedral group H_N is the group of symmetries of the unit cube in \mathbb{R}^N .

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 $N \in \mathbb{N}$:

<u>N = 1</u>. Here the 1-cube is the segment, whose symmetries are the identity *id* and the flip τ . Thus, we obtain the group with 2 elements, which is a very familiar object:

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

<u>N=2</u>. Here the 2-cube is the square, and so the corresponding symmetry group is the dihedral group D_4 , which is a group that we know well:

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

N = 3. Here the 3-cube is the usual cube, and the situation is considerably more complicated, because this usual cube has no less than 48 symmetries. 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 3.2. 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 .

3. REFLECTION GROUPS

(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. Thus, we have:

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

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 3.3. 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:

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

PROOF. As explained in the proof of Theorem 3.2, 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, 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.

Summarizing, we have so far many interesting examples of finite groups, and as a sequence of main examples, we have the following groups:

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

We will be back to these fundamental finite groups later on, on several occasions, with further results on them, both of algebraic and of analytic type.

3b. 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 3.4. The complex reflection group $H_N^s \subset U_N$, depending on parameters

$$N \in \mathbb{N}$$
 , $s \in \mathbb{N} \cup \{\infty\}$

is the group of permutation-type matrices with s-th roots of unity as entries,

$$H_N^s = M_N(\mathbb{Z}_s \cup \{0\}) \cap U_N$$

with the convention $\mathbb{Z}_{\infty} = \mathbb{T}$, at $s = \infty$.

Observe that at s = 1, 2 we obtain the following groups:

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

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

$$K_N \subset U_N$$

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

PROPOSITION 3.5. 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 3.6. 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:

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

3. REFLECTION GROUPS

PROOF. As explained in the proof of Proposition 3.5, 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.

Summarizing, and by focusing now on the cases $s = 1, 2, \infty$, which are the most important, we have extended our series of basic unitary groups, as follows:

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

In addition to this, we have the groups H_N^s with $s \in \{3, 4, \ldots, \}$. However, these will not fit well into the above series of inclusions, because we only have $s|t \implies H_N^s \subset H_N^t$. Thus, we can only extend our series of inclusions as follows:

$$\mathbb{Z}_N \subset D_N \subset S_N \subset H_N \subset H_N^4 \subset H_N^8 \subset \ldots \subset K_N$$

We will be back later to H_N^s , with more theory, and some generalizations as well.

3c. Reflection groups

Back to the rotation groups, in the real case, we have the following result:

THEOREM 3.7. 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. \Box

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 3.8. 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 3.9. 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 3.10. 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. \Box

3d. Further examples

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 3.11. 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. \Box

3. REFLECTION GROUPS

3e. Exercises

Exercises:

EXERCISE 3.12.

EXERCISE 3.13.

EXERCISE 3.14.

Exercise 3.15.

Exercise 3.16.

Exercise 3.17.

Exercise 3.18.

EXERCISE 3.19.

Bonus exercise.

CHAPTER 4

Symplectic groups

4a. Bistochastic groups

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

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

As a basic example of a bistochastic matrix, we have of course the flat matrix \mathbb{I}_N . In fact, the various above notions of stochasticity are closely related to \mathbb{I}_N , or rather to the all-one vector ξ that the matrix \mathbb{I}_N/N projects on, in the following way:

PROPOSITION 4.2. Let $M \in M_N(\mathbb{C})$ be a square matrix.

- (1) *M* is row stochastic, with sums λ , when $M\xi = \lambda\xi$.
- (2) M is column stochastic, with sums λ , when $M^t \xi = \lambda \xi$.
- (3) M is bistochastic, with sums λ , when $M\xi = M^t\xi = \lambda\xi$.

PROOF. All these assertions are clear from definitions, because when multiplying a matrix by ξ , we obtain the vector formed by the row sums.

As an observation here, we can reformulate if we want the above statement in a purely matrix-theoretic form, by using the flat matrix \mathbb{I}_N , as follows:

PROPOSITION 4.3. Let $M \in M_N(\mathbb{C})$ be a square matrix.

- (1) M is row stochastic, with sums λ , when $M\mathbb{I}_N = \lambda \mathbb{I}_N$.
- (2) M is column stochastic, with sums λ , when $\mathbb{I}_N M = \lambda \mathbb{I}_N$.
- (3) *M* is bistochastic, with sums λ , when $M\mathbb{I}_N = \mathbb{I}_N M = \lambda \mathbb{I}_N$.

4. SYMPLECTIC GROUPS

PROOF. This follows from Proposition 4.2, and from the fact that both the rows and the columns of the flat matrix \mathbb{I}_N are copies of the all-one vector ξ .

In what follows we will be mainly interested in the unitary bistochastic matrices, which are quite interesting objects. These do not exactly cover the flat matrix \mathbb{I}_N , but cover instead the following related matrix, which appears in many linear algebra questions:

$$K_N = \frac{1}{N} \begin{pmatrix} 2-N & 2\\ & \ddots & \\ 2 & 2-N \end{pmatrix}$$

As a first result, regarding such matrices, we have the following statement:

THEOREM 4.4. For a unitary matrix $U \in U_N$, the following conditions 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:

$$1 = \sum_{i} < U_{1}, U_{i} >$$
$$= \sum_{j} U_{1j} \sum_{i} \overline{U}_{ij}$$
$$= \sum_{j} U_{1j} \cdot \overline{\lambda}$$
$$= |\lambda|^{2}$$

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

$$\sum_{j} U_{ij} = \lambda, \forall i \iff \sum_{j} U_{ij}\xi_j = \lambda\xi_i, \forall i$$
$$\iff U\xi = \lambda\xi$$

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

$$\sum_{i} U_{ij} = \lambda, \forall j \iff \sum_{j} U_{ij}\xi_i = \lambda\xi_j, \forall j$$
$$\iff U^t\xi = \lambda\xi$$

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:

$$U\xi = \lambda \xi \implies U^* U\xi = \lambda U^* \xi$$
$$\implies \xi = \lambda U^* \xi$$
$$\implies \xi = \bar{\lambda} U^t \xi$$
$$\implies U^t \xi = \lambda \xi$$

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, and we have the following result:

THEOREM 4.5. The real and complex bistochastic groups, which are the sets

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

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

PROOF. Let us pick a unitary 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:

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

Observe that such matrices $F \in U_N$ exist indeed, the basic example being the normalized Fourier matrix F_N/\sqrt{N} . We have then, by using the above property of F:

$$\begin{split} u\xi &= \xi & \Longleftrightarrow \quad uFe_0 = Fe_0 \\ & \Leftrightarrow \quad F^* uFe_0 = e_0 \\ & \Leftrightarrow \quad F^* uF = diag(1,w) \end{split}$$

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

At a more advanced level now, let us begin with some geometric preliminaries. The complex projective space appears by definition as follows:

$$P_{\mathbb{C}}^{N-1} = \left(\mathbb{C}^N - \{0\}\right) / \langle x = \lambda y \rangle$$

Inside this projective space, we have the Clifford torus, constructed as follows:

$$\mathbb{T}^{N-1} = \left\{ (z_1, \dots, z_N) \in P_{\mathbb{C}}^{N-1} \Big| |z_1| = \dots = |z_N| \right\}$$

With these conventions, we have the following result, from [53]:

PROPOSITION 4.6. For a unitary matrix $U \in U_N$, the following are equivalent:

- (1) There exist $L, R \in U_N$ diagonal such that U' = LUR is bistochastic.
- (2) The standard torus $\mathbb{T}^N \subset \mathbb{C}^N$ satisfies $\mathbb{T}^N \cap U\mathbb{T}^N \neq \emptyset$. (3) The Clifford torus $\mathbb{T}^{N-1} \subset P_{\mathbb{C}}^{N-1}$ satisfies $\mathbb{T}^{N-1} \cap U\mathbb{T}^{N-1} \neq \emptyset$.

4. SYMPLECTIC GROUPS

PROOF. These equivalences are all elementary, as follows:

(1) \implies (2) Assuming that U' = LUR is bistochastic, which in terms of the all-1 vector ξ means $U'\xi = \xi$, if we set $f = R\xi \in \mathbb{T}^N$ we have:

$$Uf = \bar{L}U'\bar{R}f = \bar{L}U'\xi = \bar{L}\xi \in \mathbb{T}^N$$

Thus we have $Uf \in \mathbb{T}^N \cap U\mathbb{T}^N$, which gives the conclusion.

(2) \implies (1) Given $g \in \mathbb{T}^N \cap U\mathbb{T}^N$, we can define R, L as follows:

$$R = \begin{pmatrix} g_1 & & \\ & \ddots & \\ & & g_N \end{pmatrix} \quad , \quad \bar{L} = \begin{pmatrix} (Ug)_1 & & \\ & \ddots & \\ & & (Ug)_N \end{pmatrix}$$

With these values for L, R, we have then the following formulae:

$$R\xi = g$$
 , $\bar{L}\xi = Ug$

Thus the matrix U' = LUR is bistochastic, because:

$$U'\xi = LUR\xi = LUg = \xi$$

(2) \implies (3) This is clear, because $\mathbb{T}^{N-1} \subset P_{\mathbb{C}}^{N-1}$ appears as the projective image of $\mathbb{T}^N \subset \mathbb{C}^N$, and so $\mathbb{T}^{N-1} \cap U\mathbb{T}^{N-1}$ appears as the projective image of $\mathbb{T}^N \cap U\mathbb{T}^N$.

(3) \implies (2) We have indeed the following equivalence:

$$\mathbb{T}^{N-1} \cap U\mathbb{T}^{N-1} \neq \emptyset \iff \exists \lambda \neq 0, \lambda \mathbb{T}^N \cap U\mathbb{T}^N \neq \emptyset$$

But $U \in U_N$ implies $|\lambda| = 1$, and this gives the result.

The point now is that the condition (3) above is something familiar in symplectic geometry, and known to hold for any $U \in U_N$. Thus, following [53], we have:

THEOREM 4.7. Any unitary matrix $U \in U_N$ can be put in bistochastic form,

$$U' = LUR$$

with $L, R \in U_N$ being both diagonal, via a certain non-explicit method.

PROOF. As already mentioned, the condition $\mathbb{T}^{N-1} \cap U\mathbb{T}^{N-1} \neq \emptyset$ in Proposition 4.6 (3) is something quite natural in symplectic geometry. To be more precise:

(1) The Clifford torus $\mathbb{T}^{N-1} \subset P_{\mathbb{C}}^{N-1}$ is a Lagrangian submanifold, and the map $\mathbb{T}^{N-1} \to U\mathbb{T}^{N-1}$ is a Hamiltonian isotopy. For more on this, see Arnold [2].

(2) The point now is that a non-trivial result of Biran-Entov-Polterovich and Cho states that \mathbb{T}^{N-1} cannot be displaced from itself via a Hamiltonian isotopy.

(3) Thus, we are led to the conclusion that $\mathbb{T}^{N-1} \cap U\mathbb{T}^{N-1} \neq \emptyset$ holds indeed, for any $U \in U_N$. We therefore obtain the result, via Proposition 4.6. See [53].

4B. SYMPLECTIC GROUPS

4b. Symplectic groups

Moving ahead now, as yet another basic example of a continuous group, which is of key importance, we have the symplectic group Sp_N . Let us begin with:

DEFINITION 4.8. The "super-space" $\overline{\mathbb{C}}^N$ 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:

 $i \rightarrow \overline{i}$

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:

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

4. SYMPLECTIC GROUPS

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 4.9. 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 $\overline{O}_N = O_N$.
- (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 $U = J\overline{U}J^{-1} =$ unitary simply read:

$$V = V =$$
unitary

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

Regarding now Sp_N , we have the following result:

62

THEOREM 4.10. The symplectic group $Sp_N \subset U_N$, which is by definition

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

consists of the SU_2 patterned matrices,

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

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.

4c. Reflections, again

As a last topic of discussion, now that we have a decent understanding of the main continuous groups of unitary matrices $G \subset U_N$, let us go back to the finite groups from the previous chapter, and make a link with the material there. We first have:

THEOREM 4.11. 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 chapter 3, appearing as the $s = \infty$ particular case of the results established there for the complex reflection groups H_N^s . \Box

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 4.12. 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:

4. SYMPLECTIC GROUPS

THEOREM 4.13. 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 4.14. 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. \Box

4d. Generation questions

Getting back now to our goal, namely mixing continuous and finite subgroups $G \subset U_N$, consider the following diagram, formed by the main rotation and reflection groups:



We know from the above that this is an intersection and generation diagram. Now assume that we have an intermediate compact group, as follows:

$$H_N \subset G_N \subset U_N$$

The point is that we can think of this group as living inside the above square, and so project it on the edges, as to obtain information about it. Indeed, let us start with:

DEFINITION 4.15. Associated to any closed subgroup $G_N \subset U_N$ are its discrete, real, unitary and smooth versions, given by the formulae

$$G_N^d = G_N \cap K_N \quad , \quad G_N^r = G_N \cap O_N$$
$$G_N^u = \langle G_N, K_N \rangle \quad , \quad G_N^s = \langle G_N, O_N \rangle$$

with <,> being the topological generation operation.

Assuming now that we have an intermediate compact group $H_N \subset G_N \subset U_N$, as above, we are led in this way to the following notion:

DEFINITION 4.16. A compact group $H_N \subset G_N \subset U_N$ is called oriented if



is an intersection and generation diagram.

This notion is quite interesting, because most of our basic examples of closed subgroups $G_N \subset U_N$, finite or continuous, are oriented. Moreover, the world of oriented groups is quite rigid, due to either of the following conditions, which must be satisfied:

$$G_N = \langle G_N^d, G_N^r \rangle \quad , \quad G_N = G_N^u \cap G_N^s$$

Summarizing, we are naturally led in this way to the following question, which is certainly interesting, and is related to all that has been said above, about groups:

QUESTION 4.17. What are the oriented groups $H_N \subset G_N \subset U_N$? What about the oriented groups coming in families, $G = (G_N)$, with $N \in \mathbb{N}$?

And we will stop here our discussion, sometimes a good question is better as hunting trophy than a final theorem, or at least that's what my cats say.

We will be back to this questions, which are quite interesting, later in this book, under a number of supplementary assumptions on the groups that we consider, which will allow us to derive a number of classification results. More on this later.

4. SYMPLECTIC GROUPS

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

Another night, another dream But always you It's like a vision of love That seems to be true

CHAPTER 5

Representations

5a. Basic theory

We have seen so far that some algebraic theory for the finite subgroups $G \subset U_N$, ranging from elementary to quite advanced, can be developed. We have seen as well a few results and computations for the continuous compact subgroups $G \subset U_N$. In what follows we develop some systematic theory for the arbitrary closed subgroups $G \subset U_N$, covering both the finite and the infinite case.

The main notion that we will be interested in is that of a representation:

DEFINITION 5.1. A representation of a compact group G is a continuous group morphism, which can be faithful or not, into a unitary group:

$$u: G \to U_N$$

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 basic example here, for any compact group we always have available the trivial 1-dimensional representation, which is by definition as follows:

$$u: G \to U_1 \quad , \quad g \to (1)$$

At the level of non-trivial examples now, 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:

$$u: G \subset U_N \quad , \quad g \to g$$

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 is as follows:

5. REPRESENTATIONS

PROPOSITION 5.2. The representations of a given compact group G are subject to the following operations:

- (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. All this is elementary, and 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:

$$[(g \otimes h)(g \otimes h)^*]_{ia,jb} = \sum_{kc} (g \otimes h)_{ia,kc} ((g \otimes h)^*)_{kc,jb}$$
$$= \sum_{kc} (g \otimes h)_{ia,kc} \overline{(g \otimes h)_{jb,kc}}$$
$$= \sum_{kc} g_{ik} h_{ac} \overline{g}_{jk} \overline{h}_{bc}$$
$$= \sum_{k} g_{ik} \overline{g}_{jk} \sum_{c} h_{ac} \overline{h}_{bc}$$
$$= \delta_{ij} \delta_{ab}$$

(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. \Box

5A. BASIC THEORY

In relation now with characters, we have the following result:

PROPOSITION 5.3. We have the following formulae, regarding characters

 $\chi_{u+v} = \chi_u + \chi_v \quad , \quad \chi_{u\otimes v} = \chi_u \chi_v \quad , \quad \chi_{\bar{u}} = \bar{\chi}_u \quad , \quad \chi_{VuV^*} = \chi_u$

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:

$$\begin{aligned} Tr(diag(g,h)) &= Tr(g) + Tr(h) \quad , \quad Tr(g \otimes h) = Tr(g)Tr(h) \\ Tr(\bar{g}) &= \overline{Tr(g)} \quad , \quad Tr(VgV^*) = Tr(g) \end{aligned}$$

To be more precise, the first formula is clear from definitions. Regarding now the second formula, the computation here is immediate too, as follows:

$$Tr(g \otimes h) = \sum_{ia} (g \otimes h)_{ia,ia}$$
$$= \sum_{ia} g_{ii}h_{aa}$$
$$= Tr(q)Tr(h)$$

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 closed subgroup $G \subset U_N$. By using the above operations, we can construct a whole family of representations of G, as follows:

DEFINITION 5.4. Given a closed subgroup $G \subset U_N$, its Peter-Weyl representations are the tensor products between the fundamental representation and its conjugate:

$$u: G \subset U_N$$
 , $\bar{u}: G \subset U_N$

We denote these tensor products $u^{\otimes k}$, with $k = \circ \bullet \circ \circ \ldots$ being a colored integer, with the colored tensor powers being defined according to the rules

$$u^{\otimes \circ} = u$$
 , $u^{\otimes \bullet} = \bar{u}$, $u^{\otimes kl} = u^{\otimes k} \otimes u^{\otimes l}$

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:

$$\begin{split} u^{\otimes \circ \circ} &= u \otimes u \quad , \quad u^{\otimes \circ \bullet} = u \otimes \bar{u} \\ u^{\otimes \bullet \circ} &= \bar{u} \otimes u \quad , \quad u^{\otimes \bullet \bullet} = \bar{u} \otimes \bar{u} \end{split}$$

In relation now with characters, we have the following result:

5. REPRESENTATIONS

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

$$\chi^{\circ} = \chi$$
 , $\chi^{\bullet} = \bar{\chi}$, $\chi^{kl} = \chi^k \chi^l$

and with the convention that χ^{\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. \Box

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 compact 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 $End(u) = \mathbb{C}1$.

The terminology here is standard, with Hom and End standing 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:

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:

$$(S \otimes T)(u_g \otimes w_g) = Su_g \otimes Tw_g$$

= $v_g S \otimes t_g T$
= $(v_g \otimes t_g)(S \otimes T)$

(3) This follows from the following computation, valid for any $g \in G$:

$$\begin{array}{rcl} Tu_g = v_g T & \Longrightarrow & u_g^* T^* = T^* v_g^* \\ & \Longrightarrow & T^* v_g = u_g T^* \end{array}$$

(4) This is just a 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 chapter 6 below, with more details on all this.

The above result is quite interesting, because it shows that the combinatorics of a compact group G is described by a certain collection of linear spaces, which can be in principle investigated by using tools from linear algebra. Thus, what we have here is a "linearization" idea. We will heavily use this idea, in what follows.

5b. Peter-Weyl theory

In what follows we develop a systematic theory of the representations of the compact groups G, with emphasis on the Peter-Weyl representations, in the closed subgroup case $G \subset U_N$, that we are mostly interested in. We first have the following result:

THEOREM 5.8. Given a representation of a compact group $u : G \to U_N$, the corresponding linear space of self-intertwiners

$$End(u) \subset M_N(\mathbb{C})$$

is a *-algebra, with respect to the usual involution of the matrices.

PROOF. By definition, the space End(u) is a linear subspace of $M_N(\mathbb{C})$. We know from Theorem 5.7 (1) that this subspace End(u) is a subalgebra of $M_N(\mathbb{C})$, and then 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. \Box

The above result is quite interesting, because it gets us into linear algebra. Indeed, associated to any group representation $u: G \to U_N$ is now a quite familiar object, namely the algebra $End(u) \subset M_N(\mathbb{C})$. In order to exploit this fact, we will need a well-known result, complementing the basic operator algebra theory that we know, namely:

THEOREM 5.9. Let $A \subset M_N(\mathbb{C})$ be a *-algebra.

(1) The unit decomposes as follows, with $p_i \in A$ being central minimal projections:

 $1 = p_1 + \ldots + p_k$

(2) Each of the following linear spaces is a non-unital *-subalgebra of A:

 $A_i = p_i A p_i$

(3) We have a non-unital *-algebra sum decomposition, as follows:

 $A = A_1 \oplus \ldots \oplus A_k$

(4) We have unital *-algebra isomorphisms as follows, with $n_i = rank(p_i)$:

 $A_i \simeq M_{n_i}(\mathbb{C})$

(5) Thus, we have a *-algebra isomorphism as follows:

 $A \simeq M_{n_1}(\mathbb{C}) \oplus \ldots \oplus M_{n_k}(\mathbb{C})$

Moreover, the final conclusion holds in fact for any finite dimensional C^* -algebra.

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 $p_i^2 = p_i^* = p_i$.

<u>Step 2</u>. 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. Finally, in what regards the last assertion, that we will not really need in what follows, this can be deduced from what we have, by using the GNS representation theorem. Indeed, assuming that A is a finite dimensional C^* -algebra, that theorem gives an embedding as follows:

$$A \subset \mathcal{L}(A) \simeq M_N(\mathbb{C}) \quad , \quad N = \dim A$$

Thus, our algebra is a *-subalgebra of $M_N(\mathbb{C})$, and we get the result.

Many other things can be said here, and we will be back to this in chapter 6.

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 group representation, consider the algebra A = End(u), and write its unit as above, as follows:

$$1 = p_1 + \ldots + p_k$$

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:

$$pu_q p = u_q p$$
 , $\forall g \in G$

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:

$$tr[(PU - UP)(PU - UP)^*] = tr[(PU - UP)(U^*P - PU^*)]$$

= $tr[P - PUPU^* - UPU^*P + UPU^*]$
= $tr[P - UPU^* - UPU^* + UPU^*]$
= $tr[P - UPU^*]$
= 0

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. \Box

In order to formulate our second Peter-Weyl theorem, we need to talk about coefficients, and smoothness. Things here are quite tricky, and we can proceed as follows:

DEFINITION 5.11. Given a closed 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:

$$C_v = span \left[g \to (v_g)_{ij} \right]$$

We say that v is smooth if its matrix coefficients $g \to (v_g)_{ij}$ appear as polynomials in the standard matrix coordinates $g \to g_{ij}$, and their conjugates $g \to \overline{g}_{ij}$.

As a basic example of coefficient we have, besides the matrix coefficients $g \to (v_g)_{ij}$, the character, which appears as the diagonal sum of these coefficients:

$$\chi_v(g) = \sum_i (v_g)_{ii}$$

Regarding the notion of smoothness, things are quite tricky here, the idea being that any closed subgroup $G \subset U_N$ can be shown to be a Lie group, and that, with this result in hand, a representation $v: G \to U_M$ is smooth precisely when the condition on coefficients from the above definition is satisfied. All this is quite technical, and we will not get into it. We will simply use Definition 5.11 as such, and further comment on this later on. Here is now our second Peter-Weyl theorem, complementing Theorem 5.10:

THEOREM 5.12 (PW2). Given a closed subgroup $G \subset_u U_N$, any of its irreducible smooth representations

$$v: G \to U_M$$

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) Our smoothness assumption on $v : G \to U_M$, as formulated in Definition 5.11, means that we have an inclusion of linear spaces as follows:

$$C_v \subset \langle g_{ij} \rangle$$

(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. \Box

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. Haar integration

In order to further advance, and complete the Peter-Weyl theory, we need to talk about integration over G. In the 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.

In the continuous group case now, the simplest examples, to be studied first, are the compact abelian groups. Here things are standard again, as follows:

THEOREM 5.14. Given a compact abelian group G, with dual group denoted $\Gamma = \hat{G}$, we have an isomorphism of commutative algebras

$$C(G) \simeq C^*(\Gamma)$$

and via this isomorphism, the functional defined by linearity and the following formula,

$$\int_G g = \delta_{g_1}$$

for any $g \in \Gamma$, is the integration with respect to the unique uniform measure on G.

