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.

(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, March 2025
Teo Banica

Contents

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:

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

However, this is not a general rule, and rather the converse is true, in the sense that if a group is denoted as above, this means that the group must be abelian.

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. □

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

THEOREM 1.3. *We have the following groups:*

1. $(\mathbb{R}^N,+)$ *and* $(\mathbb{C}^N,+)$.
2. $(M_N(\mathbb{R}),+)$ *and* $(M_N(\mathbb{C}),+)$.
3. $(GL_N(\mathbb{R}),\cdot\,)$ *and* $(GL_N(\mathbb{C}),\cdot\,)$, *the invertible matrices.*
4. $(SL_N(\mathbb{R}),\cdot\,)$ *and* $(SL_N(\mathbb{C}),\cdot\,)$, *with S standing for "special", meaning* $\det=1$.
5. $(O_N,\cdot\,)$ *and* $(U_N,\cdot\,)$, *the orthogonal and unitary matrices.*
6. $(SO_N,\cdot\,)$ *and* $(SU_N,\cdot\,)$, *with S standing as above for* $\det=1$.

PROOF. All this is clear from definitions, and from our linear algebra knowledge:

(1) The axioms are indeed clearly satisfied for $\mathbb{R}^N,\mathbb{C}^N$, with the sum being the usual sum of vectors, $-v$ being the usual $-v$, and the null vector 0 being the unit.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

valid for any element $g \in G$.

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

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

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

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

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

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

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

1b. 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:

$$k \to w^k$$

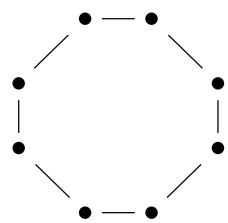
We obtain in this way all the N-roots of unity, and so our correspondence is bijective. Moreover, our correspondence transforms the sum of remainders modulo N into the multiplication of the N-th roots of unity, due to the following formula:

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

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:

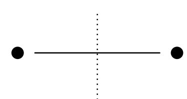
Definition 1.6. *The dihedral group D_N is the symmetry group of*



that is, of the regular polygon having N vertices.

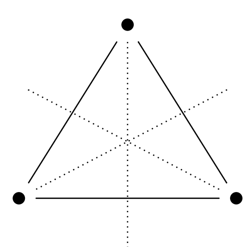
In order to understand how this works, here are the basic examples of regular N-gons, at small values of the parameter $N \in \mathbb{N}$, along with their symmetry groups:

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



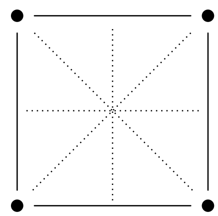
Thus we have $D_2 = \{id, \tau\}$, which in group theory terms means $D_2 = \mathbb{Z}_2$.

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



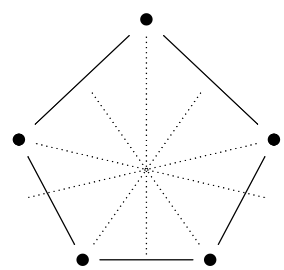
Alternatively, we can say that the symmetries are all the $3! = 6$ possible permutations of the vertices, and so that in group theory terms, we have $D_3 = S_3