5C. HAAR INTEGRATION

PROOF. This is something that we basically know, from chapters 8 and 9, coming as a consequence of the general results regarding the abelian groups and the commutative C^* -algebras developed there. To be more precise, and skipping some details here, the conclusions in the statement can be deduced as follows:

(1) We can either apply the Gelfand theorem, from operator algebras, to the group algebra $C^*(\Gamma)$, which is commutative, and this gives all the results.

(2) Or, we can use decomposition results for the compact abelian groups from chapter 9, and by reducing things to summands, once again we obtain the results. \Box

Summarizing, we have results in the finite case, and in the compact abelian case. With the remark that the proof in the compact abelian case was quite brief, but this result, coming as an illustration for more general things to follow, is not crucial for us. Let us discuss now the construction of the uniform probability measure in general. This is something quite technical, the idea being that the uniform measure μ over G can be constructed by starting with an arbitrary probability measure ν , and setting:

$$\mu = \lim_{n \to \infty} \frac{1}{n} \sum_{k=1}^{n} \nu^{*k}$$

Thus, our next task will be that of proving this result. It is convenient, for this purpose, to work with the integration functionals with respect to the various measures on G, instead of the measures themselves. Let us begin with the following key result:

PROPOSITION 5.15. 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:

$$((id \otimes \varphi^{*k})v)_{i_0i_{k+1}} = \sum_{i_1\dots i_k} M_{i_0i_1}\dots M_{i_ki_{k+1}} = (M^k)_{i_0i_{k+1}}$$

Thus we have the following formula, for any $k \in \mathbb{N}$:

$$(id \otimes \varphi^{*k})v = M'$$

It follows that our Cesàro limit is given by the following formula:

$$\lim_{n \to \infty} \frac{1}{n} \sum_{k=1}^{n} \varphi^{*k}(f) = \lim_{n \to \infty} \frac{1}{n} \sum_{k=1}^{n} \tau(M^k)$$
$$= \tau \left(\lim_{n \to \infty} \frac{1}{n} \sum_{k=1}^{n} M^k \right)$$

Now since v is unitary we have ||v|| = 1, and so $||M|| \le 1$. 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 5.16. 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 $Fix(v) = \{\xi \in \mathbb{C}^n | v\xi = \xi\}.$

PROOF. In view of Proposition 5.15, 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:

$$v\xi = \xi \implies M\xi = \xi$$

80

"C" 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:

$$f = \sum_{ijk} v_{ij} v_{ik}^* \xi_j \bar{\xi}_k - \frac{1}{N} v_{ij} \xi_j \bar{\xi}_i - \frac{1}{N} v_{ik}^* \xi_i \bar{\xi}_k + \frac{1}{N^2} \xi_i \bar{\xi}_i$$

$$= \sum_j |\xi_j|^2 - \sum_{ij} v_{ij} \xi_j \bar{\xi}_i - \sum_{ik} v_{ik}^* \xi_i \bar{\xi}_k + \sum_i |\xi_i|^2$$

$$= ||\xi||^2 - \langle v\xi, \xi \rangle - \langle v\xi, \xi \rangle + ||\xi||^2$$

$$= 2(||\xi||^2 - Re(\langle v\xi, \xi \rangle))$$

By using now our assumption $M\xi = \xi$, we obtain from this:

$$\begin{aligned} \varphi(f) &= 2\varphi(||\xi||^2 - Re(\langle v\xi, \xi \rangle)) \\ &= 2(||\xi||^2 - Re(\langle M\xi, \xi \rangle)) \\ &= 2(||\xi||^2 - ||\xi||^2) \\ &= 0 \end{aligned}$$

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 5.17. Any compact 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 $Fix(v) = \{\xi \in \mathbb{C}^n | v\xi = \xi\}.$

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 5.15. 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:

$$\int_{\varphi} \ast \varphi = \varphi \ast \int_{\varphi} = \int_{\varphi}$$

In the case where φ is assumed to be faithful, as in Proposition 5.16, 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 5.16, 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 $\int_G = \int_{\omega}$:

$$\left(\int_{G} \otimes id\right) \Delta = \left(id \otimes \int_{G}\right) \Delta = \int_{G} (.)1$$

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:

$$\left(\int_{G} \otimes \int_{G}^{\prime}\right) \Delta = \left(\int_{G}^{\prime} \otimes \int_{G}\right) \Delta = \int_{G} (.)1 = \int_{G}^{\prime} (.)1$$

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 5.18. Given a compact 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 5.17. If we denote by P the projection onto Fix(v), that formula gives, as desired:

$$\int_{G} \chi_{v} = Tr(P)$$

= dim(Im(P))
= dim(Fix(v))

(2) This follows from (1), applied to the Peter-Weyl representations, as follows:

$$\int_{G} \chi^{k} = \int_{G} \chi^{k}_{u}$$
$$= \int_{G} \chi_{u^{\otimes k}}$$
$$= \dim(Fix(u^{\otimes k}))$$

(3) This follows from (2), and from the standard fact, which follows from definitions, that a probability measure is uniquely determined by its moments. \Box

As a key remark now, the integration formula in Theorem 5.17 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 5.19. Given a closed subgroup $G \subset U_N$, the quantities

$$I_k = \int_G g_{i_1 j_1}^{e_1} \dots g_{i_k j_k}^{e_k} \, dg$$

depending on a colored integer $k = e_1 \dots e_k$, 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:

$$C(G) = \langle g_{ij} \rangle$$

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 5.20. 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

$$\int_G g_{i_1 j_1}^{e_1} \dots g_{i_k j_k}^{e_k} dg = \sum_{\pi, \sigma \in D_k} \delta_{\pi}(i) \delta_{\sigma}(j) W_k(\pi, \sigma)$$

valid for any colored integer $k = e_1 \dots e_k$ 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:

$$E(x) = \sum_{\pi \in D_k} \langle x, \xi_\pi \rangle \xi_\pi$$

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 IV below, with some concrete applications.

5d. More Peter-Weyl

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 5.21. 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:

$$\begin{array}{lll} T \in Hom(v,w) & \Longleftrightarrow & Tv = wT \\ & \Longleftrightarrow & \sum_{j} T_{aj}v_{ji} = \sum_{b} w_{ab}T_{bi}, \forall a,i \end{array}$$

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

$$T \in Fix(v \otimes \bar{w}) \iff (v \otimes \bar{w})T = \xi$$
$$\iff \sum_{jb} v_{ij}w_{ab}^*T_{bj} = T_{ai} \forall a, i$$

With these formulae in hand, both inclusions follow from the unitarity of v, w. \Box We can now formulate our third Peter-Weyl theorem, as follows:

THEOREM 5.22 (PW3). The norm dense *-subalgebra

 $\mathcal{C}(G) \subset C(G)$

generated by the coefficients of the fundamental representation decomposes as

$$\mathcal{C}(G) = \bigoplus_{v \in Irr(G)} M_{\dim(v)}(\mathbb{C})$$

with the summands being pairwise orthogonal with respect to the scalar product

$$\langle a,b \rangle = \int_{G} ab^*$$

where \int_G is the Haar integration over G.

PROOF. By combining the previous two Peter-Weyl results, we deduce that we have a linear space decomposition as follows:

$$\mathcal{C}(G) = \sum_{v \in Irr(G)} C_v = \sum_{v \in Irr(G)} M_{\dim(v)}(\mathbb{C})$$

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:

$$v \not\sim w \implies C_v \perp C_w$$

But this follows from Theorem 5.17, via Proposition 5.21. 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 5.23 (PW4). The characters of irreducible representations belong to

$$\mathcal{C}(G)_{central} = \left\{ f \in \mathcal{C}(G) \middle| f(gh) = f(hg), \forall g, h \in G \right\}$$

called algebra of smooth 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 $\mathcal{C}(G)_{central}$ is indeed an algebra, which contains all the characters. Conversely, consider a function $f \in \mathcal{C}(G)$, written as follows:

$$f = \sum_{v \in Irr(G)} f_v$$

86

The condition $f \in \mathcal{C}(G)_{central}$ states then that for any $v \in Irr(G)$, we must have:

$$f_v \in \mathcal{C}(G)_{central}$$

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 $\mathcal{C}(G)_{central}$, as stated.

(2) The fact that we have an orthogonal basis follows from Theorem 5.22.

(3) As for the fact that the characters have norm 1, this follows from:

$$\int_{G} \chi_{v} \chi_{v}^{*} = \sum_{ij} \int_{G} v_{ii} v_{jj}^{*}$$
$$= \sum_{i} \frac{1}{N}$$
$$= 1$$

Here we have used the fact, coming from Theorem 5.22, that the 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.

As a key observation here, complementing Theorem 5.23, 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.

So long for Peter-Weyl theory. As a basic illustration for all this, which clarifies some previous considerations from chapter 1, we have the following result:

THEOREM 5.24. 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 $\chi_u \in \widehat{G}$. \Box

There are also many things that can be said in the finite group case, in relation with central functions, and conjugacy classes. For more here, we recommend Serre [85].

5e. Exercises

Exercises:

EXERCISE 5.25.

EXERCISE 5.26.

EXERCISE 5.27.

Exercise 5.28.

EXERCISE 5.29.

Exercise 5.30.

Exercise 5.31.

Exercise 5.32.

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 $T \in C_{kl}$:

$$T(gh)^{\otimes k} = Tg^{\otimes k}h^{\otimes k}$$
$$= g^{\otimes l}Th^{\otimes k}$$
$$= g^{\otimes l}h^{\otimes l}T$$
$$= (gh)^{\otimes l}T$$

Also, we have $1 \in \widetilde{G}$, trivially. Finally, assuming $g \in \widetilde{G}$, we have:

$$T(g^{-1})^{\otimes k} = (g^{-1})^{\otimes l} [g^{\otimes l}T](g^{-1})^{\otimes k}$$

= $(g^{-1})^{\otimes l} [Tg^{\otimes k}](g^{-1})^{\otimes k}$
= $(g^{-1})^{\otimes l}T$

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

$$C_{kl} = \left\{ T \in \mathcal{L}(H^{\otimes k}, H^{\otimes l}) \middle| \exists g \in G, g_{i_1} \dots g_{i_k} \neq g_{j_1} \dots g_{j_l} \implies T_{j_1 \dots j_l, i_1 \dots i_k} = 0 \right\}$$

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:

 $g = \pm 1$

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 $\tilde{G} = \{1\}$, 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:

$$Tg^{\otimes k} = g^{\otimes l}T$$

6A. GENERALITIES

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:

$$T \in C_{kl} \iff Tg^{\otimes k} = g^{\otimes l}T, \forall g \in G$$

$$\iff (Tg^{\otimes k})_{ji} = (g^{\otimes l}T)_{ji}, \forall i, j, \forall g \in G$$

$$\iff T_{j_1\dots,j_l,i_1\dots i_k}g_{i_1}\dots g_{i_k} = g_{j_1}\dots g_{j_l}T_{j_1\dots,j_k,i_1\dots i_l}, \forall i, j, \forall g \in G$$

$$\iff (g_{j_1}\dots g_{i_k} - g_{j_1}\dots g_{j_l})T_{j_1\dots,j_l,i_1\dots i_k}, \forall i, j, \forall g \in G$$

Thus, we are led to the formula in the statement, namely:

$$C_{kl} = \left\{ T \in \mathcal{L}(H^{\otimes k}, H^{\otimes l}) \middle| \exists g \in G, g_{i_1} \dots g_{i_k} \neq g_{j_1} \dots g_{j_l} \implies T_{j_1 \dots j_l, i_1 \dots i_k} = 0 \right\}$$

(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:

$$g_{i_1} \dots g_{i_k} = g_{j_1} \dots g_{j_l}, \forall g \in G \iff \{i_1, \dots, i_k\}_2 = \{j_1, \dots, j_l\}_2$$

Thus, in this case we obtain the following formula, with $\{ \}_2$ being as above:

$$C_{kl} = \left\{ T \in \mathcal{L}(H^{\otimes k}, H^{\otimes l}) \middle| \{i_1, \dots, i_k\}_2 \neq \{j_1, \dots, j_l\}_2 \implies T_{j_1 \dots j_l, i_1 \dots i_k} = 0 \right\}$$

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:

$$g \in G \implies g \in C'_{11} = \Delta' = \Delta$$
$$\implies g \in \Delta \cap O_N = G$$

(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:

$$C_{11} = \left\{ T \in M_N(\mathbb{C}) \middle| T_{ij} = 0 \text{ when } i \le M, j > M \text{ or } i > M, j \le M \right\}$$

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.

6A. GENERALITIES

(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:

$$G_I = \left\{ g \in \mathbb{Z}_2^N \middle| \prod_{i \in I} g_i = 1 \right\}$$

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:

$$C_{kl} = \left\{ T \in \mathcal{L}(H^{\otimes k}, H^{\otimes l}) \middle| \{i_1, \dots, i_k\}_{2I} \neq \{j_1, \dots, j_l\}_{2I} \implies T_{j_1 \dots j_l, i_1 \dots i_k} = 0 \right\}$$

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. \Box

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:

$$G \subset G \subset O_N$$

(2) In order to prove this, consider the Tannakian category of \widetilde{G} , namely:

$$\widetilde{C}_{kl} = \left\{ T \in \mathcal{L}(H^{\otimes k}, H^{\otimes l}) \middle| Tg^{\otimes k} = g^{\otimes l}T, \forall g \in \widetilde{G} \right\}$$

6A. GENERALITIES

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:

$$C(\widetilde{G}) = \bigoplus_{\pi \in Irr(\widetilde{G})} M_{\dim \pi}(\mathbb{C}) \quad , \quad C(G) = \bigoplus_{\nu \in Irr(G)} M_{\dim \nu}(\mathbb{C})$$

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:

$$\pi \in Irr(G) \quad , \quad \pi' \notin Irr(G)$$

(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:

$$\pi \in u^{\otimes k}$$
 , $\pi' \in u'^{\otimes k}$

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 $k = \circ \bullet \circ \circ \ldots$ colored integer, defined by

$$u^{\otimes \emptyset} = 1$$
 , $u^{\otimes \circ} = u$, $u^{\otimes \bullet} = ar{u}$

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:

$$\begin{split} u^{\otimes \circ \circ} &= u \otimes u \quad , \quad u^{\otimes \circ \bullet} = u \otimes \bar{u} \\ u^{\otimes \bullet \circ} &= \bar{u} \otimes u \quad , \quad u^{\otimes \bullet \bullet} = \bar{u} \otimes \bar{u} \end{split}$$

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:

$$C(k,l) = Hom(u^{\otimes k}, u^{\otimes l})$$

$$\simeq Hom(1, \bar{u}^{\otimes k} \otimes u^{\otimes l})$$

$$= Hom(1, u^{\otimes \bar{k}l})$$

$$= Fix(u^{\otimes \bar{k}l})$$

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 $k, l = 0, \bullet$ contain the flip operator $\Sigma : a \otimes b \to b \otimes a$.

6B. TENSOR CATEGORIES

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:

$$H^{\otimes \emptyset} = \mathbb{C}$$
 , $H^{\otimes \circ} = H$, $H^{\otimes \bullet} = \bar{H} \simeq H$

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:

 $R \in Hom(1, g \otimes \overline{g})$, $R \in Hom(1, \overline{g} \otimes g)$

Indeed, given an arbitrary matrix $g \in M_N(\mathbb{C})$, we have the following computation:

$$(g \otimes \bar{g})(R(1) \otimes 1) = \left(\sum_{ijkl} e_{ij} \otimes e_{kl} \otimes g_{ij}\bar{g}_{kl}\right) \left(\sum_{a} e_{a} \otimes e_{a} \otimes 1\right)$$
$$= \sum_{ika} e_{i} \otimes e_{k} \otimes g_{ia}\bar{g}_{ka}^{*}$$
$$= \sum_{ik} e_{i} \otimes e_{k} \otimes (gg^{*})_{ik}$$

We conclude from this that we have the following equivalence:

 $R \in Hom(1, g \otimes \bar{g}) \quad \Longleftrightarrow \quad gg^* = 1$

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:

$$(g \otimes h)(\Sigma \otimes id)(e_a \otimes e_b \otimes 1) = \left(\sum_{ijkl} e_{ij} \otimes e_{kl} \otimes g_{ij}h_{kl}\right)(e_b \otimes e_a \otimes 1)$$
$$= \sum_{ik} e_i \otimes e_k \otimes g_{ib}h_{ka}$$

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

$$\begin{split} (\Sigma \otimes id)(h \otimes g)(e_a \otimes e_b \otimes 1) &= (\Sigma \otimes id) \left(\sum_{ijkl} e_{ij} \otimes e_{kl} \otimes h_{ij}g_{kl} \right) (e_a \otimes e_b \otimes 1) \\ &= (\Sigma \otimes id) \left(\sum_{ik} e_i \otimes e_k \otimes h_{ia}g_{kb} \right) \\ &= \sum_{ik} e_k \otimes e_i \otimes h_{ia}g_{kb} \\ &= \sum_{ik} e_i \otimes e_k \otimes h_{ka}g_{ib} \end{split}$$

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 $G \rightarrow C$ 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 $T \in C(k, l)$:

$$T(gh)^{\otimes k} = Tg^{\otimes k}h^{\otimes k}$$
$$= g^{\otimes l}Th^{\otimes k}$$
$$= g^{\otimes l}h^{\otimes l}T$$
$$= (gh)^{\otimes l}T$$

(2) Also, we have $1 \in G$, trivially. Finally, for $g \in G$ and $T \in C(k, l)$, we have:

$$T(g^{-1})^{\otimes k} = (g^{-1})^{\otimes l} [g^{\otimes l}T](g^{-1})^{\otimes k}$$

= $(g^{-1})^{\otimes l} [Tg^{\otimes k}](g^{-1})^{\otimes k}$
= $(g^{-1})^{\otimes l}T$

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,

$$G \subset G_{C_G}$$
 , $C \subset C_{G_C}$

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,

$$E_C^{(s)} = \bigoplus_{|k|,|l| \le s} C(k,l) \subset \bigoplus_{|k|,|l| \le s} B(H^{\otimes k},H^{\otimes l}) = B\left(\bigoplus_{|k| \le s} H^{\otimes k}\right)$$

is a finite dimensional *-subalgebra.

PROOF. This is clear indeed from the categorical axioms from Definition 6.9. \Box

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, $X' = \{T \in M_N(\mathbb{C}) | Tx = xT, \forall x \in X\}.$

PROOF. This is a particular case of von Neumann's bicommutant theorem, which follows from the explicit description of A worked out in chapter 5, 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,

$$E_{C_G}^{(s)} = End\left(\bigoplus_{|k| \le s} u^{\otimes k}\right)$$

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:

$$E_{C_G}^{(s)} = \bigoplus_{|k|,|l| \le s} Hom(u^{\otimes k}, u^{\otimes l}) \subset \bigoplus_{|k|,|l| \le s} B(H^{\otimes k}, H^{\otimes l}) = B\left(\bigoplus_{|k| \le s} H^{\otimes k}\right)$$

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:

$$(\pi_v(\varphi * \psi))_{ij} = (\varphi \otimes \psi) \Delta(v_{ij})$$

= $\sum_k \varphi(v_{ik}) \psi(v_{kj})$
= $\sum_k (\pi_v(\varphi))_{ik} (\pi_v(\psi))_{kj}$
= $(\pi_v(\varphi) \pi_v(\psi))_{ij}$

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:

$$[\pi_{v}(\varphi), T] = 0 \iff \sum_{k} \varphi(v_{ik}) T_{kj} = \sum_{k} T_{ik} \varphi(v_{kj}), \forall i, j$$
$$\iff \varphi\left(\sum_{k} v_{ik} T_{kj}\right) = \varphi\left(\sum_{k} T_{ik} v_{kj}\right), \forall i, j$$
$$\iff \varphi((vT)_{ij}) = \varphi((Tv)_{ij}), \forall i, j$$

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:

$$T \in Im(\pi_v)' \iff [\pi_v(\varphi), T] = 0, \forall \varphi$$
$$\iff \varphi((vT)_{ij}) = \varphi((Tv)_{ij}), \forall \varphi, i, j$$
$$\iff vT = Tv$$

Thus, we have obtained the desired inclusion, and we are done.

By combining the above results, we obtain the following technical statement:

102

THEOREM 6.18. We have the following equality,

$$E_{C_G}^{(s)'} = Im(\pi_v)$$

where the representation v is the following direct sum,

$$v = \bigoplus_{|k| \le s} u^{\otimes k}$$

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. $\hfill \Box$

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 $\langle u_{ij} \rangle$ 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,

$$F = \bigoplus_{k} B(H^{\otimes k})$$
, $F^* = \bigoplus_{k} B(H^{\otimes k})^*$

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 $\langle u_{ij} \rangle \simeq F^*$, 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:

$$\langle u_{ij} \rangle \simeq F^*$$
 , $u_{ij} \to f_{ij}$, $u_{ij}^* \to f_{ij}^*$

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,

$$\sum_{p_1,\dots,p_k} T_{i_1\dots i_l,p_1\dots p_k} f_{p_1j_1} \otimes \dots \otimes f_{p_kj_k} = \sum_{q_1,\dots,q_l} T_{q_1\dots q_l,j_1\dots j_k} f_{i_1q_1} \otimes \dots \otimes f_{i_lq_l}$$

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:

$$\mathcal{A}_{C} = \left\langle (u_{ij})_{i,j=1,\dots,N} \middle| T \in Hom(u^{\otimes k}, u^{\otimes l}), \forall k, l, \forall T \in C(k,l) \right\rangle$$

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 $\langle u_{ij} \rangle \simeq F^*$ 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 $\langle u_{ij} \rangle$ is equivalent to the following conditions:

$$\sum_{p_1,\dots,p_k} T_{i_1\dots i_l,p_1\dots p_k} u_{p_1j_1}\dots u_{p_kj_k} = \sum_{q_1,\dots,q_l} T_{q_1\dots q_l,j_1\dots j_k} u_{i_1q_1}\dots u_{i_lq_l}$$

Now by recalling that the isomorphism of *-algebras $\langle u_{ij} \rangle \rightarrow F^*$ is given by $u_{ij} \rightarrow f_{ij}$, 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

$$\pi_v: \mathcal{A}_C^* \to B\left(\bigoplus_{|k| \le s} H^{\otimes k}\right)$$

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 $J = \langle f_T \rangle$, 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:

$$f_T(a) = 0$$

$$\iff \sum_{p_1,\dots,p_k} T_{i_1\dots i_l,p_1\dots p_k}(a_k)_{p_1\dots p_k,j_1\dots j_k} = \sum_{q_1,\dots,q_l} T_{q_1\dots q_l,j_1\dots j_k}(a_l)_{i_1\dots i_l,q_1\dots q_l}, \forall i,j$$

$$\iff (Ta_k)_{i_1\dots i_l,j_1\dots j_k} = (a_l T)_{i_1\dots i_l,j_1\dots j_k}, \forall i,j$$

$$\iff Ta_k = a_l T$$

Thus, \mathcal{A}_C^* is given by the formula in the statement. It remains to compute π_v :

$$\pi_v: \mathcal{A}_C^* \to B\left(\bigoplus_{|k| \le s} H^{\otimes k}\right)$$

With $a = (a_k)$, we have the following computation:

$$\pi_v(a)_{i_1\dots i_k, j_1\dots j_k} = a(v_{i_1\dots i_k, j_1\dots j_k})$$

= $(f_{i_1j_1} \otimes \dots \otimes f_{i_kj_k})(a)$
= $(a_k)_{i_1\dots i_k, j_1\dots j_k}$

Thus, our representation π_v appears diagonally, by truncating, as claimed.

In order to further advance, consider the following vector spaces:

$$F_s = \bigoplus_{|k| \le s} B\left(H^{\otimes k}\right) \quad , \quad F_s^* = \bigoplus_{|k| \le s} B\left(H^{\otimes k}\right)^*$$

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:

$$F_s \subset B\left(\bigoplus_{|k| \le s} H^{\otimes k}\right)$$

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 $s \in \mathbb{N}$:

$$J \cap F_s^* = \left\{ f \in F_s^* \middle| f_{|E_C^{(s)'}} = 0 \right\}$$

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 $X = \bigcup_s X_s$ 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:

"C" This follows from the following fact, for any $T \in C(k, l)$ with $|k|, |l| \leq s$:

$$(f_T)_{|\{T\}'} = 0 \implies (f_T)_{|E_C^{(s)'}} = 0$$
$$\implies f_T \in X_s$$

" \supset " This follows from our description of J, because from $E_C^{(s)} \subset E_C$ we obtain:

$$f_{|E_C^{(s)'}} = 0 \implies f_{|E_C'} = 0$$

Summarizing, we have proved our claim. On the other hand, we have:

$$J \cap F_s^* = \left\{ f \in F^* \middle| f_{|E'_C} = 0 \right\} \cap F_s^*$$
$$= \left\{ f \in F_s^* \middle| f_{|E'_C} = 0 \right\}$$
$$= \left\{ f \in F_s^* \middle| f_{|(E'_C)_s} = 0 \right\}$$

Thus, our claim is exactly the inclusion that we wanted to prove, and we are done. \Box

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 ,

$$T_{\pi}(e_{i_1} \otimes \ldots \otimes e_{i_k}) = \sum_{j_1 \dots j_l} \delta_{\pi} \begin{pmatrix} i_1 & \cdots & i_k \\ j_1 & \cdots & j_l \end{pmatrix} e_{j_1} \otimes \ldots \otimes e_{j_l}$$

and with the coefficients on the right being Kronecker type symbols,

$$\delta_{\pi} \begin{pmatrix} i_1 & \dots & i_k \\ j_1 & \dots & j_l \end{pmatrix} \in \{0, 1\}$$

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 $\delta_{\pi}({}^i_j) = 1$. Otherwise, we set $\delta_{\pi}({}^i_j) = 0$.

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) $T_{\cap} = (1 \rightarrow \sum_{i} e_{i} \otimes e_{i}).$ (2) $T_{\cup} = (e_{i} \otimes e_{j} \rightarrow \delta_{ij}).$ (3) $T_{||...||} = id.$ (4) $T_{\chi} = (e_{a} \otimes e_{b} \rightarrow e_{b} \otimes e_{a}).$

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:

$$T_{\cap}(1) = \sum_{ij} \delta_{\cap}(i \ j) e_i \otimes e_j$$
$$= \sum_{ij} \delta_{ij} e_i \otimes e_j$$
$$= \sum_i e_i \otimes e_i$$

(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 $|| \dots || \in P_2(k, k)$, with $k = \circ \circ \dots \circ \circ$. The corresponding linear map is then the identity, because we have:

$$T_{||\dots||}(e_{i_1} \otimes \dots \otimes e_{i_k}) = \sum_{j_1 \dots j_k} \delta_{||\dots||} \begin{pmatrix} i_1 & \dots & i_k \\ j_1 & \dots & j_k \end{pmatrix} e_{j_1} \otimes \dots \otimes e_{j_k}$$
$$= \sum_{j_1 \dots j_k} \delta_{i_1 j_1} \dots \delta_{i_k j_k} e_{j_1} \otimes \dots \otimes e_{j_k}$$
$$= e_{i_1} \otimes \dots \otimes e_{i_k}$$

(4) For the basic crossing $X \in P_2(\circ\circ, \circ\circ)$, 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:

$$T_{\chi}(e_i \otimes e_j) = \sum_{kl} \delta_{\chi} \begin{pmatrix} i & j \\ k & l \end{pmatrix} e_k \otimes e_l$$
$$= \sum_{kl} \delta_{il} \delta_{jk} e_k \otimes e_l$$
$$= e_j \otimes e_i$$

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 assignment $\pi \to T_{\pi}$ is categorical, in the sense that

$$T_{\pi} \otimes T_{\sigma} = T_{[\pi\sigma]}$$
, $T_{\pi}T_{\sigma} = N^{c(\pi,\sigma)}T_{[\sigma]}$, $T_{\pi}^* = T_{\pi}$

where $c(\pi, \sigma)$ is the number of circles appearing in the middle, when concatenating.

PROOF. The concatenation axiom follows from the following computation:

$$(T_{\pi} \otimes T_{\sigma})(e_{i_{1}} \otimes \ldots \otimes e_{i_{p}} \otimes e_{k_{1}} \otimes \ldots \otimes e_{k_{r}})$$

$$= \sum_{j_{1} \dots j_{q}} \sum_{l_{1} \dots l_{s}} \delta_{\pi} \begin{pmatrix} i_{1} & \dots & i_{p} \\ j_{1} & \dots & j_{q} \end{pmatrix} \delta_{\sigma} \begin{pmatrix} k_{1} & \dots & k_{r} \\ l_{1} & \dots & l_{s} \end{pmatrix} e_{j_{1}} \otimes \ldots \otimes e_{j_{q}} \otimes e_{l_{1}} \otimes \ldots \otimes e_{l_{s}}$$

$$= \sum_{j_{1} \dots j_{q}} \sum_{l_{1} \dots l_{s}} \delta_{[\pi\sigma]} \begin{pmatrix} i_{1} & \dots & i_{p} & k_{1} & \dots & k_{r} \\ j_{1} & \dots & j_{q} & l_{1} & \dots & l_{s} \end{pmatrix} e_{j_{1}} \otimes \ldots \otimes e_{j_{q}} \otimes e_{l_{1}} \otimes \ldots \otimes e_{l_{s}}$$

$$= T_{[\pi\sigma]}(e_{i_{1}} \otimes \ldots \otimes e_{i_{p}} \otimes e_{k_{1}} \otimes \ldots \otimes e_{k_{r}})$$

The composition axiom follows from the following computation:

$$T_{\pi}T_{\sigma}(e_{i_{1}}\otimes\ldots\otimes e_{i_{p}})$$

$$=\sum_{j_{1}\ldots j_{q}}\delta_{\sigma}\begin{pmatrix}i_{1}&\ldots&i_{p}\\j_{1}&\ldots&j_{q}\end{pmatrix}\sum_{k_{1}\ldots k_{r}}\delta_{\pi}\begin{pmatrix}j_{1}&\ldots&j_{q}\\k_{1}&\ldots&k_{r}\end{pmatrix}e_{k_{1}}\otimes\ldots\otimes e_{k_{r}}$$

$$=\sum_{k_{1}\ldots k_{r}}N^{c(\pi,\sigma)}\delta_{[\frac{\sigma}{\pi}]}\begin{pmatrix}i_{1}&\ldots&i_{p}\\k_{1}&\ldots&k_{r}\end{pmatrix}e_{k_{1}}\otimes\ldots\otimes e_{k_{r}}$$

$$=N^{c(\pi,\sigma)}T_{[\frac{\sigma}{\pi}]}(e_{i_{1}}\otimes\ldots\otimes e_{i_{p}})$$

6. TANNAKIAN DUALITY

Finally, the involution axiom follows from the following computation:

$$T_{\pi}^{*}(e_{j_{1}} \otimes \ldots \otimes e_{j_{q}})$$

$$= \sum_{i_{1} \ldots i_{p}} < T_{\pi}^{*}(e_{j_{1}} \otimes \ldots \otimes e_{j_{q}}), e_{i_{1}} \otimes \ldots \otimes e_{i_{p}} > e_{i_{1}} \otimes \ldots \otimes e_{i_{p}}$$

$$= \sum_{i_{1} \ldots i_{p}} \delta_{\pi} \begin{pmatrix} i_{1} & \ldots & i_{p} \\ j_{1} & \ldots & j_{q} \end{pmatrix} e_{i_{1}} \otimes \ldots \otimes e_{i_{p}}$$

$$= T_{\pi^{*}}(e_{j_{1}} \otimes \ldots \otimes e_{j_{q}})$$

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, $(\pi, \sigma) \rightarrow [\pi\sigma]$.
- (2) Stability under vertical concatenation $(\pi, \sigma) \to [\sigma]$, 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 $|| \dots ||$.
- (5) The sets $P(\emptyset, \bullet \bullet)$ and $P(\emptyset, \bullet \circ)$ both contain the semicircle \cap .
- (6) The sets $P(k, \bar{k})$ with |k| = 2 contain the crossing partition χ .

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:

$$u^* = u^{-1}$$
 , $u^t = \bar{u}^{-1}$

But these relations tell us precisely that the following two operators must be in the associated Tannakian category C:

$$T_{\pi}$$
 : $\pi = \bigcap_{\circ \bullet}^{\cap}, \bigcap_{\bullet \circ}^{\cap}$

Thus the associated Tannakian category is $C = span(T_{\pi} | \pi \in D)$, with:

$$D = < \cap_{\circ \bullet} , \circ_{\circ \circ} > = \mathcal{P}_2$$

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.

6. TANNAKIAN DUALITY

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:

$$T_{\pi}$$
 : $\pi = 4$,

Thus the associated Tannakian category is $C = span(T_{\pi} | \pi \in D)$, with:

$$D = \langle \mathcal{P}_2, \overset{\circ}{\bullet}, \overset{\circ}{\bullet} \rangle = P_2$$

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 IV, 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 ,

$$T_{\pi}(e_{i_1} \otimes \ldots \otimes e_{i_k}) = \sum_{j_1 \dots j_l} \delta_{\pi} \begin{pmatrix} i_1 & \cdots & i_k \\ j_1 & \cdots & j_l \end{pmatrix} e_{j_1} \otimes \ldots \otimes e_{j_l}$$

and with the coefficients on the right being Kronecker type symbols.

To be more precise here, in order to compute the Kronecker type symbols $\delta_{\pi}(i_j) \in \{0,1\}$, 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 $\delta_{\pi}(i_j) = 1$. Otherwise, we set $\delta_{\pi}(i_j) = 0$.

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.

7A. EASY GROUPS

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, $(\pi, \sigma) \rightarrow [\pi\sigma]$.
- (2) Stability under vertical concatenation $(\pi, \sigma) \to [\frac{\sigma}{\pi}]$, 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 $\| \dots \|$.
- (5) The sets $P(\emptyset, \bullet \bullet)$ and $P(\emptyset, \bullet \circ)$ both contain the semicircle \cap .
- (6) The sets $P(k, \bar{k})$ with |k| = 2 contain the crossing partition χ .

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 assignment $\pi \to T_{\pi}$ is categorical, in the sense that

$$T_{\pi} \otimes T_{\sigma} = T_{[\pi\sigma]}$$
, $T_{\pi}T_{\sigma} = N^{c(\pi,\sigma)}T_{[\frac{\sigma}{\pi}]}$, $T_{\pi}^* = T_{\pi}^*$

where $c(\pi, \sigma)$ are certain integers, coming from the erased components in the middle.

PROOF. This is something that we already know for pairings, and the proof in general is similar. The concatenation axiom follows from the following computation:

$$(T_{\pi} \otimes T_{\sigma})(e_{i_{1}} \otimes \ldots \otimes e_{i_{p}} \otimes e_{k_{1}} \otimes \ldots \otimes e_{k_{r}})$$

$$= \sum_{j_{1} \ldots j_{q}} \sum_{l_{1} \ldots l_{s}} \delta_{\pi} \begin{pmatrix} i_{1} & \ldots & i_{p} \\ j_{1} & \ldots & j_{q} \end{pmatrix} \delta_{\sigma} \begin{pmatrix} k_{1} & \ldots & k_{r} \\ l_{1} & \ldots & l_{s} \end{pmatrix} e_{j_{1}} \otimes \ldots \otimes e_{j_{q}} \otimes e_{l_{1}} \otimes \ldots \otimes e_{l_{s}}$$

$$= \sum_{j_{1} \ldots j_{q}} \sum_{l_{1} \ldots l_{s}} \delta_{[\pi\sigma]} \begin{pmatrix} i_{1} & \ldots & i_{p} & k_{1} & \ldots & k_{r} \\ j_{1} & \ldots & j_{q} & l_{1} & \ldots & l_{s} \end{pmatrix} e_{j_{1}} \otimes \ldots \otimes e_{j_{q}} \otimes e_{l_{1}} \otimes \ldots \otimes e_{l_{s}}$$

$$= T_{[\pi\sigma]}(e_{i_{1}} \otimes \ldots \otimes e_{i_{p}} \otimes e_{k_{1}} \otimes \ldots \otimes e_{k_{r}})$$

The composition axiom follows from the following computation:

$$T_{\pi}T_{\sigma}(e_{i_{1}}\otimes\ldots\otimes e_{i_{p}})$$

$$=\sum_{j_{1}\ldots j_{q}}\delta_{\sigma}\begin{pmatrix}i_{1}&\ldots&i_{p}\\j_{1}&\ldots&j_{q}\end{pmatrix}\sum_{k_{1}\ldots k_{r}}\delta_{\pi}\begin{pmatrix}j_{1}&\ldots&j_{q}\\k_{1}&\ldots&k_{r}\end{pmatrix}e_{k_{1}}\otimes\ldots\otimes e_{k_{r}}$$

$$=\sum_{k_{1}\ldots k_{r}}N^{c(\pi,\sigma)}\delta_{[\pi]}\begin{pmatrix}i_{1}&\ldots&i_{p}\\k_{1}&\ldots&k_{r}\end{pmatrix}e_{k_{1}}\otimes\ldots\otimes e_{k_{r}}$$

$$=N^{c(\pi,\sigma)}T_{[\pi]}(e_{i_{1}}\otimes\ldots\otimes e_{i_{p}})$$

Finally, the involution axiom follows from the following computation:

$$T_{\pi}^{*}(e_{j_{1}} \otimes \ldots \otimes e_{j_{q}})$$

$$= \sum_{i_{1} \ldots i_{p}} < T_{\pi}^{*}(e_{j_{1}} \otimes \ldots \otimes e_{j_{q}}), e_{i_{1}} \otimes \ldots \otimes e_{i_{p}} > e_{i_{1}} \otimes \ldots \otimes e_{i_{p}}$$

$$= \sum_{i_{1} \ldots i_{p}} \delta_{\pi} \begin{pmatrix} i_{1} & \ldots & i_{p} \\ j_{1} & \ldots & j_{q} \end{pmatrix} e_{i_{1}} \otimes \ldots \otimes e_{i_{p}}$$

$$= T_{\pi^{*}}(e_{j_{1}} \otimes \ldots \otimes e_{j_{q}})$$

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.

7A. EASY GROUPS

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 $D = \langle D \rangle$ 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.

117

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:

$$D = < \cap_{\circ \bullet} \cap_{\circ \circ} \cap_{\circ \circ} > = \mathcal{P}_2$$

(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:

$$D = \langle \mathcal{P}_2, \overset{\circ}{\bullet}, \overset{\circ}{\bullet} \rangle = P_2$$

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.

118

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:

$$u\xi = \xi$$
 , $\bar{u}\xi = \xi$

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:

$$T_{\pi}$$
 : $\pi = \downarrow$, \downarrow

Thus the associated Tannakian category is $C = span(T_{\pi} | \pi \in D)$, with:

$$D = \langle \mathcal{P}_2, \downarrow, \downarrow \rangle = \mathcal{P}_{12}$$

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:

$$D = \langle \mathcal{P}_{12}, \mathcal{P}_2 \rangle = \mathcal{P}_{12}$$

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,



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:



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:

$$u = (u_{ij})_{ij}$$
, $u^{\otimes 2} = (u_{ij}u_{kl})_{ik,jl}$, $T_Y = (\delta_{ijk})_{i,jk}$

120

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. \Box

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:

$$(T_H \otimes id)u^{\otimes 2}(e_a \otimes e_b) = (T_H \otimes id) \left(\sum_{ijkl} e_{ij} \otimes e_{kl} \otimes u_{ij}u_{kl}\right) (e_a \otimes e_b)$$
$$= (T_H \otimes id) \left(\sum_{ik} e_i \otimes e_k \otimes u_{ia}u_{kb}\right)$$
$$= \sum_i e_i \otimes e_i \otimes u_{ia}u_{ib}$$

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

$$u^{\otimes 2}(T_H \otimes id)(e_a \otimes e_b) = \delta_{ab} \left(\sum_{ijkl} e_{ij} \otimes e_{kl} \otimes u_{ij}u_{kl} \right) (e_a \otimes e_a)$$
$$= \delta_{ab} \sum_{ij} e_i \otimes e_k \otimes u_{ia}u_{ka}$$

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:

$$D = \langle H \rangle$$

But the category on the right can be computed by drawing pictures, and we have:

$$\langle H \rangle = P_{even}$$

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,



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:



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].

123

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: $\langle H, K \rangle$ 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 $\langle H, K \rangle$ are given by the following formulae,

$$C(H \cap K) = C(U_N) / \langle I, J \rangle$$
$$C(\langle H, K \rangle) = C(U_N) / (I \cap J)$$

$$C(\langle H, K \rangle) = C(U_N)/(I + I)$$

at the level of the associated algebras of functions.

PROOF. This is indeed clear from the definition of the operations \cap and \langle , \rangle , 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 \langle , \rangle can be constructed via the Tannakian correspondence $G \to C_G$, as follows:

- (1) Intersection: defined via $C_{G \cap H} = \langle C_G, C_H \rangle$.
- (2) Generation: defined via $C_{\langle G,H \rangle} = C_G \cap C_H$.

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:

$$C(G) = C(U_N) \Big/ \left\langle T \in Hom(u^{\otimes k}, u^{\otimes l}) \Big| \forall k, \forall l, \forall T \in Hom(v^{\otimes k}, v^{\otimes l}) \right\rangle$$

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:

$$C_{H\cap K} = \langle C_H, C_K \rangle$$

= $\langle span(D_H), span(D_K) \rangle$
= $span(\langle D_H, D_K \rangle)$

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

 $\langle H, K \rangle \subset \{H, K\}$

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:

$$C_{\langle H,K\rangle} = C_H \cap C_K$$

= $span(D_H) \cap span(D_K)$
 $\supset span(D_H \cap D_K)$

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 $D_{G \cap H} = \langle D_G, D_H \rangle$.
- (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



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:



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. \Box

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:

$$G \subset G \subset U_N$$

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:

$$\langle H, K \rangle \subset \langle \widetilde{H, K} \rangle \subset \{H, K\}$$

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:

$$T_{[\pi\sigma]} = T_{\pi} \otimes T_{\sigma} \quad , \quad T_{[\sigma]} \sim T_{\pi}T_{\sigma} \quad , \quad T_{\pi^*} = T_{\pi}^*$$

Together with the fact that C is a tensor category, we deduce from these formulae that we have the following implication:

$$\pi, \sigma \in D^{1} \implies T_{\pi}, T_{\sigma} \in C$$
$$\implies T_{\pi} \otimes T_{\sigma} \in C$$
$$\implies T_{[\pi\sigma]} \in C$$
$$\implies [\pi\sigma] \in D^{1}$$

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

$$\pi, \sigma \in D^{1} \implies T_{\pi}, T_{\sigma} \in C$$
$$\implies T_{\pi}T_{\sigma} \in C$$
$$\implies T_{[\frac{\sigma}{\pi}]} \in C$$
$$\implies [\frac{\sigma}{\pi}] \in D^{1}$$

Finally, we have as well the following implication:

$$\begin{array}{ccc} \in D^1 & \Longrightarrow & T_{\pi} \in C \\ & \Longrightarrow & T_{\pi}^* \in C \\ & \Longrightarrow & T_{\pi^*} \in C \\ & \Longrightarrow & \pi^* \in D^1 \end{array}$$

Thus D^1 is indeed a category of partitions, as claimed.

π

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:

128

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

$$D^{1}(k,l) = \left\{ \pi \in P(k,l) \middle| T_{\pi} \in C(k,l) \right\}$$

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

$$G^1 = (\langle G, S_N \rangle)^1$$

where $\langle G, S_N \rangle \subset U_N$ is the smallest closed subgroup containing G, S_N .

PROOF. According to our Tannakian results, the subgroup $\langle G, S_N \rangle \subset U_N$ in the statement exists indeed, and can be obtained by intersecting categories, as follows:

$$C_{\langle G, S_N \rangle} = C_G \cap C_{S_N}$$

We conclude from this that for any $\pi \in P(k, l)$ we have:

$$T_{\pi} \in C_{\langle G, S_N \rangle}(k, l) \iff T_{\pi} \in C_G(k, l)$$

It follows that the D^1 categories for the groups $\langle G, S_N \rangle$ and G coincide, and so the easy envelopes $(\langle G, S_N \rangle)^1$ 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

$$E^{p}(k,l) = \left\{ \alpha_{1}T_{\pi_{1}} + \ldots + \alpha_{p}T_{\pi_{p}} \in C(k,l) \middle| \alpha_{i} \in \mathbb{C}, \pi_{i} \in P(k,l) \right\}$$

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:

$$Hom(u^{\otimes k}, u^{\otimes l}) \simeq Fix(u^{\otimes \overline{k}l})$$

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, $G = G^1$.

130

131

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. \Box

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:

$$\begin{aligned} \xi_{\pi} \in Fix(v^{\otimes k}) &\iff (v^{\otimes k}\xi_{\pi})_{i_{1}\dots i_{k}} = (\xi_{\pi})_{i_{1}\dots i_{k}}, \forall i \\ &\iff \sum_{j} (v^{\otimes k})_{i_{1}\dots i_{k}, j_{1}\dots j_{k}} (\xi_{\pi})_{j_{1}\dots j_{k}} = (\xi_{\pi})_{i_{1}\dots i_{k}}, \forall i \\ &\iff \sum_{j} \delta_{\pi}(j_{1},\dots,j_{k})v_{i_{1}j_{1}}\dots v_{i_{k}j_{k}} = \delta_{\pi}(i_{1},\dots,i_{k}), \forall i \end{aligned}$$

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:

$$\sum_{j'} \delta_{\pi}(j_1, \dots, j_k)(v^{\otimes k'})_{i'j'} = \delta_{\pi}(i_1, \dots, i_k), \forall i$$

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:

<u>Case 1</u>. 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:

$$\sum_{j'} \delta_{\pi}(j'_1, \dots, j'_{k'})(v^{\otimes k'})_{i'j'} = \delta_{\pi}(i'_1, \dots, i'_{k'})$$

<u>Case 2</u>. 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,



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:



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:

$$k, l \in L, k > l \implies k - l \in L$$

 $k \in L, k \ge 2 \implies 2k - 2 \in L$

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:

$$b_k = \left\{ \begin{matrix} \square & \dots & \square \\ 1 & 2 & \dots & k \end{matrix} \right\}$$

For k > l, we can write b_{k-l} in the following way:

$$b_{k-l} = \begin{cases} \Box \Box & \dots & \dots & \Box & \Box \\ 1 & 2 & \dots & l & l+1 & \dots & k \\ \Box \Box & \dots & \Box & | & \dots & | \\ & & & 1 & \dots & k-l \end{cases}$$

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:

<u>Case 1</u>. 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 $L = \{1, 2, ..., m\}$, for a certain number $m \in \{1, 2, ..., \infty\}$. On the other hand, by using the second formula we get:

$$m \in L \implies 2m - 2 \in L$$
$$\implies 2m - 2 \leq m$$
$$\implies m \in \{1, 2, \infty\}$$

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 .

<u>Case 2</u>. 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 $L = \{2, 4, ..., 2p\}$, for a certain number $p \in \{1, 2, ..., \infty\}$. On the other hand, by using the second formula we get:

$$2p \in L \implies 4p - 2 \in L$$
$$\implies 4p - 2 \leq 2p$$
$$\implies p \in \{1, \infty\}$$

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 $G'_N = G_N \times \mathbb{Z}_2$:



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,



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:



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]. \Box

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

Gram determinants

8a. Gram determinants

Let us discuss now a key algebraic problem, that we already met before, on various occasions, namely the linear independence of the vectors ξ_{π} . We first have:

DEFINITION 8.1. 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 $\pi \lor \sigma \in P(k)$ 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 $P(2) = \{||, \square\}$, and we have:

 $|| \leq \Box$

Also, at k = 3 we have $P(3) = \{|||, \Box|, \Box, |\Box, \Box\Box\}$, and the order relation is as follows:

 $||| \leq |\Pi|, |\Pi| \leq |\Pi|$

In relation with our linear independence questions, the idea will be that of using:

PROPOSITION 8.2. The Gram matrix of the vectors ξ_{π} is given by the formula

$$<\xi_{\pi},\xi_{\sigma}>=N^{|\pi\vee\sigma|}$$

where \lor is the superposition operation, and |.| is the number of blocks.

PROOF. According to the formula of the vectors ξ_{π} , we have:

$$<\xi_{\pi},\xi_{\sigma}> = \sum_{i_{1}\dots i_{k}} \delta_{\pi}(i_{1},\dots,i_{k})\delta_{\sigma}(i_{1},\dots,i_{k})$$
$$= \sum_{i_{1}\dots i_{k}} \delta_{\pi\vee\sigma}(i_{1},\dots,i_{k})$$
$$= N^{|\pi\vee\sigma|}$$

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:

8. GRAM DETERMINANTS

DEFINITION 8.3. The Möbius function of any lattice, and so of P, is given by

$$\mu(\pi, \sigma) = \begin{cases} 1 & \text{if } \pi = \sigma \\ -\sum_{\pi \le \tau < \sigma} \mu(\pi, \tau) & \text{if } \pi < \sigma \\ 0 & \text{if } \pi \nleq \sigma \end{cases}$$

with the construction being performed by recurrence.

As an illustration here, for $P(2) = \{||, \Box\}$, we have by definition:

$$\mu(||,||) = \mu(\Box,\Box) = 1$$

Also, $|| < \Box$, with no intermediate partition in between, so we obtain:

$$\mu(||, \sqcap) = -\mu(||, ||) = -1$$

Finally, we have $\sqcap \not\leq \mid\mid$, 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:

$$f(\sigma) = \sum_{\pi \leq \sigma} g(\pi) \quad \Longrightarrow \quad g(\sigma) = \sum_{\pi \leq \sigma} \mu(\pi, \sigma) f(\pi)$$

In linear algebra terms, the statement and proof of this formula are as follows:

THEOREM 8.4. The inverse of the adjacency matrix of P(k), given by

$$A_k(\pi, \sigma) = \begin{cases} 1 & \text{if } \pi \leq \sigma \\ 0 & \text{if } \pi \nleq \sigma \end{cases}$$

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 8.3.

8b. Symmetric groups

Now back to our Gram matrix considerations, we have the following key result:

PROPOSITION 8.5. 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, $G_k = A_k L_k$, where

$$L_k(\pi, \sigma) = \begin{cases} N(N-1)\dots(N-|\pi|+1) & \text{if } \sigma \le \pi\\ 0 & \text{otherwise} \end{cases}$$

and where A_k is the adjacency matrix of P(k).

PROOF. We have the following computation, based on Proposition 8.2:

$$G_k(\pi, \sigma) = N^{|\pi \vee \sigma|}$$

= $\# \left\{ i_1, \dots, i_k \in \{1, \dots, N\} \middle| \ker i \ge \pi \vee \sigma \right\}$
= $\sum_{\tau \ge \pi \vee \sigma} \# \left\{ i_1, \dots, i_k \in \{1, \dots, N\} \middle| \ker i = \tau \right\}$
= $\sum_{\tau \ge \pi \vee \sigma} N(N-1) \dots (N-|\tau|+1)$

According now to the definition of A_k, L_k , this formula reads:

$$G_k(\pi, \sigma) = \sum_{\tau \ge \pi} L_k(\tau, \sigma)$$
$$= \sum_{\tau} A_k(\pi, \tau) L_k(\tau, \sigma)$$
$$= (A_k L_k)(\pi, \sigma)$$

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

As an illustration for the above result, at k = 2 we have $P(2) = \{||, \square\}$, 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 8.6. 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:

$$det(G_k) = det(A_k) det(L_k)$$

= $det(L_k)$
= $\prod_{\pi} L_k(\pi, \pi)$
= $\prod_{\pi} N(N-1) \dots (N-|\pi|+1)$

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

8. GRAM DETERMINANTS

8c. Reflection groups

We discuss now the systematic computation of the Gram determinants. Let us begin with some simple observations, coming from definitions:

PROPOSITION 8.7. 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 8.7, in the following way:

PROPOSITION 8.8. 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 8.7, using a variable t around 1. Note that in (2) we regard the variable N as a formal parameter, going to 0. \Box

The trace can be understood in terms of the associated Stirling numbers, as follows:

PROPOSITION 8.9. 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 8.10. 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 before, this follows from the Weingarten formula.

Getting now to concrete computations, for the reflection groups, we have here:

THEOREM 8.11. 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:

$$G'_{kN}(\pi,\sigma) = \begin{cases} N(N-1)\dots(N-|\sigma|+1) & \text{if } \pi \le \sigma \\ 0 & \text{otherwise} \end{cases}$$

Thus the matrix is upper triangular, and by computing the product on the diagonal we obtain the formula in the statement. $\hfill \Box$

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 8.12. 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 8.11 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.

 \square

8. GRAM DETERMINANTS

8d. 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 8.13. The determinant of the Gram matrix of O_N is given by

$$\det(G_{kN}) = \prod_{|\lambda|=k/2} f_N(\lambda)^{f^*}$$

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 8.14. We have a bijection $NC(k) \simeq NC_2(2k)$, as follows:

- (1) The application $NC(k) \rightarrow NC_2(2k)$ is the "fattening" one, obtained by doubling all the legs, and doubling all the strings as well.
- (2) Its inverse $NC_2(2k) \rightarrow NC(k)$ 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. \Box

At the level of the associated Gram matrices, the result is as follows:

PROPOSITION 8.15. 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 8.14, 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 8.16. The first Gram matrices and determinants for O_N^+ are

$$\det \begin{pmatrix} N^2 & N \\ N & N^2 \end{pmatrix} = N^2 (N^2 - 1)$$
$$\det \begin{pmatrix} N^3 & N^2 & N^2 & N^2 \\ N^2 & N^3 & N & N^2 \\ N^2 & N & N^3 & N & N^2 \\ N^2 & N & N & N^3 & N^2 \\ N & N^2 & N^2 & N^2 & N^3 \end{pmatrix} = N^5 (N^2 - 1)^4 (N^2 - 2)$$

with the matrices being written by using the lexicographic order on $NC_2(2k)$.

PROOF. The formula at k = 2, where $NC_2(4) = \{ \Box \Box, \bigcap \}$, is clear from definitions. At k = 3 however, things are tricky. The partitions here are as follows:

$$NC(3) = \{|||, \Box|, \Box, |\Box, \Box\}$$

The Gram matrix and its determinant are, according to Theorem 8.6:

$$\det \begin{pmatrix} N^3 & N^2 & N^2 & N^2 & N \\ N^2 & N^2 & N & N & N \\ N^2 & N & N^2 & N & N \\ N^2 & N & N & N^2 & N \\ N & N & N & N & N \end{pmatrix} = N^5 (N-1)^4 (N-2)$$

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 $k \ge 4$. However, following Di Francesco [19], we have the following result:

THEOREM 8.17. 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

 $P_0 = 1$, $P_1 = X$, $P_{r+1} = XP_r - P_{r-1}$

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 $k \notin \mathbb{Z}$.

8. GRAM DETERMINANTS

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 8.18. 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

$$P_0 = 1$$
 , $P_1 = X$, $P_{r+1} = XP_r - P_{r-1}$

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 8.17, by using Proposition 8.15.

8e. Exercises

Exercises:

Exercise 8.19.

EXERCISE 8.20.

EXERCISE 8.21.

EXERCISE 8.22.

EXERCISE 8.23.

EXERCISE 8.24.

EXERCISE 8.25.

EXERCISE 8.26.

Bonus exercise.
Part III

Lie algebras

If trouble comes your way Just ask for me My friends all know me As the General Lee

Lie algebras

9a. Lie algebras

A Lie group is by definition a group which is a smooth manifold. So, let us start our discussion with this, smooth manifolds. Here is their definition:

DEFINITION 9.1. A smooth manifold is a space X which is locally isomorphic to \mathbb{R}^N . To be more precise, this space X must be covered by charts, bijectively mapping open pieces of it to open pieces of \mathbb{R}^N , with the changes of charts being C^{∞} functions.

It is possible to talk as well about C^k manifolds, with $k < \infty$, but this is rather technical material, that we will not need, in relation with our considerations here.

As basic examples of smooth manifolds, we have \mathbb{R}^N itself, or any open subset $X \subset \mathbb{R}^N$, with only 1 chart being needed here. Other basic examples include the circle, or curves like ellipses and so on, for obvious reasons. To be more precise, the unit circle can be covered by 2 charts as above, by using polar coordinates, in the obvious way, and then by applying dilations, translations and other such transformations, namely bijections which are smooth, we obtain a whole menagery of circle-looking manifolds.

Here is a more precise statement in this sense, covering the conics:

THEOREM 9.2. The following are smooth manifolds, in the plane:

- (1) The circles.
- (2) The ellipses.
- (3) The non-degenerate conics.
- (4) Smooth deformations of these.

PROOF. All this is quite intuitive, the idea being as follows:

(1) Consider the unit circle, $x^2 + y^2 = 1$. We can write then $x = \cos t$, $y = \sin t$, with $t \in [0, 2\pi)$, and we seem to have here the solution to our problem, just using 1 chart. But this is of course wrong, because $[0, 2\pi)$ is not open, and we have a problem at 0. In practice we need to use 2 such charts, say with the first one being with $t \in (0, 3\pi/2)$, and the second one being with $t \in (\pi, 5\pi/2)$. As for the fact that the change of charts is indeed smooth, this comes by writing down the formulae, or just thinking a bit, and arguing that this change of chart being actually a translation, it is automatically linear.

9. LIE ALGEBRAS

(2) This follows from (1), by pulling the circle in both the Ox and Oy directions, and the formulae here, based on the standard formulae for ellipses, are left to you reader.

(3) We already have the ellipses, and the case of the parabolas and hyperbolas is elementary as well, and in fact simpler than the case of the ellipses. Indeed, a parabola is clearly homeomorphic to \mathbb{R} , and a hyperbola, to two copies of \mathbb{R} .

(4) This is something which is clear too, depending of course on what exactly we mean by "smooth deformation", and by using a bit of multivariable calculus if needed. \Box

In higher dimensions, as basic examples, we have the spheres, as shown by:

THEOREM 9.3. The sphere is a smooth manifold.

PROOF. There are several proofs for this, all instructive, as follows:

(1) A first idea is to use spherical coordinates, which are as follows:

$$\begin{cases} x_1 = r \cos t_1 \\ x_2 = r \sin t_1 \cos t_2 \\ \vdots \\ x_{N-1} = r \sin t_1 \sin t_2 \dots \sin t_{N-2} \cos t_{N-1} \\ x_N = r \sin t_1 \sin t_2 \dots \sin t_{N-2} \sin t_{N-1} \end{cases}$$

Indeed, these produce explicit charts for the sphere.

(2) A second idea, which makes use of less charts, is to use the stereographic projection, which should be given by inverse maps as follows:

$$\Phi: \mathbb{R}^N \to S^N_{\mathbb{R}} - \{\infty\} \quad , \quad \Psi: S^N_{\mathbb{R}} - \{\infty\} \to \mathbb{R}^N$$

Indeed, we are looking for the formulae of the isomorphism $\mathbb{R}^N \simeq S_{\mathbb{R}}^N - \{\infty\}$, obtained by identifying $\mathbb{R}^N = \mathbb{R}^N \times \{0\} \subset \mathbb{R}^{N+1}$ with the unit sphere $S_{\mathbb{R}}^N \subset \mathbb{R}^{N+1}$, with the convention that the point which is added is $\infty = (1, 0, \dots, 0)$, via the stereographic projection. That is, we need the precise formulae of two inverse maps, as follows:

$$\Phi: \mathbb{R}^N \to S^N_{\mathbb{R}} - \{\infty\} \quad , \quad \Psi: S^N_{\mathbb{R}} - \{\infty\} \to \mathbb{R}^N$$

In one sense, according to our conventions above, we must have a formula as follows for our map Φ , with the parameter $t \in (0, 1)$ being such that $||\Phi(v)|| = 1$:

$$\Phi(v) = t(0, v) + (1 - t)(1, 0)$$

The equation for the parameter $t \in (0, 1)$ can be solved as follows:

$$(1-t)^2 + t^2 ||v||^2 = 1 \iff t^2 (1+||v||^2) = 2t$$

 $\iff t = \frac{2}{1+||v||^2}$

We conclude that the formula of the map Φ is as follows:

$$\Phi(v) = (1,0) + \frac{2}{1+||v||^2} \left(-1,v\right)$$

In the other sense now we must have, for a certain $\alpha \in \mathbb{R}$:

$$(0, \Psi(c, x)) = \alpha(c, x) + (1 - \alpha)(1, 0)$$

But from $\alpha c + 1 - \alpha = 0$ we get the following formula for the parameter α :

$$\alpha = \frac{1}{1-c}$$

We conclude that the formula of the map Ψ is as follows:

$$\Psi(c,x) = \frac{x}{1-c}$$

Here, as before, we use the convention in the statement, namely $\mathbb{R}^{N+1} = \mathbb{R} \times \mathbb{R}^N$, with the coordinate of \mathbb{R} denoted x_0 , and with the coordinates of \mathbb{R}^N denoted x_1, \ldots, x_N .

(3) We have as well cylindrical coordinates, as well as many other types of more specialized coordinates, which can be useful in physics, and also geography, economics and so on. We will leave some thinking here as an instructive exercise. \Box

Other key examples of manifolds include the projective spaces, as shown by:

THEOREM 9.4. The projective space $P_{\mathbb{R}}^{N-1}$ is a smooth manifold, with charts

$$(x_1,\ldots,x_N) \rightarrow \left(\frac{x_1}{x_i},\ldots,\frac{x_{i-1}}{x_i},\frac{x_{i+1}}{x_i},\ldots,\frac{x_N}{x_i}\right)$$

where $x_i \neq 0$. This manifold is compact, and of dimension N-1.

PROOF. We know that $P_{\mathbb{R}}^{N-1}$ appears by definition as the space of lines in \mathbb{R}^N passing through the origin, so we have the following formula, with ~ being the proportionality of vectors, given as usual by $x \sim y$ when $x = \lambda y$, for some scalar $\lambda \neq 0$:

$$P_{\mathbb{R}}^{N-1} = \mathbb{R}^N - \{0\} / \sim$$

Alternatively, we can restrict if we want the attention to the vectors on the unit sphere $S_{\mathbb{R}}^{N-1} \subset \mathbb{R}^N$, and this because any line in \mathbb{R}^N passing through the origin will certainly cross this sphere. Moreover, it is clear that our line will cross the sphere in exactly two points $\pm x$, and we conclude that we have the following formula, with \sim being now the proportionality of vectors on the sphere, given by $x \sim y$ when $x = \pm y$:

$$P_{\mathbb{R}}^{N-1} = S_{\mathbb{R}}^{N-1} / \sim$$

9. LIE ALGEBRAS

With this discussion made, let us get now to what is to be proved. Obviously, once we fix an index $i \in \{1, ..., N\}$, the condition $x_i \neq 0$ on the vectors $x \in \mathbb{R}^N - \{0\}$ defines an open subset $U_i \subset P_{\mathbb{R}}^{N-1}$, and the open subsets that we get in this way cover $P_{\mathbb{R}}^{N-1}$:

$$P_{\mathbb{R}}^{N-1} = U_1 \cup \ldots \cup U_N$$

Moreover, the map in the statement is injective $U_i \to \mathbb{R}^{N-1}$, and it is clear too that the changes of charts are C^{∞} . Thus, we have our smooth manifold, as claimed.

Now back to the general setting, that of Definition 9.1, the question is, what to do with our smooth manifolds X. And in answer, we have the following construction:

THEOREM 9.5. Given a smooth manifold X, and a point $x \in X$, we can talk about the tangent space T_xX , in the obvious way. This space varies smoothly with x.

PROOF. This is something which is quite self-explanatory, and we will leave the clarification of all this as an instructive exercise. If needed, you can consult as well any introductory differential geometry book, but beware of the many abstractions there. \Box

Getting now to what we wanted to do, in the present chapter of this book, namely Lie groups and Lie algebras, here is their definition, based on the above:

DEFINITION 9.6. A Lie group is a group G which is a smooth manifold, with the corresponding multiplication and inverse maps

$$m: G \times G \to G \quad , \quad i: G \to G$$

being assumed to be smooth. The tangent space at the origin $1 \in G$ is denoted

 $\mathfrak{g} = T_1 G$

and is called Lie algebra of G.

So, this is our definition, and as a first observation, the examples of Lie groups abound, with the circle \mathbb{T} and with the higher dimensional tori \mathbb{T}^N being the standard examples. For these, the Lie algebra is obviously equal to \mathbb{R} and \mathbb{R}^N , respectively. There are of course many other examples, all very interesting, and more on this in a moment.

Before getting into examples, let us discuss a basic question, that you surely have in mind, namely why calling the tangent space $\mathfrak{g} = T_1 G$ an algebra. In answer, since G is a group, with a certain multiplication map $m: G \times G \to G$, we can normally expect this map m to produce some sort of "algebra structure" on the tangent space $\mathfrak{g} = T_1 G$.

This was for the idea, but in practice, things are more complicated than this, because even for the simplest examples of Lie groups, what we get in this way is not an associative algebra, but rather a new type of beast, called Lie algebra.

So, coming as a continuation and complement to Definition 9.6, we have:

9A. LIE ALGEBRAS

DEFINITION 9.7. A Lie algebra is a vector space \mathfrak{g} with an operation $(x, y) \to [x, y]$, called Lie bracket, subject to the following conditions:

- (1) [x+y,z] = [x,z] + [y,z], [x,y+z] = [x,y] + [x,z].
- (2) $[\lambda x, y] = [x, \lambda y] = \lambda [x, y].$
- (3) [x, x] = 0.
- (4) [[x, y], z] + [[y, z], x] + [[z, x], y] = 0.

As a basic example, consider a usual, associative algebra A. We can define then the Lie bracket on it as being the usual commutator, namely:

$$[x,y] = xy - yx$$

The above axioms (1,2,3) are then clearly satisfied, and in what regards axiom (4), called Jacobi identity, this is satisfied too, the verification being as follows:

$$\begin{aligned} & [[x, y], z] + [[y, z], x] + [[z, x], y] \\ &= & [xy - yx, z] + [yz - zy, x] + [zx - xz, y] \\ &= & xyz - yxz - zxy + zyx + yzx - zyx - xyz + xzy + zxy - xzy - yzx + yxz \\ &= & 0 \end{aligned}$$

We will see in a moment that up to a certain abstract operation $\mathfrak{g} \to U\mathfrak{g}$, called enveloping Lie algebra construction, and which is something quite elementary, any Lie algebra appears in this way, with its Lie bracket being formally given by:

[x, y] = xy - yx

Before that, however, you might wonder where that Gothic letter \mathfrak{g} in Definition 9.7 comes from. That comes from the following fundamental result, making the connection with the theory of Lie groups from Definition 9.6, denoted as usual by G:

THEOREM 9.8. Given a Lie group G, that is, a group which is a smooth manifold, with the group operations being smooth, the tangent space at the identity

$$\mathfrak{g} = T_1(G)$$

is a Lie algebra, with its Lie bracket being basically a usual commutator.

PROOF. This is something non-trivial, the idea being as follows:

(1) Let us first have a look at the orthogonal and unitary groups O_N, N_N . These are both Lie groups, and the corresponding Lie algebras $\boldsymbol{o}_N, \boldsymbol{u}_N$ can be computed by differentiating the equations defining O_N, U_N , with the conclusion being as follows:

$$\mathfrak{o}_N = \left\{ A \in M_N(\mathbb{R}) \middle| A^t = -A \right\}$$
$$\mathfrak{u}_N = \left\{ B \in M_N(\mathbb{C}) \middle| B^* = -B \right\}$$

9. LIE ALGEBRAS

This was for the correspondences $O_N \to \mathfrak{o}_N$ and $U_N \to \mathfrak{u}_N$. In the other sense, the correspondences $\mathfrak{o}_N \to O_N$ and $\mathfrak{u}_N \to U_N$ appear by exponentiation, the result here stating that, around 1, the orthogonal matrices can be written as $U = e^A$, with $A \in \mathfrak{o}_N$, and the unitary matrices can be written as $U = e^B$, with $B \in \mathfrak{u}_N$.

(2) Getting now to the Lie bracket, the first observation is that both $\mathfrak{o}_N, \mathfrak{u}_N$ are stable under the usual commutator of the $N \times N$ matrices. Indeed, assuming that $A, B \in M_N(\mathbb{R})$ satisfy $A^t = -A, B^t = -B$, their commutator satisfies $[A, B] \in M_N(\mathbb{R})$, and:

$$[A, B]^t = (AB - BA)^t$$
$$= B^t A^t - A^t B^t$$
$$= BA - AB$$
$$= -[A, B]$$

Similarly, assuming that $A, B \in M_N(\mathbb{C})$ satisfy $A^* = -A, B^* = -B$, their commutator $[A, B] \in M_N(\mathbb{C})$ satisfies the condition $[A, B]^* = -[A, B]$.

(3) We conclude from this discussion that both the tangent spaces $\mathbf{o}_N, \mathbf{u}_N$ are Lie algebras, with the Lie bracket being the usual commutator of the $N \times N$ matrices. It remains now to understand how the Lie bracket [A, B] = AB - BA is related to the group commutator $[U, V] = UVU^{-1}V^{-1}$ via the exponentiation map $U = e^A$, and this can be indeed done, by making use of the differential geometry of O_N, U_N , and the situation is quite similar when dealing with an arbitrary Lie group G.

(4) All this is very standard, but quite non-trivial, and we will be back to it, with details, later in this book, when systematically discussing Lie theory. \Box

With this understood, let us go back to the arbitrary Lie algebras, as axiomatized in Definition 9.7. There is an obvious analogy there with the axioms for the usual, associative algebras, and based on this analogy, we can build some abstract algebra theory for the Lie algebras. Let us record some basic results, along these lines:

PROPOSITION 9.9. Let \mathfrak{g} be a Lie algebra. If we define its ideals as being the vector spaces $\mathfrak{i} \subset \mathfrak{g}$ satisfying the condition

$$x \in \mathfrak{i}, y \in \mathfrak{g} \implies [x, y] \in \mathfrak{i}$$

then the quotients $\mathfrak{g}/\mathfrak{i}$ are Lie algebras. Also, given a morphism of Lie algebras $f: \mathfrak{g} \to \mathfrak{h}$, its kernel $ker(f) \subset \mathfrak{g}$ is an ideal, and we have $\mathfrak{g}/ker(f) = Im(f)$.

PROOF. All this is very standard, exactly as in the case of the associative algebras, and we will leave the various verifications here as an instructive exercise. \Box

Getting now to the point, remember our claim from the discussion after Definition 9.7, stating that up to a certain abstract operation $\mathfrak{g} \to U\mathfrak{g}$, called enveloping Lie algebra construction, any Lie algebra appears in fact from the "trivial" associative algebra

construction, that is, with its Lie bracket being formally a usual commutator:

$$[x, y] = xy - yx$$

Time now to clarify this. The result here, making as well to the link with the various Lie group considerations from Theorem 9.8 and its proof, is as follows:

THEOREM 9.10. Given a Lie algebra \mathfrak{g} , define its enveloping Lie algebra $U\mathfrak{g}$ as being the quotient of the tensor algebra of \mathfrak{g} , namely

$$T(\mathfrak{g}) = \bigoplus_{k=0}^{\infty} \mathfrak{g}^{\otimes k}$$

by the following associative algebra ideal, with x, y ranging over the elements of \mathfrak{g} :

$$I = \langle x \otimes y - y \otimes x - [x, y] \rangle$$

Then $U\mathfrak{g}$ is an associative algebra, so it is a Lie algebra too, with bracket

$$[x,y] = xy - yx$$

and the standard embedding $\mathfrak{g} \subset U\mathfrak{g}$ is a Lie algebra embedding.

PROOF. This is something which is quite self-explanatory, and in what regards the examples, illustrations, and other things that can be said, for instance in relation with the Lie groups, we will leave some further reading here as an instructive exercise. \Box

Importantly, the above enveloping Lie algebra construction makes the link with our Hopf algebra considerations, from the present book, via the following result:

THEOREM 9.11. Given a Lie algebra \mathfrak{g} , its enveloping Lie algebra $U\mathfrak{g}$ is a cocommutative Hopf algebra, with comultiplication, counit and antipode given by

$$\begin{split} \Delta : U\mathfrak{g} \to U(\mathfrak{g} \oplus \mathfrak{g}) &= U\mathfrak{g} \otimes U\mathfrak{g} \quad , \quad x \to x + x \\ \varepsilon : U\mathfrak{g} \to F \quad , \quad x \to 1 \\ S : U\mathfrak{g} \to U\mathfrak{g}^{opp} &= (U\mathfrak{g})^{opp} \quad , \quad x \to -x \end{split}$$

via various standard identifications, for the various associative algebras involved.

PROOF. Again, this is something quite self-explanatory, and in what regards the examples, illustrations, and other things that can be said, for instance in relation with the Lie groups, we will leave some further reading here as an instructive exercise. \Box

Many other things can be said, as a continuation of this.

9b.

9c.

9d.

9e. Exercises

Exercises:

Exercise 9.12.

EXERCISE 9.13.

EXERCISE 9.14.

Exercise 9.15.

Exercise 9.16.

Exercise 9.17.

Exercise 9.18.

EXERCISE 9.19.

10a.

10b.

10c.

10d.

10e. Exercises

Exercises:

Exercise 10.1.

Exercise 10.2.

Exercise 10.3.

EXERCISE 10.4.

Exercise 10.5.

EXERCISE 10.6.

Exercise 10.7.

Exercise 10.8.

11a.

11b.

11c.

11d.

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.

12a.

12b.

12c.

12d.

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.

Part IV

Analytic aspects

Your smile is like a breath of spring Your voice is soft like summer rain And I cannot compete with you Jolene

Haar integration

13a. Spherical integrals

In a purely mathematical context, the simplest way of recovering the normal laws is by looking at the coordinates over the real spheres $S_{\mathbb{R}}^{N-1}$, in the $N \to \infty$ limit. To start with, at N = 2 the sphere is the unit circle \mathbb{T} , and with $z = e^{it}$ the coordinates are $\cos t, \sin t$. Let us first integrate powers of these coordinates. We have here:

PROPOSITION 13.1. We have the following formulae,

$$\int_0^{\pi/2} \cos^k t \, dt = \int_0^{\pi/2} \sin^k t \, dt = \left(\frac{\pi}{2}\right)^{\varepsilon(k)} \frac{k!!}{(k+1)!!}$$

where $\varepsilon(k) = 1$ if k is even, and $\varepsilon(k) = 0$ if k is odd.

PROOF. Let us call I_k the integral on the left in the statement. In order to compute it, we use partial integration. We have the following formula:

$$(\cos^{k} t \sin t)' = k \cos^{k-1} t (-\sin t) \sin t + \cos^{k} t \cos t$$
$$= (k+1) \cos^{k+1} t - k \cos^{k-1} t$$

By integrating between 0 and $\pi/2$, we obtain the following formula:

$$(k+1)I_{k+1} = kI_{k-1}$$

Thus we can compute I_k by recurrence, and we obtain in this way:

$$I_{k} = \frac{k-1}{k} I_{k-2}$$

$$= \frac{k-1}{k} \cdot \frac{k-3}{k-2} I_{k-4}$$

$$= \frac{k-1}{k} \cdot \frac{k-3}{k-2} \cdot \frac{k-5}{k-4} I_{k-6}$$

$$\vdots$$

$$= \frac{k!!}{(k+1)!!} I_{1-\varepsilon(k)}$$

The initial data being $I_0 = \pi/2$ and $I_1 = 1$, we obtain the result. As for the second formula, this follows from the first one, with the change of variables $t = \pi/2 - s$.

More generally now, we have the following result:

THEOREM 13.2. We have the following formula,

$$\int_0^{\pi/2} \cos^r t \sin^s t \, dt = \left(\frac{\pi}{2}\right)^{\varepsilon(r)\varepsilon(s)} \frac{r!!s!!}{(r+s+1)!!}$$

where $\varepsilon(r) = 1$ if r is even, and $\varepsilon(r) = 0$ if r is odd.

PROOF. Let us call I_{rs} the integral in the statement. In order to do the partial integration, observe that we have the following formula:

$$(\cos^r t \sin^s t)' = r \cos^{r-1} t (-\sin t) \sin^s t + \cos^r t \cdot s \sin^{s-1} t \cos t = -r \cos^{r-1} t \sin^{s+1} t + s \cos^{r+1} t \sin^{s-1} t$$

By integrating between 0 and $\pi/2$, we obtain, for r, s > 0:

$$rI_{r-1,s+1} = sI_{r+1,s-1}$$

Thus, we can compute I_{rs} by recurrence. When s is even we have:

$$I_{rs} = \frac{s-1}{r+1} I_{r+2,s-2}$$

= $\frac{s-1}{r+1} \cdot \frac{s-3}{r+3} I_{r+4,s-4}$
= $\frac{s-1}{r+1} \cdot \frac{s-3}{r+3} \cdot \frac{s-5}{r+5} I_{r+6,s-6}$
:
= $\frac{r!!s!!}{(r+s)!!} I_{r+s}$

But the last term comes from Proposition 13.1, and we obtain the result:

$$I_{rs} = \frac{r!!s!!}{(r+s)!!} I_{r+s}$$

= $\frac{r!!s!!}{(r+s)!!} \left(\frac{\pi}{2}\right)^{\varepsilon(r+s)} \frac{(r+s)!!}{(r+s+1)!!}$
= $\left(\frac{\pi}{2}\right)^{\varepsilon(r)\varepsilon(s)} \frac{r!!s!!}{(r+s+1)!!}$

Observe that this gives the result for r even as well, by symmetry. In the remaining case now, where both the exponents r, s are odd, we can use once again the formula

 $rI_{r-1,s+1} = sI_{r+1,s-1}$ found above, and the recurrence goes as follows:

$$I_{rs} = \frac{s-1}{r+1} I_{r+2,s-2}$$

= $\frac{s-1}{r+1} \cdot \frac{s-3}{r+3} I_{r+4,s-4}$
= $\frac{s-1}{r+1} \cdot \frac{s-3}{r+3} \cdot \frac{s-5}{r+5} I_{r+6,s-6}$
:
= $\frac{r!!s!!}{(r+s-1)!!} I_{r+s-1,1}$

In order to compute the last term, observe that we have:

$$I_{r1} = \int_{0}^{\pi/2} \cos^{r} t \sin t \, dt$$
$$= -\frac{1}{r+1} \int_{0}^{\pi/2} (\cos^{r+1} t)' \, dt$$
$$= \frac{1}{r+1}$$

Thus, we obtain the formula in the statement, the exponent of $\pi/2$ appearing there being $\varepsilon(r)\varepsilon(s) = 0 \cdot 0 = 0$ in the present case, and this finishes the proof.

In order to deal now with the higher spheres, we will use spherical coordinates:

THEOREM 13.3. We have spherical coordinates in N dimensions,

$$\begin{cases} x_1 &= r \cos t_1 \\ x_2 &= r \sin t_1 \cos t_2 \\ \vdots \\ x_{N-1} &= r \sin t_1 \sin t_2 \dots \sin t_{N-2} \cos t_{N-1} \\ x_N &= r \sin t_1 \sin t_2 \dots \sin t_{N-2} \sin t_{N-1} \end{cases}$$

the corresponding Jacobian being given by the following formula:

$$J(r,t) = r^{N-1} \sin^{N-2} t_1 \sin^{N-3} t_2 \dots \sin^2 t_{N-3} \sin t_{N-2}$$

PROOF. The fact that we have indeed spherical coordinates is clear. Regarding now the Jacobian, by developing over the last column, we have:

$$J_{N} = r \sin t_{1} \dots \sin t_{N-2} \sin t_{N-1} \times \sin t_{N-1} J_{N-1} + r \sin t_{1} \dots \sin t_{N-2} \cos t_{N-1} \times \cos t_{N-1} J_{N-1} = r \sin t_{1} \dots \sin t_{N-2} (\sin^{2} t_{N-1} + \cos^{2} t_{N-1}) J_{N-1} = r \sin t_{1} \dots \sin t_{N-2} J_{N-1}$$

Thus, we obtain the formula in the statement, by recurrence.

As a first application, we can compute the volume of the sphere:

THEOREM 13.4. The volume of the unit sphere in \mathbb{R}^N is given by

$$\frac{V}{2^N} = \left(\frac{\pi}{2}\right)^{[N/2]} \frac{1}{(N+1)!!}$$

with our usual convention $m!! = (m-1)(m-3)(m-5)\dots$ for double factorials.

PROOF. If we denote by Q the positive part of the sphere, obtained by cutting the sphere in 2^N parts, we have, by using Theorems 13.2 and 13.3 and Fubini:

$$\frac{V}{2^{N}} = \int_{0}^{1} \int_{0}^{\pi/2} \dots \int_{0}^{\pi/2} r^{N-1} \sin^{N-2} t_{1} \dots \sin t_{N-2} dr dt_{1} \dots dt_{N-1}
= \int_{0}^{1} r^{N-1} dr \int_{0}^{\pi/2} \sin^{N-2} t_{1} dt_{1} \dots \int_{0}^{\pi/2} \sin t_{N-2} dt_{N-2} \int_{0}^{\pi/2} 1 dt_{N-1}
= \frac{1}{N} \times \left(\frac{\pi}{2}\right)^{[N/2]} \times \frac{(N-2)!!}{(N-1)!!} \cdot \frac{(N-3)!!}{(N-2)!!} \dots \frac{2!!}{3!!} \cdot \frac{1!!}{2!!} \cdot 1
= \left(\frac{\pi}{2}\right)^{[N/2]} \frac{1}{(N+1)!!}$$

Here we have used the following formula for computing the exponent of $\pi/2$, where $\varepsilon(r) = 1$ if r is even and $\varepsilon(r) = 0$ if r is odd, as in Theorem 13.2:

$$\varepsilon(0) + \varepsilon(1) + \varepsilon(2) + \ldots + \varepsilon(N-2) = 1 + 0 + 1 + 0 + \ldots + \varepsilon(N-2)$$
$$= \left[\frac{N-2}{2}\right] + 1$$
$$= \left[\frac{N}{2}\right]$$

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

Let us discuss now the computation of the arbitrary polynomial integrals, over the spheres of arbitrary dimension. The result here is as follows:

166

THEOREM 13.5. The spherical integral of $x_{i_1} \dots x_{i_r}$ vanishes, unless each index $a \in \{1, \dots, N\}$ appears an even number of times in the sequence i_1, \dots, i_r . We have

$$\int_{S_{\mathbb{R}}^{N-1}} x_{i_1} \dots x_{i_r} \, dx = \frac{(N-1)!!k_1!!\dots k_N!!}{(N+\Sigma k_i - 1)!!}$$

with k_a being this number of occurrences.

PROOF. In what concerns the first assertion, regarding vanishing when some multiplicity k_a is odd, this follows via the change of variables $x_a \to -x_a$. Regarding now the formula in the statement, assume that we are in the case $k_a \in 2\mathbb{N}$, for any $a \in \{1, \ldots, N\}$. The integral in the statement can be written in spherical coordinates, as follows:

$$I = \frac{2^N}{V} \int_0^{\pi/2} \dots \int_0^{\pi/2} x_1^{k_1} \dots x_N^{k_N} J \, dt_1 \dots dt_{N-1}$$

In this formula V is the volume of the sphere, J is the Jacobian, and the 2^N factor comes from the restriction to the $1/2^N$ part of the sphere where all the coordinates are positive. According to the formula in Theorem 13.4, the normalization constant is:

$$\frac{2^N}{V} = \left(\frac{2}{\pi}\right)^{[N/2]} (N+1)!!$$

As for the unnormalized integral, this is given by:

$$I' = \int_0^{\pi/2} \dots \int_0^{\pi/2} (\cos t_1)^{k_1} (\sin t_1 \cos t_2)^{k_2}$$

$$\vdots$$

$$(\sin t_1 \sin t_2 \dots \sin t_{N-2} \cos t_{N-1})^{k_{N-1}}$$

$$(\sin t_1 \sin t_2 \dots \sin t_{N-2} \sin t_{N-1})^{k_N}$$

$$\sin^{N-2} t_1 \sin^{N-3} t_2 \dots \sin^2 t_{N-3} \sin t_{N-2}$$

$$dt_1 \dots dt_{N-1}$$

By rearranging the terms, we obtain:

$$I' = \int_{0}^{\pi/2} \cos^{k_{1}} t_{1} \sin^{k_{2}+...+k_{N}+N-2} t_{1} dt_{1}$$
$$\int_{0}^{\pi/2} \cos^{k_{2}} t_{2} \sin^{k_{3}+...+k_{N}+N-3} t_{2} dt_{2}$$
$$\vdots$$
$$\int_{0}^{\pi/2} \cos^{k_{N-2}} t_{N-2} \sin^{k_{N-1}+k_{N}+1} t_{N-2} dt_{N-2}$$
$$\int_{0}^{\pi/2} \cos^{k_{N-1}} t_{N-1} \sin^{k_{N}} t_{N-1} dt_{N-1}$$

Now by using the formula in Theorem 13.2, this gives:

$$I' = \frac{k_1!!(k_2 + \ldots + k_N + N - 2)!!}{(k_1 + \ldots + k_N + N - 1)!!} \left(\frac{\pi}{2}\right)^{\varepsilon(N-2)}$$

$$\frac{k_2!!(k_3 + \ldots + k_N + N - 3)!!}{(k_2 + \ldots + k_N + N - 2)!!} \left(\frac{\pi}{2}\right)^{\varepsilon(N-3)}$$

$$\vdots$$

$$\frac{k_{N-2}!!(k_{N-1} + k_N + 1)!!}{(k_{N-2} + k_{N-1} + k_N + 2)!!} \left(\frac{\pi}{2}\right)^{\varepsilon(1)}$$

$$\frac{k_{N-1}!!k_N!!}{(k_{N-1} + k_N + 1)!!} \left(\frac{\pi}{2}\right)^{\varepsilon(0)}$$

Now observe that the various double factorials multiply up to quantity in the statement, modulo a (N-1)!! factor, and that the $\pi/2$ factors multiply up to:

$$F = \left(\frac{\pi}{2}\right)^{[N/2]}$$

Thus by multiplying by the normalization constant, we obtain the result.

We can now recover the normal laws, geometrically, as follows:

THEOREM 13.6. The moments of the hyperspherical variables are

$$\int_{S^{N-1}_{\mathbb{R}}} x_i^p dx = \frac{(N-1)!!p!!}{(N+p-1)!!}$$

and the rescaled variables $y_i = \sqrt{N}x_i$ become normal and independent with $N \to \infty$.

PROOF. The moment formula in the statement follows from Theorem 13.5. As a consequence, with $N \to \infty$ we have the following estimate:

$$\int_{S_{\mathbb{R}}^{N^{-1}}} x_i^p dx \simeq N^{-p/2} \times p!! = N^{-p/2} M_p(g_1)$$

Thus, the rescaled variables $\sqrt{N}x_i$ become normal with $N \to \infty$, as claimed. As for the proof of the asymptotic independence, this is standard too, once again by using the formula in Theorem 13.5. Indeed, the joint moments of x_1, \ldots, x_N are given by:

$$\int_{S_{\mathbb{R}}^{N-1}} x_1^{k_1} \dots x_N^{k_N} \, dx = \frac{(N-1)!! k_1 !! \dots k_N !!}{(N+\Sigma k_i - 1)!!} \simeq N^{-\Sigma k_i} \times k_1 !! \dots k_N !!$$

By rescaling, the joint moments of the variables $y_i = \sqrt{N}x_i$ are given by:

$$\int_{S_{\mathbb{R}}^{N-1}} y_1^{k_1} \dots y_N^{k_N} \, dx \simeq k_1 !! \dots k_N !!$$

Thus, we have multiplicativity, and so independence with $N \to \infty$, as claimed. \Box

As a last result about the normal laws, we can recover these as well in connection with rotation groups. Indeed, we have the following reformulation of Theorem 13.6:

THEOREM 13.7. We have the integration formula

$$\int_{O_N} U_{ij}^p \, dU = \frac{(N-1)!!p!!}{(N+p-1)!!}$$

and the rescaled variables $V_{ij} = \sqrt{N}U_{ij}$ become normal and independent with $N \to \infty$.

PROOF. We use the basic fact that the rotations $U \in O_N$ act on the points of the real sphere $z \in S_{\mathbb{R}}^{N-1}$, with the stabilizer of z = (1, 0, ..., 0) being the subgroup $O_{N-1} \subset O_N$. In algebraic terms, this gives an identification as follows:

$$S_{\mathbb{R}}^{N-1} = O_N / O_{N-1}$$

In functional analytic terms, this result provides us with an embedding as follows, for any i, which makes correspond the respective integration functionals:

$$C(S^{N-1}_{\mathbb{R}}) \subset C(O_N) \quad , \quad x_i \to U_{1i}$$

With this identification made, the result follows from Theorem 13.6.

13b. Complex variables

We have seen so far a number of interesting results regarding the normal laws, and their geometric interpretation. As a next topic for this chapter, let us discuss now the complex analogues of all this. To start with, we have the following definition:

DEFINITION 13.8. The complex Gaussian law of parameter t > 0 is

$$G_t = law\left(\frac{1}{\sqrt{2}}(a+ib)\right)$$

where a, b are independent, each following the law g_t .

As in the real case, these measures form convolution semigroups:

THEOREM 13.9. The complex Gaussian laws have the property

$$G_s * G_t = G_{s+t}$$

for any s, t > 0, and so they form a convolution semigroup.

PROOF. This follows indeed from the real result, namely $g_s * g_t = g_{s+t}$, established before, simply by taking real and imaginary parts.

We have as well the following complex analogue of the CLT:

THEOREM 13.10 (CCLT). Given complex variables $f_1, f_2, f_3, \ldots \in L^{\infty}(X)$ which are *i.i.d.*, centered, and with common variance t > 0, we have

$$\frac{1}{\sqrt{n}}\sum_{i=1}^n f_i \sim G_t$$

with $n \to \infty$, in moments.

PROOF. This follows indeed from the real CLT, established before, simply by taking the real and imaginary parts of all variables involved. \Box

Regarding now the moments, the situation is more complicated than in the real case, because in order to have good results, we have to deal with both the complex variables, and their conjugates. Let us formulate the following definition:

DEFINITION 13.11. The moments a complex variable $f \in L^{\infty}(X)$ are the numbers

$$M_k = E(f^k)$$

depending on colored integers $k = \circ \bullet \bullet \circ \ldots$, with the conventions

 $f^{\emptyset} = 1$, $f^{\circ} = f$, $f^{\bullet} = \bar{f}$

and multiplicativity, in order to define the colored powers f^k .

Observe that, since f, \bar{f} commute, we can permute terms, and restrict the attention to exponents of type $k = \ldots \circ \circ \circ \bullet \bullet \bullet \bullet \ldots$, if we want to. However, our result about the complex Gaussian laws, and other complex laws, later on, will actually look better without doing is, and so we will use Definition 13.11 as stated. We first have:

THEOREM 13.12. The moments of the complex normal law are given by

$$M_k(G_t) = \begin{cases} t^p p! & (k \text{ uniform, of length } 2p) \\ 0 & (k \text{ not uniform}) \end{cases}$$

where $k = \circ \bullet \circ \circ \ldots$ is called uniform when it contains the same number of \circ and \bullet .

PROOF. We must compute the moments, with respect to colored integer exponents $k = \circ \bullet \bullet \circ \ldots$, of the variable from Definition 13.8, namely:

$$f = \frac{1}{\sqrt{2}}(a+ib)$$

We can assume that we are in the case t = 1, and the proof here goes as follows:

(1) As a first observation, in the case where our exponent $k = \circ \bullet \circ \circ \ldots$ is not uniform, a standard rotation argument shows that the corresponding moment of f vanishes. To be more precise, the variable f' = wf is complex Gaussian too, for any complex number $w \in \mathbb{T}$, and from $M_k(f) = M_k(f')$ we obtain $M_k(f) = 0$, in this case.

(2) In the uniform case now, where the exponent $k = \circ \bullet \circ \circ \ldots$ consists of p copies of \circ and p copies of \bullet , the corresponding moment can be computed as follows:

$$M_{k} = \int (f\bar{f})^{p}$$

$$= \frac{1}{2^{p}} \int (a^{2} + b^{2})^{p}$$

$$= \frac{1}{2^{p}} \sum_{r} {p \choose r} \int a^{2r} \int b^{2p-2r}$$

$$= \frac{1}{2^{p}} \sum_{r} {p \choose r} (2r)!! (2p-2r)!!$$

$$= \frac{1}{2^{p}} \sum_{r} \frac{p!}{r!(p-r)!} \cdot \frac{(2r)!}{2^{r}r!} \cdot \frac{(2p-2r)!}{2^{p-r}(p-r)!}$$

$$= \frac{p!}{4^{p}} \sum_{r} {2r \choose r} {2p-2r \choose p-r}$$

(3) In order to finish now the computation, let us recall that we have the following formula, coming from the generalized binomial formula, or from the Taylor formula:

$$\frac{1}{\sqrt{1+t}} = \sum_{q=0}^{\infty} \binom{2q}{q} \left(\frac{-t}{4}\right)^q$$

By taking the square of this series, we obtain the following formula:

$$\frac{1}{1+t} = \sum_{qr} {2q \choose q} {2r \choose r} \left(\frac{-t}{4}\right)^{q+r}$$
$$= \sum_{p} \left(\frac{-t}{4}\right)^{p} \sum_{r} {2r \choose r} {2p-2r \choose p-r}$$

Now by looking at the coefficient of t^p on both sides, we conclude that the sum on the right equals 4^p . Thus, we can finish the moment computation in (2), as follows:

$$M_k = \frac{p!}{4^p} \times 4^p = p!$$

We are therefore led to the conclusion in the statement.

Given a colored integer $k = \circ \bullet \circ \circ \ldots$, we say that a pairing $\pi \in P_2(k)$ is matching when it pairs $\circ - \bullet$ symbols. With this convention, we have the following result:

THEOREM 13.13. The moments of the complex normal law are the numbers

$$M_k(G_t) = \sum_{\pi \in \mathcal{P}_2(k)} t^{|\pi|}$$

where $\mathcal{P}_2(k)$ are the matching pairings of $\{1, \ldots, k\}$, and |.| is the number of blocks.

PROOF. This is a reformulation of Theorem 13.12. Indeed, we can assume that we are in the case t = 1, and here we know from Theorem 13.12 that the moments are:

$$M_{k} = \begin{cases} (|k|/2)! & (k \text{ uniform}) \\ 0 & (k \text{ not uniform}) \end{cases}$$

On the other hand, the numbers $|\mathcal{P}_2(k)|$ are given by exactly the same formula. Indeed, in order to have a matching pairing of k, our exponent $k = \circ \bullet \circ \circ \ldots$ must be uniform, consisting of p copies of \circ and p copies of \bullet , with p = |k|/2. But then the matching pairings of k correspond to the permutations of the \bullet symbols, as to be matched with \circ symbols, and so we have p! such pairings. Thus, we have the same formula as for the moments of f, and we are led to the conclusion in the statement. \Box

In practice, we also need to know how to compute joint moments of independent normal variables. We have here the following result, to be heavily used later on:

THEOREM 13.14 (Wick formula). Given independent variables f_i , each following the complex normal law G_t , with t > 0 being a fixed parameter, we have the formula

$$E\left(f_{i_1}^{k_1}\dots f_{i_s}^{k_s}\right) = t^{s/2} \#\left\{\pi \in \mathcal{P}_2(k) \middle| \pi \le \ker i\right\}$$

where $k = k_1 \dots k_s$ and $i = i_1 \dots i_s$, for the joint moments of these variables, where $\pi \leq \ker i$ means that the indices of i must fit into the blocks of π , in the obvious way.

13B. COMPLEX VARIABLES

PROOF. This is something well-known, which can be proved as follows:

(1) Let us first discuss the case where we have a single variable f, which amounts in taking $f_i = f$ for any i in the formula in the statement. What we have to compute here are the moments of f, with respect to colored integer exponents $k = \circ \bullet \circ \ldots$, and the formula in the statement tells us that these moments must be:

$$E(f^k) = t^{|k|/2} |\mathcal{P}_2(k)|$$

But this is the formula in Theorem 13.13, so we are done with this case.

(2) In general now, when expanding the product $f_{i_1}^{k_1} \dots f_{i_s}^{k_s}$ and rearranging the terms, we are left with doing a number of computations as in (1), and then making the product of the expectations that we found. But this amounts in counting the partitions in the statement, with the condition $\pi \leq \ker i$ there standing for the fact that we are doing the various type (1) computations independently, and then making the product. \Box

Getting back now to geometric aspects, we first have the following result:

THEOREM 13.15. We have the following integration formula over the complex sphere $S_{\mathbb{C}}^{N-1} \subset \mathbb{C}^N$, with respect to the normalized uniform measure,

$$\int_{S_{\mathbb{C}}^{N-1}} |z_1|^{2k_1} \dots |z_N|^{2k_N} dz = \frac{(N-1)!k_1!\dots k_n!}{(N+\sum k_i-1)!}$$

valid for any exponents $k_i \in \mathbb{N}$. As for the other polynomial integrals in z_1, \ldots, z_N and their conjugates $\bar{z}_1, \ldots, \bar{z}_N$, these all vanish.

PROOF. Consider an arbitrary polynomial integral over $S_{\mathbb{C}}^{N-1}$, written as follows:

$$I = \int_{S_{\mathbb{C}}^{N-1}} z_{i_1} \bar{z}_{i_2} \dots z_{i_{2k-1}} \bar{z}_{i_{2k}} \, dz$$

By using transformations of type $p \to \lambda p$ with $|\lambda| = 1$, we see that this integral I vanishes, unless each z_a appears as many times as \bar{z}_a does, and this gives the last assertion. So, assume now that we are in the non-vanishing case. Then the k_a copies of z_a and the k_a copies of \bar{z}_a produce by multiplication a factor $|z_a|^{2k_a}$, so we have:

$$I = \int_{S_{\mathbb{C}}^{N-1}} |z_1|^{2k_1} \dots |z_N|^{2k_N} \, dz$$

Now by using the standard identification $S_{\mathbb{C}}^{N-1} \simeq S_{\mathbb{R}}^{2N-1}$, we obtain:

$$I = \int_{S_{\mathbb{R}}^{2N-1}} (x_1^2 + y_1^2)^{k_1} \dots (x_N^2 + y_N^2)^{k_N} d(x, y)$$

=
$$\sum_{r_1 \dots r_N} \binom{k_1}{r_1} \dots \binom{k_N}{r_N} \int_{S_{\mathbb{R}}^{2N-1}} x_1^{2k_1 - 2r_1} y_1^{2r_1} \dots x_N^{2k_N - 2r_N} y_N^{2r_N} d(x, y)$$

By using the formula in Theorem 13.5, we obtain:

$$I = \sum_{r_1...r_N} \binom{k_1}{r_1} \dots \binom{k_N}{r_N} \frac{(2N-1)!!(2r_1)!!\dots(2r_N)!!(2k_1-2r_1)!!\dots(2k_N-2r_N)!!}{(2N+2\sum k_i-1)!!}$$

$$= \sum_{r_1...r_N} \binom{k_1}{r_1} \dots \binom{k_N}{r_N} \frac{2^{N-1}(N-1)!\prod(2r_i)!/(2^{r_i}r_i!)\prod(2k_i-2r_i)!/(2^{k_i-r_i}(k_i-r_i)!)}{2^{N+\sum k_i-1}(N+\sum k_i-1)!}$$

$$= \sum_{r_1...r_N} \binom{k_1}{r_1} \dots \binom{k_N}{r_N} \frac{(N-1)!(2r_1)!\dots(2r_N)!(2k_1-2r_1)!\dots(2k_N-2r_N)!}{4\sum k_i(N+\sum k_i-1)!r_1!\dots r_N!(k_1-r_1)!\dots(k_N-r_N)!}$$

Now observe that can rewrite this quantity in the following way:

$$I = \sum_{r_1...r_N} \frac{k_1! \dots k_N! (N-1)! (2r_1)! \dots (2r_N)! (2k_1 - 2r_1)! \dots (2k_N - 2r_N)!}{4^{\sum k_i} (N + \sum k_i - 1)! (r_1! \dots r_N! (k_1 - r_1)! \dots (k_N - r_N)!)^2}$$

$$= \sum_{r_1} \binom{2r_1}{r_1} \binom{2k_1 - 2r_1}{k_1 - r_1} \dots \sum_{r_N} \binom{2r_N}{r_N} \binom{2k_N - 2r_N}{k_N - r_N} \frac{(N-1)!k_1! \dots k_N!}{4^{\sum k_i} (N + \sum k_i - 1)!}$$

$$= 4^{k_1} \times \dots \times 4^{k_N} \times \frac{(N-1)!k_1! \dots k_N!}{4^{\sum k_i} (N + \sum k_i - 1)!}$$

$$= \frac{(N-1)!k_1! \dots k_N!}{(N + \sum k_i - 1)!}$$

Thus, we obtain the formula in the statement.

Regarding now the hyperspherical variables, we have here the following result:

THEOREM 13.16. The rescalings $\sqrt{N}z_i$ of the unit complex sphere coordinates

 $z_i: S^{N-1}_{\mathbb{C}} \to \mathbb{C}$

as well as the rescalings $\sqrt{N}U_{ij}$ of the unitary group coordinates

 $U_{ij}: U_N \to \mathbb{C}$

become complex Gaussian and independent with $N \to \infty$.

PROOF. We have several assertions to be proved, the idea being as follows:

(1) According to the formula in Theorem 13.15, the polynomials integrals in z_i, \bar{z}_i vanish, unless the number of z_i, \bar{z}_i is the same. In this latter case these terms can be grouped together, by using $z_i \bar{z}_i = |z_i|^2$, and the relevant integration formula is:

$$\int_{S_{\mathbb{C}}^{N-1}} |z_i|^{2k} \, dz = \frac{(N-1)!k!}{(N+k-1)!}$$

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

$$\int_{S_{\mathbb{C}}^{N-1}} |z_i|^{2k} dx \simeq N^{-k} \times k!$$

Thus, the rescaled variables $\sqrt{N}z_i$ become normal with $N \to \infty$, as claimed.

(2) As for the proof of the asymptotic independence, this is standard too, again by using Theorem 13.15. Indeed, the joint moments of z_1, \ldots, z_N are given by:

$$\int_{S_{\mathbb{R}}^{N-1}} |z_1|^{2k_1} \dots |z_N|^{2k_N} dx = \frac{(N-1)!k_1! \dots k_n!}{(N+\sum k_i-1)!} \\ \simeq N^{-\Sigma k_i} \times k_1! \dots k_N!$$

By rescaling, the joint moments of the variables $y_i = \sqrt{N}z_i$ are given by:

$$\int_{S_{\mathbb{R}}^{N-1}} |y_1|^{2k_1} \dots |y_N|^{2k_N} \, dx \simeq k_1! \dots k_N!$$

Thus, we have multiplicativity, and so independence with $N \to \infty$, as claimed.

(3) Regarding the last assertion, we can use the basic fact that the rotations $U \in U_N$ act on the points of the sphere $z \in S_{\mathbb{C}}^{N-1}$, with the stabilizer of z = (1, 0, ..., 0) being the subgroup $U_{N-1} \subset U_N$. In algebraic terms, this gives an identification as follows:

$$S_{\mathbb{C}}^{N-1} = U_N / U_{N-1}$$

In functional analytic terms, this result provides us with an embedding as follows, for any i, which makes correspond the respective integration functionals:

$$C(S^{N-1}_{\mathbb{C}}) \subset C(U_N) \quad , \quad x_i \to U_{1i}$$

With this identification made, the result follows from (1,2).

13c. Poisson laws

Derangements. Poisson laws. Compound Poisson. Bessel laws.

13d. Asymptotic characters

As a last objective, for the remainder of this chapter, we would like to compute the asymptotic laws of main characters $\chi = \chi_v$ for the main examples of easy groups. And here, 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 $v^{\otimes k}$.

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):

$$\xi_{\pi} = \sum_{i_1 \dots i_k} \delta_{\pi} \begin{pmatrix} i_1 & \dots & i_k \end{pmatrix} e_{i_1} \otimes \dots \otimes e_{i_k}$$

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 now linear independence questions for the vectors ξ_{π} , we will use the Gram matrix of these vectors. Let us begin with some standard definitions, as follows:

DEFINITION 13.17. 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 $\pi \lor \nu \in P(k)$ be the partition obtained by superposing π, ν .

As an illustration here, at k = 2 we have $P(2) = \{||, \square\}$, and the order is:

$$\parallel \leq \sqcap$$

At k = 3 we have $P(3) = \{|||, \Box|, \Box, \Box, \Box\}$, and the order relation is as follows: $||| \leq \Box|, \Box, |\Box \leq \Box\Box$

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 13.18. The Gram matrix $G_{kN}(\pi,\nu) = \langle \xi_{\pi}, \xi_{\nu} \rangle$ 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:

$$\langle \xi_{\pi}, \xi_{\nu} \rangle = \sum_{i_{1}...i_{k}} \delta_{\pi}(i_{1},...,i_{k}) \delta_{\nu}(i_{1},...,i_{k})$$
$$= \sum_{i_{1}...i_{k}} \delta_{\pi \lor \nu}(i_{1},...,i_{k})$$
$$= N^{|\pi \lor \nu|}$$

Thus, we have obtained the formula in the statement.

Now recall from chapter 8 that we have the following result:

THEOREM 13.19. 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 $N \ge k$, the vectors $\{\xi_{\pi} | \pi \in P(k)\}$ are linearly independent.

PROOF. This is indeed something very standard, that we know from chapter 8.

Now back to the laws of characters, we can formulate:

THEOREM 13.20. 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 13.19.

With these preliminaries in hand, we can now state and prove:

THEOREM 13.21. 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,



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:



Thus, we can use Theorem 13.20, are we are led into counting partitions, and then recovering the measures via their moments, which can be done as follows:

(1) For O_N the associated category of partitions is P_2 , so the asymptotic moments of the main character are as follows, with the convention k!! = 0 when k is odd:

$$M_k = \# P_2(k) = k!$$

Thus, we obtain the real Gaussian law, as desired.

(2) For U_N , this follows from some combinatorics. To be more precise, the asymptotic moments of the main character, with respect to the colored integers, are as follows:

$$M_k = \# \mathcal{P}_2(k)$$

Thus, we obtain this time the complex Gaussian law, as desired.

(3) For the discrete counterparts H_N, K_N of the rotation groups O_N, U_N the situation is similar, and we obtain the real and complex Bessel laws.

13e. Exercises

Exercises:

EXERCISE 13.22.

EXERCISE 13.23.

- Exercise 13.24.
- EXERCISE 13.25.

EXERCISE 13.26.

EXERCISE 13.27.

EXERCISE 13.28.

EXERCISE 13.29.

Bonus exercise.

Weingarten calculus

14a. Weingarten formula

We have seen in the previous chapter that some conceptual probability theory, based on the notion of easiness, and generalizing several ad-hoc computations from Parts I-II, can be developed for the main examples of rotation and reflection groups, namely:



Our purpose here will be that of further building on this. Based on the notion of easiness, we will develop an advanced integration theory for the easy groups. This theory, known as "Weingarten calculus", following [95], will allow us in particular to extend our t = 1 character results to the general case, involving a parameter $t \in (0, 1]$. Let us start with a general formula that we know from chapter 5, namely:

THEOREM 14.1. 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

$$\int_G g_{i_1j_1}^{e_1} \dots g_{i_kj_k}^{e_k} dg = \sum_{\pi,\nu \in D(k)} \delta_\pi(i) \delta_\sigma(j) W_k(\pi,\nu)$$

valid for any colored integer $k = e_1 \dots e_k$ 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 that we know from chapter 5, the idea being that the integrals in the statement, with the multi-indices i, j varying, form altogether the orthogonal projection onto the space $Fix(v^{\otimes k}) = span(D(k))$. But this projection can be computed by doing some linear algebra, and this gives the formula in the statement.

In the easy case, we have the following more concrete result:

14. WEINGARTEN CALCULUS

THEOREM 14.2. For an easy group $G \subset U_N$, coming from a category of partitions D = (D(k, l)), we have the Weingarten formula

$$\int_{G} g_{i_1 j_1}^{e_1} \dots g_{i_k j_k}^{e_k} \, dg = \sum_{\pi, \nu \in D(k)} \delta_{\pi}(i) \delta_{\nu}(j) W_{kN}(\pi, \nu)$$

for any $k = e_1 \dots e_k$ 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 14.1. Indeed, the Kronecker type symbols there are then the usual ones, as shown by:

$$\delta_{\xi_{\pi}}(i) = \langle \xi_{\pi}, e_{i_1} \otimes \ldots \otimes e_{i_k} \rangle$$

= $\left\langle \sum_{j} \delta_{\pi}(j_1, \ldots, j_k) e_{j_1} \otimes \ldots \otimes e_{j_k}, e_{i_1} \otimes \ldots \otimes e_{i_k} \right\rangle$
= $\delta_{\pi}(i_1, \ldots, i_k)$

The Gram matrix being as well the correct one, we obtain the result.

As a toy example for the Weingarten formula, let us first work out the case of the symmetric group S_N . Here there is no really need for the Weingarten formula, because we have the following elementary result, which completely solves the problem:

PROPOSITION 14.3. The integrals over $S_N \subset O_N$ are given by

$$\int_{S_N} g_{i_1 j_1} \dots g_{i_k j_k} \, dg = \begin{cases} \frac{(N - |\ker i|)!}{N!} & \text{if } \ker i = \ker j \\ 0 & \text{otherwise} \end{cases}$$

where |.| denotes as usual the number of blocks.

PROOF. This is something that we know from chapter 13, but let us recall the proof. Since the embedding $S_N \subset O_N$ is given by $g_{ij} = \delta_{\sigma(j)i}$, we have:

$$\int_{S_N} g_{i_1 j_1} \dots g_{i_k j_k} \, dg = \frac{1}{N!} \# \left\{ g \in S_N \left| g(j_1) = i_1, \dots, g(j_k) = i_k \right\} \right\}$$

In the case ker $i \neq \text{ker } j$ there is no $g \in S_N$ as above, and the integral vanishes. As for the case left, namely ker i = ker j, here 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 - bpoints, and so (N - b)! solutions, and the integral is $\frac{(N-b)!}{N!}$, as claimed. \Box

Getting back now to Weingarten matrices, the point is that Proposition 14.3 allows their precise computation, and evaluation, the result being as follows:

180
THEOREM 14.4. For S_N the Weingarten function is given by

$$W_{kN}(\pi,\nu) = \sum_{\tau \le \pi \land \nu} \mu(\tau,\pi) \mu(\tau,\nu) \frac{(N-|\tau|)!}{N!}$$

and satisfies the following estimate,

$$W_{kN}(\pi,\nu) = N^{-|\pi\wedge\nu|}(\mu(\pi\wedge\nu,\pi)\mu(\pi\wedge\nu,\nu) + O(N^{-1}))$$

with μ being the Möbius function of P(k).

PROOF. The first assertion follows from the Weingarten formula, namely:

$$\int_{S_N} g_{i_1 j_1} \dots g_{i_k j_k} \, dg = \sum_{\pi, \nu \in P(k)} \delta_\pi(i) \delta_\nu(j) W_{kN}(\pi, \nu)$$

Indeed, in this formula the integrals on the left are known, from the explicit integration formula over S_N that we established in Proposition 14.3, namely:

$$\int_{S_N} g_{i_1 j_1} \dots g_{i_k j_k} \, dg = \begin{cases} \frac{(N - |\ker i|)!}{N!} & \text{if } \ker i = \ker j \\ 0 & \text{otherwise} \end{cases}$$

But this allows the computation of the right term, via the Möbius inversion formula, from chapter 13. As for the second assertion, this follows from the first one. \Box

The above result is of course something very special, coming from the fact that the integration over S_N is something very simple. For other groups, such as the orthogonal group O_N or the unitary group U_N , we will see that things are far more complicated.

14b. Basic estimates

Let us discuss now the computation of the polynomial integrals over the orthogonal group O_N . These are best introduced in a rectangular way, as follows:

DEFINITION 14.5. Associated to any matrix $a \in M_{p \times q}(\mathbb{N})$ is the integral

$$I(a) = \int_{O_N} \prod_{i=1}^{p} \prod_{j=1}^{q} v_{ij}^{a_{ij}} \, dv$$

with respect to the Haar measure of O_N , where $N \ge p, q$.

We can of course complete our matrix with 0 values, as to always deal with square matrices, $a \in M_N(\mathbb{N})$. However, the parameters p, q are very useful, because they measure the complexity of the problem, as shown by our various results below. Let us set as usual $m!! = (m-1)(m-3)(m-5)\ldots$, with the product ending at 1 or 2, depending on the parity of m. With this convention, we have the following result:

PROPOSITION 14.6. At p = 1 we have the formula

$$I(a_1 \ldots a_q) = \varepsilon \cdot \frac{(N-1)!!a_1!! \ldots a_q!!}{(N+\Sigma a_i-1)!!}$$

where $\varepsilon = 1$ if all a_i are even, and $\varepsilon = 0$ otherwise.

PROOF. This follows from the fact, already used in chapter 13, that the first slice of O_N is isomorphic to the real sphere $S_{\mathbb{R}}^{N-1}$. Indeed, this gives the following formula:

$$I(a_1 \ldots a_q) = \int_{S^{N-1}_{\mathbb{R}}} x_1^{a_1} \ldots x_q^{a_q} dx$$

But this latter integral can be computed by using polar coordinates, as explained in chapter 13, and we obtain the formula in the statement. \Box

Another simple computation, as well of trigonometric nature, is the one at N = 2. We have here the following result, which completely solves the problem in this case:

PROPOSITION 14.7. At N = 2 we have the formula

$$I\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \varepsilon \cdot \frac{(a+d)!!(b+c)!!}{(a+b+c+d+1)!!}$$

where $\varepsilon = 1$ if a, b, c, d are even, $\varepsilon = -1$ is a, b, c, d are odd, and $\varepsilon = 0$ if not.

PROOF. When computing the integral over O_2 , we can restrict the integration to $SO_2 = \mathbb{T}$, then further restrict the attention to the first quadrant. We obtain:

$$I\begin{pmatrix}a&b\\c&d\end{pmatrix} = \varepsilon \cdot \frac{2}{\pi} \int_0^{\pi/2} (\cos t)^{a+d} (\sin t)^{b+c} dt$$

But this gives the formula in the statement, via the formulae in chapter 13.

The above computations tend to suggest that I(a) decomposes as a product of factorials. This is far from being true, but in the 2 × 2 case it is known that I(a) decomposes as a quite reasonable sum of products of factorials. We will be back to this. In general now, we can compute the integrals I(a) by using the Weingarten formula:

THEOREM 14.8. We have the Weingarten formula

$$\int_{O_N} v_{i_1 j_1} \dots v_{i_{2k} j_{2k}} dv = \sum_{\pi, \nu \in D_k} \delta_\pi(i) \delta_\nu(j) W_{kN}(\pi, \nu)$$

where the objects on the right are as follows:

- (1) D_k is the set of pairings of $\{1, \ldots, 2k\}$.
- (2) The delta symbols are 1 or 0, depending on whether indices fit or not.
- (3) The Weingarten matrix is $W_{kN} = G_{kN}^{-1}$, where $G_{kN}(\pi, \nu) = N^{|\pi \vee \nu|}$.

PROOF. This is indeed the usual Weingarten formula, for $G = O_N$.

182

As an example, the integrals of quantities of type $v_{i_1j_1}v_{i_2j_2}v_{i_3j_3}u_{i_4j_4}$ appear as sums of coefficients of the Weingarten matrix W_{2N} , which is given by:

$$W_{2N} = \begin{pmatrix} N^2 & N & N \\ N & N^2 & N \\ N & N & N^2 \end{pmatrix}^{-1} = \frac{1}{N(N-1)(N+2)} \begin{pmatrix} N+1 & -1 & -1 \\ -1 & N+1 & -1 \\ -1 & -1 & N+1 \end{pmatrix}$$

More precisely, the various consequences at k = 2 can be summarized as follows:

PROPOSITION 14.9. We have the following results:

(1) $I_{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}} = 3/(N(N+2)).$ (2) $I_{\begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}} = 1/(N(N+2)).$ (3) $I_{\begin{pmatrix} 0 & 2 \\ 0 & 2 \end{pmatrix}} = (N+1)/(N(N-1)(N+2)).$

PROOF. These results all follow from the Weingarten formula, by using the above numeric values for the entries of W_{2N} , the computations being as follows:

$$I\begin{pmatrix} 4 & 0\\ 0 & 0 \end{pmatrix} = \int v_{11}v_{11}v_{11}v_{11} = \sum_{\pi\sigma} W_{2N}(\pi,\sigma) = \frac{3(N+1)-6}{N(N-1)(N+2)} = \frac{3}{N(N+2)}$$
$$I\begin{pmatrix} 2 & 2\\ 0 & 0 \end{pmatrix} = \int v_{11}v_{11}v_{12}v_{12} = \sum_{\pi} W_{2N}(\pi,\cap\cap) = \frac{(N+1)-2}{N(N-1)(N+2)} = \frac{1}{N(N+2)}$$
$$I\begin{pmatrix} 2 & 0\\ 0 & 2 \end{pmatrix} = \int v_{11}v_{11}v_{22}v_{22} = W_{2N}(\cap\cap,\cap\cap) = \frac{N+1}{N(N-1)(N+2)}$$

Observe that the first two formulae follow in fact as well from Proposition 14.6. \Box

In terms of the integrals I(a), the Weingarten formula reformulates as follows:

THEOREM 14.10. We have the Weingarten formula

$$I(a) = \sum_{\pi,\nu} \delta_{\pi}(a_l) \delta_{\nu}(a_r) W_{kN}(\pi,\nu)$$

where $k = \sum a_{ij}/2$, and where the multi-indices a_l/a_r are defined as follows:

- (1) Start with $a \in M_{p \times q}(\mathbb{N})$, and replace each *ij*-entry by a_{ij} copies of i/j.
- (2) Read this matrix in the usual way, as to get the multi-indices a_l/a_r .

PROOF. This is simply a reformulation of the usual Weingarten formula. Indeed, according to our definitions, the integral in the statement is given by:

$$I(a) = \int_{O_N} \underbrace{v_{11} \dots v_{11}}_{a_{11}} \underbrace{v_{12} \dots v_{12}}_{a_{12}} \dots \underbrace{v_{pq} \dots v_{pq}}_{a_{pq}} du$$

Thus what we have here is an integral as in Theorem 14.8, the multi-indices being:

$$a_{l} = (\underbrace{1 \dots 1}_{a_{11}} \underbrace{1 \dots 1}_{a_{12}} \dots \underbrace{p \dots p}_{a_{pq}})$$
$$a_{r} = (\underbrace{1 \dots 1}_{a_{11}} \underbrace{2 \dots 2}_{a_{12}} \dots \underbrace{q \dots q}_{a_{pq}})$$

With this observation, the result follows now from the Weingarten formula.

We can now extend the various vanishing results appearing before, as follows:

PROPOSITION 14.11. We have I(a) = 0, unless the matrix a is "admissible", in the sense that all p + q sums on its rows and columns are even numbers.

PROOF. Observe first that the left multi-index associated to a consists of $k_1 = \sum a_{1j}$ copies of 1, $k_2 = \sum a_{2j}$ copies of 2, and so on, up to $k_p = \sum a_{pj}$ copies of p. In the case where one of these numbers is odd we have $\delta_{\pi}(a) = 0$ for any π , and so I(a) = 0. A similar argument with the right multi-index associated to a shows that the sums on the columns of a must be even as well, and we are done.

A natural question now is whether the converse of Proposition 14.11 holds, and if so, the question of computing the sign of I(a) appears as well. These are both subtle questions, and we begin our investigations with a $N \to \infty$ study. We have here:

THEOREM 14.12. The Weingarten matrix is asymptotically diagonal, in the sense that:

$$W_{kN}(\pi,\nu) = N^{-k}(\delta_{\pi\nu} + O(N^{-1}))$$

Moreover, the $O(N^{-1})$ remainder is asymptotically smaller that $(2k/e)^k N^{-1}$.

PROOF. It is convenient, for the purposes of this proof, to drop the indices k, N. We know that the Gram matrix is given by $G(\pi, \nu) = N^{|\pi \vee \nu|}$, so we have:

$$G(\pi,\nu) = \begin{cases} N^k & \text{for } \pi = \nu \\ N, N^2, \dots, N^{k-1} & \text{for } \pi \neq \nu \end{cases}$$

Thus the Gram matrix is of the following form, with $||H||_{\infty} \leq N^{-1}$:

$$G = N^k (I + H)$$

Now recall that for any complex $K \times K$ matrix A, we have the following lineup of standard inequalities, which all follow from definitions:

$$||A||_{\infty} \le ||A|| \le ||A||_2 \le K ||A||_{\infty}$$

In the case of our matrix H, the size is this matrix is K = (2k)!!, so we have:

$$||H|| \le KN^{-1}$$

We can perform the inversion operation, by using the following formula:

$$(I+H)^{-1} = I - H + H^2 - H^3 + \dots$$

We obtain in this way the following estimate:

$$||I - (I + H)^{-1}|| \le \frac{||H||}{1 - ||H||}$$

Thus, we have the following estimate:

$$|I - N^{k}W||_{\infty} = ||I - (1 + H)^{-1}||_{\infty}$$

$$\leq ||I - (1 + H)^{-1}||$$

$$\leq \frac{||H||}{1 - ||H||}$$

$$\leq \frac{KN^{-1}}{1 - KN^{-1}}$$

$$= \frac{K}{N - K}$$

Together with the Stirling estimate $K \approx (2k/e)^k$, this gives the result.

Regarding now the integrals themselves, we have here the following result:

THEOREM 14.13. We have the estimate

$$I(a) = N^{-k} \left(\prod_{i=1}^{p} \prod_{j=1}^{q} a_{ij} !! + O(N^{-1}) \right)$$

when all a_{ij} are even, and $I(a) = O(N^{-k-1})$ otherwise.

PROOF. By using the above results, we have the following estimate:

$$I(a) = \sum_{\pi,\nu} \delta_{\pi}(a_{l}) \delta_{\nu}(a_{r}) W_{kN}(\pi,\nu)$$

= $N^{-k} \sum_{\pi,\nu} \delta_{\pi}(a_{l}) \delta_{\nu}(a_{r}) (\delta_{\pi\nu} + O(N^{-1}))$
= $N^{-k} \left(\# \{\pi | \delta_{\pi}(a_{l}) = \delta_{\pi}(a_{r}) = 1\} + O(N^{-1}) \right)$

In order to count now the partitions appearing in the last set, let us go back to the multi-indices a_l, a_r , as described in Theorem 14.10. It is convenient to view both these

multi-indices in a rectangular way, in the following way:

$$a_{l} = \begin{pmatrix} \underbrace{1 \dots 1}_{a_{11}} \dots \underbrace{1 \dots 1}_{a_{1q}} \\ \dots & \dots \\ \underbrace{p \dots p}_{a_{p1}} \dots \underbrace{p \dots p}_{a_{pq}} \end{pmatrix} \quad , \quad a_{r} = \begin{pmatrix} \underbrace{1 \dots 1}_{a_{11}} \dots \underbrace{q \dots q}_{a_{1q}} \\ \dots & \dots \\ \underbrace{1 \dots 1}_{a_{p1}} \dots \underbrace{p \dots p}_{a_{pq}} \end{pmatrix}$$

In other words, the multi-indices a_l/a_r are simply obtained from the matrix a by "dropping" from each entry a_{ij} a sequence of a_{ij} numbers, all equal to i/j. With this picture, the pairings π which contribute are simply those connecting sequences of indices "dropped" from the same a_{ij} , and this gives the following results, as desired:

(1) If one of the entries a_{ij} is odd, there is no pairing that can contribute to the leading term under consideration, so we have $I(a) = O(N^{-k-1})$, and we are done.

(2) If all the entries a_{ij} are even, the pairings that contribute to the leading term are those connecting points inside the pq "dropped" sets, i.e. are made out of a pairing of a_{11} points, a pairing of a_{12} points, and so on, up to a pairing of a_{pq} points. Now since an x-point set has x!! pairings, this gives the formula in the statement.

In order to further advance, let $d(\pi, \nu) = k - |\pi \vee \nu|$. It is well-known, and elementary to check, that this is a distance function on D_k . With this convention, we have:

THEOREM 14.14. The Weingarten function W_{kN} has a series expansion of the form

$$W_{kN}(\pi,\nu) = N^{-k-d(\pi,\nu)} \sum_{g=0}^{\infty} K_g(\pi,\nu) N^{-g}$$

where the objects on the right are defined as follows:

- (1) A path from π to ν is a sequence $p = [\pi = \tau_0 \neq \tau_1 \neq \ldots \neq \tau_r = \nu]$.
- (2) The signature of such a path is + when r is even, and when r is odd.
- (3) The geodesicity defect of such a path is $g(p) = \sum_{i=1}^{r} d(\tau_{i-1}, \tau_i) d(\pi, \nu)$.
- (4) K_g counts the signed paths from π to ν , with geodesicity defect g.

PROOF. Let us go back to the proof of our main estimate so far. We can write:

$$G_{kn} = N^{-k}(I+H)$$

In terms of the Brauer space distance, the formula of the matrix H is simply:

$$H(\pi,\nu) = \begin{cases} 0 & \text{for } \pi = \sigma \\ N^{-d(\pi,\nu)} & \text{for } \pi \neq \nu \end{cases}$$

Consider now the set $P_r(\pi, \nu)$ of r-paths between π and ν . According to the usual rule of matrix multiplication, the powers of H are given by:

$$H^{r}(\pi,\nu) = \sum_{p \in P_{r}(\pi,\nu)} H(\tau_{0},\tau_{1}) \dots H(\tau_{r-1},\tau_{r})$$
$$= \sum_{p \in P_{r}(\pi,\nu)} N^{-d(\pi,\nu)-g(p)}$$

We can use now $(1 + H)^{-1} = 1 - H + H^2 - H^3 + ...$, and we obtain:

$$W_{kN}(\pi,\nu) = N^{-k} \sum_{r=0}^{\infty} (-1)^r H^r(\pi,\nu)$$
$$= N^{-k-d(\pi,\nu)} \sum_{r=0}^{\infty} \sum_{p \in P_r(\pi,\nu)} (-1)^r N^{-g(p)}$$

Now by rearranging the various terms of the double sum according to the value of their geodesicity defect g = g(p), this gives the formula in the statement.

In order to discuss now the I(a) reformulation of the above result, it is convenient to use the total length of a path, defined as follows:

$$d(p) = \sum_{i=1}^{r} d(\tau_{i-1}, \tau_i)$$

Observe that we have $d(p) = d(\pi, \sigma) + g(p)$. With these conventions, we have:

THEOREM 14.15. The integral I(a) has a series expansion in N^{-1} of the form

$$I(a) = N^{-k} \sum_{d=0}^{\infty} H_d(a) N^{-d}$$

where the coefficient on the right can be interpreted as follows:

- (1) Starting from $a \in M_{p \times q}(\mathbb{N})$, construct the multi-indices a_l, a_r as usual.
- (2) Call a path "a-admissible" if its endpoints satisfy $\delta_{\pi}(a_l) = 1$ and $\delta_{\sigma}(a_r) = 1$.
- (3) Then $H_d(a)$ counts all a-admissible signed paths in D_k , of total length d.

PROOF. By combining the above results, we obtain, with our various notations:

$$I(a) = \sum_{\pi,\nu} \delta_{\pi}(a_{l}) \delta_{\nu}(a_{r}) W_{kN}(\pi,\nu)$$

= $N^{-k} \sum_{\pi,\nu} \delta_{\pi}(a_{l}) \delta_{\nu}(a_{r}) \sum_{g=0}^{\infty} K_{g}(\pi,\nu) N^{-d(\pi,\nu)-g}$

Now let $H_d(\pi, \nu)$ be the number of signed paths between π and ν , of total length d. In terms of the new variable $d = d(\pi, \nu) + g$, the above expression becomes:

$$I(a) = N^{-k} \sum_{\pi,\nu} \delta_{\pi}(a_l) \delta_{\nu}(a_r) \sum_{d=0}^{\infty} H_d(\pi,\nu) N^{-d}$$
$$= N^{-k} \sum_{d=0}^{\infty} \left(\sum_{\pi,\nu} \delta_{\pi}(a_l) \delta_{\nu}(a_r) H_d(\pi,\nu) \right) N^{-d}$$

We recognize in the middle the quantity $H_d(a)$, and this gives the result.

Let us derive now some concrete consequences from the abstract results established above. First, we have the following result, due to Collins and Śniady [16]:

THEOREM 14.16. We have the estimate

$$W_{kN}(\pi,\nu) = N^{-k-d(\pi,\nu)}(\mu(\pi,\nu) + O(N^{-1}))$$

where μ is the Möbius function.

PROOF. We know from the above that we have the following estimate:

$$W_{kN}(\pi,\nu) = N^{-k-d(\pi,\nu)}(K_0(\pi,\nu) + O(N^{-1}))$$

Now since one of the possible definitions of the Möbius function μ is that this counts the signed geodesic paths, we have $K_0 = \mu$, and we are done.

Let us go back now to our integrals I(a). We have here the following result:

THEOREM 14.17. We have the estimate

$$I(a) = N^{-k-e(a)}(\mu(a) + O(N^{-1}))$$

where the objects on the right are as follows:

- (1) $e(a) = \min\{d(\pi, \nu) | \pi, \nu \in D_k, \delta_{\pi}(a_l) = \delta_{\nu}(a_r) = 1\}.$
- (2) $\mu(a)$ counts all a-admissible signed paths in D_k , of total length e(a).

PROOF. We know that we have an estimate of the following type:

$$I(a) = N^{-k-e}(H_e(a) + O(N^{-1}))$$

Here, according to the various notations above, $e \in \mathbb{N}$ is the smallest total length of an *a*-admissible path, and $H_e(a)$ counts all signed *a*-admissible paths of total length *e*. Now since the smallest total length of such a path is attained when the path is just a segment, we have e = e(a) and $H_e(a) = \mu(a)$, and we are done.

At a more advanced level, we have the following formula, due to Collins-Matsumoto and Zinn-Justin, which uses the theory of zonal spherical functions:

THEOREM 14.18. We have the formula

$$W_{kN}(\pi,\nu) = \frac{\sum_{\lambda \vdash k, \, l(\lambda) \le k} \chi^{2\lambda}(1_k) w^{\lambda}(\pi^{-1}\nu)}{(2k)!! \prod_{(i,j) \in \lambda} (N+2j-i-1)}$$

where the various objects on the right are as follows:

- (1) The sum is over all partitions of $\{1, \ldots, 2k\}$ of length $l(\lambda) \leq k$.
- (2) w^{λ} is the corresponding zonal spherical function of (S_{2k}, H_k) . (3) $\chi^{2\lambda}$ is the character of S_{2k} associated to $2\lambda = (2\lambda_1, 2\lambda_2, \ldots)$.
- (4) The product is over all squares of the Young diagram of λ .

PROOF. This is something advanced, that we will not attempt to explain here, but that we included however for completeness. For details on all this, we refer to the abovementioned papers of Collins-Matsumoto and Zinn-Justin.

In relation with the integrals I(a), let us just record the following consequence:

PROPOSITION 14.19. The possible poles of I(a) can be at the numbers

$$-(k-1), -(k-2), \ldots, 2k-1, 2k$$

where $k \in \mathbb{N}$ associated to the admissible matrix $a \in M_{p \times q}(\mathbb{N})$ is given by $k = \sum a_{ij}/2$.

PROOF. We know from Theorem 14.10 that the possible poles of I(a) can only come from those of the Weingarten function. On the other hand, Theorem 4.18 tells us that these latter poles are located at the numbers of the form -2j + i + 1, with (i, j) ranging over all possible squares of all possible Young diagrams, and this gives the result.

We will be back to integration over O_N , with a number of more specialized results, which are complementary to the above ones, at the end of the present chapter.

14c. Truncated characters

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 14.20. 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:

$$\int_{G} (g_{11} + \ldots + g_{ss})^{k} dg = \sum_{i_{1}=1}^{s} \ldots \sum_{i_{k}=1}^{s} \int_{G} g_{i_{1}i_{1}} \ldots g_{i_{k}i_{k}} dg$$
$$= \sum_{\pi,\nu \in D(k)} W_{kN}(\pi,\nu) \sum_{i_{1}=1}^{s} \ldots \sum_{i_{k}=1}^{s} \delta_{\pi}(i) \delta_{\nu}(i)$$
$$= \sum_{\pi,\nu \in D(k)} W_{kN}(\pi,\nu) G_{ks}(\nu,\pi)$$
$$= Tr(W_{kN}G_{ks})$$

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 14.21. For an easy group $G = (G_N)$, coming from a category of partitions $D \subset P$, the following conditions are equivalent:

- (1) $G_{N-1} = G_N \cap U_{N-1}$, via the embedding $U_{N-1} \subset U_N$ given by $u \to diag(u, 1)$.
- (2) $G_{N-1} = G_N \cap U_{N-1}$, via the N possible diagonal embeddings $U_{N-1} \subset U_N$.
- (3) D is stable under the operation which consists in removing blocks.

If these conditions are satisfied, we say that $G = (G_N)$ is uniform.

PROOF. We use the general easiness theory from chapter 7, as follows:

(1) \iff (2) This is 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 v, 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:

$$\begin{aligned} \xi_{\pi} \in Fix(v^{\otimes k}) &\iff (u^{\otimes k}\xi_{\pi})_{i_{1}\dots i_{k}} = (\xi_{\pi})_{i_{1}\dots i_{k}}, \forall i \\ &\iff \sum_{j} (u^{\otimes k})_{i_{1}\dots i_{k}, j_{1}\dots j_{k}} (\xi_{\pi})_{j_{1}\dots j_{k}} = (\xi_{\pi})_{i_{1}\dots i_{k}}, \forall i \\ &\iff \sum_{j} \delta_{\pi}(j_{1},\dots,j_{k})u_{i_{1}j_{1}}\dots u_{i_{k}j_{k}} = \delta_{\pi}(i_{1},\dots,i_{k}), \forall i \end{aligned}$$

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:

$$\sum_{j'} \delta_{\pi}(j_1, \dots, j_k)(u^{\otimes k'})_{i'j'} = \delta_{\pi}(i_1, \dots, i_k), \forall i$$

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:

<u>Case 1</u>. 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:

$$\sum_{j'} \delta_{\pi}(j'_1, \dots, j'_{k'})(u^{\otimes k'})_{i'j'} = \delta_{\pi}(i'_1, \dots, i'_{k'})$$

<u>Case 2</u>. 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 $\xi_{\pi'} \in Fix(u^{\otimes k'})$, for any subpartition $\pi' \subset \pi$, as desired.

Now back to the laws of truncated characters, we have the following result:

THEOREM 14.22. 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 14.20. 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:

$$\int_{G_N} \chi_t^k \simeq \sum_{\pi \in D(k)} W_{kN}(\pi, \pi) G_{k[tN]}(\pi, \pi)$$

$$= \sum_{\pi \in D(k)} N^{-|\pi|} [tN]^{|\pi|}$$

$$\simeq \sum_{\pi \in D(k)} N^{-|\pi|} (tN)^{|\pi|}$$

$$= \sum_{\pi \in D(k)} t^{|\pi|}$$

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

We can now enlarge our collection of truncated character results, and we have:

THEOREM 14.23. 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 use the general formula for the asymptotic moments of the truncated characters found in Theorem 14.22, namely:

$$\lim_{N \to \infty} \int_{G_N} \chi_t^k = \sum_{\pi \in D(k)} t^{|\pi|}$$

By doing now some standard moment combinatorics, which was actually already done in the above, in all cases under consideration, at t = 1, and was done too in the general situation t > 0, in most of the cases under consideration, this gives the results.

As a main consequence of the above result, we have:

THEOREM 14.24. In the $N \to \infty$ limit, the laws of truncated characters for the main easy groups, real and complex, and discrete and continuous, are as follows,



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 is something that we already know from chapter 13 for usual characters, t = 1, and which follows from Theorem 14.23 in the general case, $t \in (0, 1]$.

There are many other things that can be said about the Weingarten matrices, as well as many other applications of the Weingarten formula. We will be back to this.

14d. Rotation groups

Let us go back now to the group O_N , with a number of more advanced results. The interpretation of the Weingarten matrix that we will need is in terms of the 0-1-2 matrices having sum 2 on each column, that we call "elementary", as follows:

PROPOSITION 14.25. The Weingarten matrix entries are given by

$$W_{kN}(\pi,\nu) = I(a)$$

where $a \in M_k(\mathbb{N})$ is the elementary matrix obtained as follows:

- (1) Label π_1, \ldots, π_k the strings of π .
- (2) Label ν_1, \ldots, ν_k the strings of ν .
- (3) Set $a_{ij} = \#\{r \in \{1, \dots, 2k\} | r \in \pi_i, r \in \nu_j\}.$

PROOF. Consider the multi-indices $i, j \in \{1, \ldots, k\}^{2k}$ given by $i_r \in \pi_r$ and $j_r \in \nu_r$, for any $r \in \{1, \ldots, k\}$. We have $\delta_{\pi'}(i) = \delta_{\pi\pi'}$ and $\delta_{\nu'}(j) = \delta_{\nu\nu'}$ for any pairings π', ν' , so if we apply the Weingarten formula to the quantity $v_{i_1j_1} \ldots v_{i_2k_j_{2k}}$, we obtain:

$$\int_{O_N} v_{i_1 j_1} \dots v_{i_{2k} j_{2k}} dv = \sum_{\pi' \nu'} \delta_{\pi'}(i) \delta_{\nu'}(j) W_{kN}(\pi', \nu')$$
$$= \sum_{\pi' \nu'} \delta_{\pi \pi'} \delta_{\nu \nu'} W_{kN}(\pi', \nu')$$
$$= W_{kN}(\pi, \nu)$$

The integral on the left can be written in the form I(a), for a certain matrix a. Our choice of i, j shows that a is the elementary matrix in the statement, and we are done. \Box

As an illustration for the above result, consider the partitions $\pi = \cap \cap \cap$ and $\nu = \bigcap \cap$. We have i = (112233) and j = (122133), and we obtain:

$$W_{3N}(\pi,\nu) = \int_{O_N} v_{11}v_{12}v_{22}v_{21}v_{33}v_{33} dv$$

= $\int_{O_N} v_{11}v_{12}v_{22}v_{21}v_{33}^2 dv$
= $I\begin{pmatrix} 1 & 1 & 0\\ 1 & 1 & 0\\ 0 & 0 & 2 \end{pmatrix}$

In general now, we would like to have a better understanding of the integrals I(a). It is convenient to make the following normalization:

DEFINITION 14.26. For a, b vectors with even entries we make the normalization

$$I\begin{pmatrix}a\\b\end{pmatrix} = I_{N-1}(a) I_{N-1}(b) J\begin{pmatrix}a\\b\end{pmatrix}$$

where I_{N-1} is the integration, in the sense of Definition 14.5, over the group O_{N-1} .

The new quantity J is just a normalization of the usual integral I. More precisely, by using the formula in Proposition 14.6 we have the following alternative definition:

PROPOSITION 14.27. We have the following formula:

$$J\binom{a}{b} = \frac{(\sum a_i + N - 2)!!(\sum b_i + N - 2)!!}{(N - 2)!!(N - 2)!! \prod a_i!! \prod b_i!!} I\binom{a}{b}$$

PROOF. This follows indeed from the one-row formula in Proposition 14.6.

As a first, basic example, for any one-row vector a we have $J(_0^a) = I_N(a)/I_{N-1}(a)$, and according to Proposition 14.6, this gives the following formula:

$$J\binom{a}{0} = \frac{(N-1)!!}{(N-2)!!} \cdot \frac{(\Sigma a_i + N - 2)!!}{(\Sigma a_i + N - 1)!!}$$

The advantage of using J instead of I comes from a number of invariance properties at the general level, to be established later. For the moment, let us find some rules for computing J. For $k, x \in \mathbb{N}$ we let $k^x = k \dots k$ (x times). We have:

THEOREM 14.28. We have the "elementary expansion" formula

$$J\begin{pmatrix}2a\\2b\end{pmatrix} = \sum_{r_1\dots r_q} \prod_{i=1}^q \frac{4^{r_i}a_i!b_i!}{(2r_i)!(a_i - r_i)!(b_i - r_i)!} J\begin{pmatrix}1^{2R} & 2^{A-R} & 0^{B-R}\\1^{2R} & 0^{A-R} & 2^{B-R}\end{pmatrix}$$

where the sum is over $r_i = 0, 1, ..., \min(a_i, b_i)$, and $A = \sum a_i, B = \sum b_i, R = \sum r_i$.

PROOF. Let us apply the Weingarten formula to the integral in the statement:

$$I\begin{pmatrix} 2a\\ 2b \end{pmatrix} = \int_{O_N} v_{11}^{2a_1} \dots v_{1q}^{2a_q} v_{21}^{2b_1} \dots v_{2q}^{2b_q} dv$$

$$= \sum_{\pi\nu} \delta_{\pi} (1^{2A} 2^{2B}) \delta_{\nu} (1^{2a_1} \dots q^{2a_q} 1^{2b_1} \dots q^{2b_q}) W_{kN}(\pi, \nu)$$

$$= \sum_{\nu} \delta_{\nu} (1^{2a_1} \dots q^{2a_q} 1^{2b_1} \dots q^{2b_q}) \sum_{\pi} \delta_{\pi} (1^{2A} 2^{2B}) W_{kN}(\pi, \nu)$$

Now let us look at ν . In order for δ_{ν} not to vanish, ν must connect between themselves the $2a_1 + 2b_1$ copies of 1, the $2a_2 + 2b_2$ copies of 2, and so on, up to the $2a_q + 2b_q$ copies of q. So, for any $i \in \{1, \ldots, q\}$, let us denote by $2r_i \in \{0, 2, \ldots, \min(2a_i, 2b_i)\}$ the number of "type a" copies of i coupled with "type b" copies of i. Our claim is that when these parameters r_1, \ldots, r_q are fixed, the sum on the right does not depend on σ , and provides us with a decomposition of the following type:

$$I\begin{pmatrix}2a\\2b\end{pmatrix} = \sum_{r_1\dots r_q} N_r(a,b)I_r(a,b)$$

Indeed, let us label ν_1, \ldots, ν_k the strings of ν , and consider the multi-index $j \in \{1, \ldots, k\}^{2k}$ given by $j_r \in \nu_r$, for any $r \in \{1, \ldots, k\}$. We have $\delta_{\nu'}(j) = \delta_{\nu\nu'}$ for any

pairing ν' , so by applying once again the Weingarten formula we obtain:

$$\int_{O_N} v_{1j_1} \dots v_{1j_{2A}} v_{2j_{2A+1}} \dots v_{2j_{2A+2B}} dv = \sum_{\pi\nu'} \delta_{\pi} (1^{2A} 2^{2B}) \delta_{\nu'}(j) W_{kN}(\pi, \nu')$$
$$= \sum_{\pi\nu'} \delta_{\pi} (1^{2A} 2^{2B}) \delta_{\nu\nu'} W_{kN}(\pi, \nu')$$
$$= \sum_{\pi} \delta_{\pi} (1^{2A} 2^{2B}) W_{kN}(\pi, \nu)$$

Now let us look at the integral on the left. This can be written in the form I(m), for a certain matrix m, the procedure being simply to group together, by using exponents, the identical terms in the product of u_{ij} . Now by getting back to the definition of the multi-index j, we conclude that this procedure leads to the following formula:

$$\int_{O_N} v_{1j_1} \dots v_{1j_{2A}} v_{2j_{2A+1}} \dots v_{2j_{2A+2B}} \, dv = I \begin{pmatrix} 1^{2R} & 2^{A-R} & 0^{B-R} \\ 1^{2R} & 0^{A-R} & 2^{B-R} \end{pmatrix}$$

Thus $I_r(a, b)$ is the integral in the statement. That is, we have proved the following formula, where $N_r(a, b)$ is the number of pairings ν as those considered above:

$$I\begin{pmatrix}2a\\2b\end{pmatrix} = \sum_{r_1...r_q} N_r(a,b) I\begin{pmatrix}1^{2R} & 2^{A-R} & 0^{B-R}\\1^{2R} & 0^{A-R} & 2^{B-R}\end{pmatrix}$$

Let us compute now $N_r(a, b)$. The pairings ν as above are obtained as follows: (1) pick $2r_i$ elements among $2a_i$ elements, (2) pick $2r_i$ elements among $2b_i$ elements, (3) couple the "type a" $2r_i$ elements to the "type b" $2r_i$ elements, (4) couple the remaining $2a_i - 2r_i$ elements, (5) couple the remaining $2b_i - 2r_i$ elements. Thus we have:

$$N_{r}(a,b) = \prod_{i=1}^{q} \binom{2a_{i}}{2r_{i}} \binom{2b_{i}}{2r_{i}} (2r_{i})!(2a_{i}-2r_{i})!!(2b_{i}-2r_{i})!!$$

$$= \prod_{i=1}^{q} \frac{(2a_{i})!(2b_{i})!(2r_{i})!(2a_{i}-2r_{i})!!(2b_{i}-2r_{i})!!}{(2r_{i})!(2a_{i}-2r_{i})!(2b_{i}-2r_{i})!}$$

$$= \prod_{i=1}^{q} \frac{(2a_{i})!(2b_{i})!}{(2r_{i})!(2a_{i}-2r_{i}+1)!!(2b_{i}-2r_{i}+1)!!}$$

Summing up, we have proved the following formula:

$$I\begin{pmatrix}2a\\2b\end{pmatrix} = \sum_{r_1\dots r_q} \prod_{i=1}^q \frac{(2a_i)!(2b_i)!}{(2r_i)!(2a_i - 2r_i + 1)!!(2b_i - 2r_i + 1)!!} I\begin{pmatrix}1^{2R} & 2^{A-R} & 0^{B-R}\\1^{2R} & 0^{A-R} & 2^{B-R}\end{pmatrix}$$

By applying now Proposition 14.27 twice, we obtain:

$$J\begin{pmatrix}2a\\2b\end{pmatrix} = \frac{(2A+N-2)!!(2B+N-2)!!}{(N-2)!!\prod(2a_i)!!\prod(2b_i)!!}I\begin{pmatrix}2a\\2b\end{pmatrix}$$
$$J\begin{pmatrix}1^{2R}&2^{A-R}&0^{B-R}\\1^{2R}&0^{A-R}&2^{B-R}\end{pmatrix} = \frac{(2A+N-2)!!(2B+N-2)!!}{(N-2)!!(N-2)!!}I\begin{pmatrix}1^{2R}&2^{A-R}&0^{B-R}\\1^{2R}&0^{A-R}&2^{B-R}\end{pmatrix}$$

Thus when passing to J quantities, the only thing that happens is that the numeric coefficient gets divided by $\prod (2a_i)!! \prod (2b_i)!!$. So, this coefficient becomes:

$$N'_{r}(a,b) = \prod_{i=1}^{q} \frac{1}{(2a_{i})!!(2b_{i})!!} \prod_{i=1}^{q} \frac{(2a_{i})!(2b_{i})!}{(2r_{i})!(2a_{i}-2r_{i}+1)!!(2b_{i}-2r_{i}+1)!!}$$

$$= \prod_{i=1}^{q} \frac{(2a_{i}+1)!!(2b_{i}+1)!!}{(2r_{i})!(2a_{i}-2r_{i}+1)!!(2b_{i}-2r_{i}+1)!!}$$

$$= \prod_{i=1}^{q} \frac{4^{r_{i}}a_{i}!b_{i}!}{(2r_{i})!(a_{i}-r_{i})!(b_{i}-r_{i})!}$$

Thus we have obtained the formula in the statement, and we are done.

As a first consequence, we have the following result:

THEOREM 14.29. We have the "compression formula"

$$J\begin{pmatrix}a & c\\b & 0\end{pmatrix} = J\begin{pmatrix}a & \Sigma c_i\\b & 0\end{pmatrix}$$

valid for any vectors with even entries $a, b \in \mathbb{N}^p$ and $c \in \mathbb{N}^q$.

PROOF. It is convenient to replace a, b, c with their doubles 2a, 2b, 2c. Consider now the elementary expansion formula for the matrix in the statement:

$$J\begin{pmatrix}2a & 2c\\2b & 0\end{pmatrix} = \sum_{r_1\dots r_q} \prod_{i=1}^q \frac{4^{r_i}a_i!b_i!}{(2r_i)!(a_i - r_i)!(b_i - r_i)!} J\begin{pmatrix}1^{2R} & 2^{A+C-R} & 0^{B-R}\\1^{2R} & 0^{A+C-R} & 2^{B-R}\end{pmatrix}$$

Since the numeric coefficient does not depend on c, and the function on the right depends only on $C = \Sigma c_i$, this gives the formula in the statement.

We explore now a problematics which is somehow opposite to the "compression principle": what happens when "extending" the original matrix $\binom{a}{b}$ with a $\binom{c}{0}$ component? Let us begin with a basic result, as follows:

PROPOSITION 14.30. We have the "basic extension" formula

$$J\begin{pmatrix}a&2\\b&0\end{pmatrix} = \frac{1}{N-q} \left((\Sigma a_i + N - 1)J\begin{pmatrix}a\\b\end{pmatrix} - \sum_{s=1}^q (a_s + 1)J\begin{pmatrix}a^{(s)}\\b\end{pmatrix} \right)$$

for any $a, b \in (2\mathbb{N})^q$, where $a^{(s)} = (a_1, \dots, a_{s-1}, a_s + 2, a_{s+1}, \dots, a_q)$.

PROOF. By using the trivial identity $\Sigma v_{1i}^2 = 1$, we obtain the following formula:

$$I\begin{pmatrix}a\\b\end{pmatrix} = \sum_{s=1}^{q} I\begin{pmatrix}a^{(s)}\\b\end{pmatrix} + (N-q)I\begin{pmatrix}a&2\\b&0\end{pmatrix}$$

On the other hand, according to Proposition 4.27, we have:

$$J\begin{pmatrix}a\\b\end{pmatrix} = \frac{(\sum a_i + N - 2)!!(\sum b_i + N - 2)!!}{(N - 2)!!(N - 2)!!\prod a_i!!\prod b_i!!}I\begin{pmatrix}a\\b\end{pmatrix}$$
$$J\begin{pmatrix}a^{(s)}\\b\end{pmatrix} = \frac{(\sum a_i + N)!!(\sum b_i + N - 2)!!}{(N - 2)!!(N - 2)!!\prod a_i!!\prod b_i!!(a_s + 1)}I\begin{pmatrix}a^{(s)}\\b\end{pmatrix}$$
$$J\begin{pmatrix}a&2\\b&0\end{pmatrix} = \frac{(\sum a_i + N)!!(\sum b_i + N - 2)!!}{(N - 2)!!(N - 2)!!\prod a_i!!\prod b_i!!}I\begin{pmatrix}a&2\\b&0\end{pmatrix}$$

Thus our above formula translates as follows:

$$(\Sigma a_i + N - 1)J\begin{pmatrix}a\\b\end{pmatrix} = \sum_{s=1}^q (a_s + 1)J\begin{pmatrix}a^{(s)}\\b\end{pmatrix} + (N - q)J\begin{pmatrix}a & 2\\b & 0\end{pmatrix}$$

But this gives the formula in the statement.

We have as well a recursive version of the above result, as follows:

PROPOSITION 14.31. We have the "recursive extension" formula

$$J\begin{pmatrix}a & c+2\\b & 0\end{pmatrix} = \frac{1}{N+c-q} \left((\Sigma a_i + c + N - 1)J\begin{pmatrix}a & c\\b & 0\end{pmatrix} - \sum_{s=1}^q (a_s + 1)J\begin{pmatrix}a^{(s)} & c\\b & 0\end{pmatrix} \right)$$

valid for any two vectors $a, b \in (2\mathbb{N})^q$, and any $c \in 2\mathbb{N}$.

PROOF. We use the compression formula. This gives:

$$J\begin{pmatrix}a & c+2\\b & 0\end{pmatrix} = J\begin{pmatrix}a & c&2\\b & 0&0\end{pmatrix}$$

Now if we denote the quantity on the left by K, and we apply to the quantity on the right the basic extension formula, we obtain:

$$K = \frac{1}{n-q-1} \left((\Sigma a_i + c + N - 1)J \begin{pmatrix} a & c \\ b & 0 \end{pmatrix} - \sum_{s=1}^q (a_s + 1)J \begin{pmatrix} a^{(s)} & c \\ b & 0 \end{pmatrix} - (c+1)K \right)$$

But this gives the formula of K in the statement.

As a first consequence of our results, we can establish now a number of concrete formulae. The first such formula computes all the joint moments of v_{11}, v_{12}, v_{21} :

THEOREM 14.32. We have the "triangular formula"

$$J\begin{pmatrix} a & c \\ b & 0 \end{pmatrix} = \frac{(N-1)!!}{(N-2)!!} \cdot \frac{(a+c+N-2)!!(b+c+N-2)!!}{(c+N-2)!!(a+b+c+N-1)!!}$$

valid for any $a, b, c \in 2\mathbb{N}$.

PROOF. We prove this by recurrence over $c \in 2\mathbb{N}$. At c = 0 this follows from the 1-row formula, so assume that this is true at c. By using Proposition 14.31, we get:

$$J\begin{pmatrix}a & c+2\\b & 0\end{pmatrix} = \frac{1}{N+c-1}\left((a+c+N-1)J\begin{pmatrix}a & c\\b & 0\end{pmatrix} - (a+1)J\begin{pmatrix}a+2 & c\\b & 0\end{pmatrix}\right)$$

Let us call L - R the above expression. According to the recurrence, we have:

$$L = \frac{(N-1)!!}{(N-2)!!} \cdot \frac{(a+c+N)!!(b+c+N-2)!!}{(c+N)!!(a+b+c+N-1)!!}$$
$$R = (a+1)\frac{(N-1)!!}{(N-2)!!} \cdot \frac{(a+c+N)!!(b+c+N-2)!!}{(c+N)!!(a+b+c+N+1)!!}$$

Thus we obtain the following formula:

$$J\begin{pmatrix} a & c+2\\ b & 0 \end{pmatrix}$$

$$= \frac{(N-1)!!}{(N-2)!!} \cdot \frac{(a+c+N)!!(b+c+N-2)!!}{(c+N)!!(a+b+c+N+1)!!} ((a+b+c+N) - (a+1))$$

$$= \frac{(N-1)!!}{(N-2)!!} \cdot \frac{(a+c+N)!!(b+c+N-2)!!}{(c+N)!!(a+b+c+N+1)!!} (b+c+N-1)$$

$$= \frac{(N-1)!!}{(N-2)!!} \cdot \frac{(a+c+N)!!(b+c+N)!!}{(c+N)!!(a+b+c+N+1)!!}$$

Thus the formula to be proved is true at c + 2, and we are done.

As a first observation, by combining the above formula with the compression formula we obtain the following result, fully generalizing Proposition 14.6:

PROPOSITION 14.33. We have the formula

$$J\begin{pmatrix} a & c_1 & \dots & c_q \\ b & 0 & \dots & 0 \end{pmatrix} = \frac{(N-1)!!}{(N-2)!!} \cdot \frac{(a+\Sigma c_i+N-2)!!(b+\Sigma c_i+N-2)!!}{(\Sigma c_i+N-2)!!(a+b+\Sigma c_i+N-1)!!}$$

valid for any even numbers a, b and c_1, \ldots, c_q .

PROOF. This follows indeed from Theorem 14.32 and from the compression principle. Observe that with b = 0 we recover indeed the formula in Proposition 14.6.

As a second observation, at a = 0 the triangular formula computes all the joint moments of v_{12}, v_{21} , and we obtain an interesting formula here, as follows:

14D. ROTATION GROUPS

PROPOSITION 14.34. The joint moments of 2 orthogonal group coordinates $x, y \in \{u_{ij}\}$, chosen in generic position, not on the same row or column, are given by

$$\int_{O_N} x^{\alpha} y^{\beta} \, dv = \frac{(N-2)! \alpha !! \beta !! (\alpha + \beta + N - 2) !!}{(\alpha + N - 2)!! (\beta + N - 2)!! (\alpha + \beta + N - 1)!!}$$

for α, β even, and vanish if one of α, β is odd.

PROOF. By symmetry we may assume that our coordinates are $x = v_{12}$ and $y = v_{21}$, and the result follows from Theorem 14.32, with $a = 0, c = \alpha, b = \beta$.

Moving ahead, we would like to understand what happens to $J(^a_b)$ when flipping a column of $\binom{a}{b}$. Let us begin with the case of the elementary matrices:

PROPOSITION 14.35. We have the formula

$$J\begin{pmatrix} 2^{a} & 0^{b} \\ 0^{a} & 2^{b} \end{pmatrix} = \frac{(N-1)!!}{(N-2)!!} \cdot \frac{(2a+2b+N-2)!!}{(2a+2b+N-1)!!}$$

valid for any $a, b \in \mathbb{N}$.

PROOF. Indeed, by using the compression principle, we obtain:

$$J\begin{pmatrix}2^{a} & 0^{b}\\0^{a} & 2^{b}\end{pmatrix} = J\begin{pmatrix}2a & 0\\0 & 2b\end{pmatrix} = J\begin{pmatrix}0 & 2a\\2b & 0\end{pmatrix}$$

On the other hand, by applying the triangular formula, we obtain:

$$J\begin{pmatrix} 0 & 2a\\ 2b & 0 \end{pmatrix} = \frac{(N-1)!!}{(N-2)!!} \cdot \frac{(2a+N-2)!!(2a+2b+N-2)!!}{(2a+N-2)!!(2a+2b+N-1)!!}$$

By simplifying the fraction, we obtain the formula in the statement.

We have the following generalization of the above result:

PROPOSITION 14.36. We have the "elementary flipping" formula

$$J\begin{pmatrix} 1^{2s} & 2^{a} & 0^{b} \\ 1^{2s} & 0^{a} & 2^{b} \end{pmatrix} = J\begin{pmatrix} 1^{2s} & 2^{c} & 0^{d} \\ 1^{2s} & 0^{c} & 2^{d} \end{pmatrix}$$

valid for any $s \in \mathbb{N}$ and any $a, b, c, d \in \mathbb{N}$ satisfying a + b = c + d.

PROOF. We prove this by recurrence over s. At s = 0 this follows from Proposition 14.35, because the right term there depends only on a + b. So, assume that the result is true at $s \in \mathbb{N}$. We use the following equality, coming from the triangular formula:

$$J\begin{pmatrix}2a & 2c\\2b & 0\end{pmatrix} = J\begin{pmatrix}2a & 0\\2b & 2c\end{pmatrix}$$

Assume $a \ge b$ and consider the elementary expansion of the above two quantities, where $K_r(a, b)$ denotes the coefficient appearing in the elementary expansion formula:

$$J\begin{pmatrix} 2a & 2c\\ 2b & 0 \end{pmatrix} = \sum_{r=0}^{b} K_r(a,b) J\begin{pmatrix} 1^{2r} & 2^{a+c-r} & 0^{b-r}\\ 1^{2r} & 0^{a+c-r} & 2^{b-r} \end{pmatrix}$$
$$J\begin{pmatrix} 2a & 0\\ 2b & 2c \end{pmatrix} = \sum_{r=0}^{b} K_r(a,b) J\begin{pmatrix} 1^{2r} & 2^{a-r} & 0^{b+c-r}\\ 1^{2r} & 0^{a-r} & 2^{b+c-r} \end{pmatrix}$$

We know that the sums on the right are equal, for any a, b, c with $a \ge b$. With the choice b = s, this equality becomes:

$$\sum_{r=0}^{s} K_r(a,s) J \begin{pmatrix} 1^{2r} & 2^{a+c-r} & 0^{s-r} \\ 1^{2r} & 0^{a+c-r} & 2^{s-r} \end{pmatrix} = \sum_{r=0}^{s} K_r(a,s) J \begin{pmatrix} 1^{2r} & 2^{a-r} & 0^{s+c-r} \\ 1^{2r} & 0^{a-r} & 2^{s+c-r} \end{pmatrix}$$

Now by the induction assumption, the first r terms of the above two sums coincide. So, the above equality tells us that the last terms (r = s) of the two sums are equal:

$$J\begin{pmatrix} 1^{2s} & 2^{a+c-s} \\ 1^{2s} & 0^{a+c-s} \end{pmatrix} = J\begin{pmatrix} 1^{2s} & 2^{a-s} & 0^c \\ 1^{2s} & 0^{a-s} & 2^c \end{pmatrix}$$

Since this equality holds for any $a \ge s$ and any c, this shows that the elementary flipping formula holds at s, and we are done.

We can now formulate a main result, as follows:

THEOREM 14.37. We have the "flipping formula"

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

valid for any vectors $a, b \in \mathbb{N}^p$ and $c, d \in \mathbb{N}^q$.

PROOF. Consider the elementary expansion of the two quantities in the statement, where $K_r(a, b)$ are the coefficients appearing in the elementary expansion formula:

$$J\begin{pmatrix} 2a & 2c\\ 2b & 2d \end{pmatrix} = \sum_{r_i s_j} \prod_{ij} K_{r_i}(a_i, b_i) K_{s_j}(c_j, d_j) J\begin{pmatrix} 1^{2R+2S} & 2^{A+C-R-S} & 0^{B+D-R-S}\\ 1^{2R+2S} & 0^{A+C-R-S} & 2^{B+D-R-S} \end{pmatrix}$$
$$J\begin{pmatrix} 2a & 2d\\ 2b & 2c \end{pmatrix} = \sum_{r_i s_j} \prod_{ij} K_{r_i}(a_i, b_i) K_{s_j}(d_j, c_j) J\begin{pmatrix} 1^{2R+2S} & 2^{A+D-R-S} & 0^{B+C-R-S}\\ 1^{2R+2S} & 0^{A+D-R-S} & 2^{B+C-R-S} \end{pmatrix}$$

Our claim is that two formulae are in fact identical. Indeed, the first remark is that the various indices vary in the same sets. Also, since the function $K_r(a, b)$ is symmetric in a, b, the numeric coefficients are the same. As for the J terms on the left, these are equal as well, due to elementary flipping formula, so we are done.

14D. ROTATION GROUPS

As an application of the above, we will work out now a concrete formula for the arbitrary two-row integrals. We already know that these integrals are subject to an "elementary expansion" formula, so what is left to do is to compute the values of the elementary integrals. These values are given by the following technical result:

PROPOSITION 14.38. For any a, b, r we have:

$$J\begin{pmatrix} 1^{2r} & 2^{a} & 0^{b} \\ 1^{2r} & 0^{a} & 2^{b} \end{pmatrix} = (-1)^{r} \frac{(N-1)!!}{(N-2)!!} \cdot \frac{(2r)!!(2a+2b+2r+N-2)!!}{(2a+2b+4r+N-1)!!}$$

PROOF. As a first observation, at r = 0 the result follows from Proposition 14.36. In general now, consider the elementary expansion formula, with $a, b \in \mathbb{N}$, $a \ge b$:

$$J\binom{2a}{2b} = \sum_{r=0}^{b} \frac{4^{r}a!b!}{(2r)!(a-r)!(b-r)!} J\binom{1^{2r}}{1^{2r}} \frac{2^{a-r}}{2^{a-r}} \binom{0^{b-r}}{1^{2r}}$$

By using the "flipping principle", this formula becomes:

$$J\begin{pmatrix}2a\\2b\end{pmatrix} = \sum_{r=0}^{b} \frac{4^{r}a!b!}{(2r)!(a-r)!(b-r)!} J\begin{pmatrix}1^{2r} & 2^{a+b-2r}\\1^{2r} & 0^{a+b-2r}\end{pmatrix}$$

The point is that the quantity on the left is known, and this allows the computation of the integrals on the right. More precisely, let us introduce the following function:

$$\psi_r(a) = J \begin{pmatrix} 1^{2r} & 2^a \\ 1^{2r} & 0^a \end{pmatrix}$$

Then the above equality translates into the following equation:

$$J\binom{2a}{2b} = \sum_{r=0}^{b} \frac{4^{r}a!b!}{(2r)!(a-r)!(b-r)!} \psi_{r}(a+b-2r)$$

According to Propositions 14.6 and 14.37, the values on the left are given by:

$$J\binom{2a}{2b} = \frac{(N-1)!!(2a+N-2)!!(2b+N-2)!!}{(N-2)!!(N-2)!!(2a+2b+N-1)!!}$$

Now by taking b = 0, 1, 2, ..., the above equations will successively produce the values of $\psi_r(a)$ for r = 0, 1, 2, ..., so we have here an algorithm for computing these values. On the other hand, a direct computation based on standard summation formulae shows that our system is solved by the values of $\psi_r(a)$ given in the statement, namely:

$$\psi_r(a) = (-1)^r \frac{(N-1)!!}{(N-2)!!} \cdot \frac{(2r)!!(2a+2r+N-2)!!}{(2a+4r+N-1)!!}$$

Now by using one more time the flipping principle, the knowledge of the quantities $\psi_r(a)$ fully recovers the general formula in the statement, and we are done.

We are now in position of stating and proving a main result, as follows:

THEOREM 14.39. The 2-row integrals over O_N are given by the formula

$$J\binom{2a}{2b} = \frac{(N-1)!!}{(N-2)!!} \sum_{r_1,\dots,r_q} (-1)^R \prod_{i=1}^q \frac{4^{r_i}a_i!b_i!}{(2r_i)!(a_i-r_i)!(b_i-r_i)!} \cdot \frac{(2R)!!(2S-2R+N-2)!!}{(2S+N-1)!!}$$

where the sum is over $r_i = 0, 1, ..., \min(a_i, b_i)$, and $S = \sum a_i + \sum b_i, R = \sum r_i$.

PROOF. This follows from the elementary expansion formula, by plugging in the explicit values for the elementary integrals, that we found in Proposition 14.38. \Box

For more complicated integrals, involving 3 rows or coordinates or more, the situation is quite complex, and we refer here to the literature on the subject.

14e. Exercises

Exercises:

EXERCISE 14.40. EXERCISE 14.41. EXERCISE 14.42. EXERCISE 14.43. EXERCISE 14.44. EXERCISE 14.45. EXERCISE 14.45. EXERCISE 14.46. EXERCISE 14.47. Bonus exercise.

CHAPTER 15

15a.

15b.

15c.

15d.

15e. Exercises

Exercises:

Exercise 15.1.

EXERCISE 15.2.

EXERCISE 15.3.

EXERCISE 15.4.

EXERCISE 15.5.

EXERCISE 15.6.

Exercise 15.7.

EXERCISE 15.8.

Bonus exercise.

CHAPTER 16

16a. 16b. 16c. 16d.

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. Sniady, 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).

BIBLIOGRAPHY

- [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).

BIBLIOGRAPHY

- [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(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).

BIBLIOGRAPHY

- [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.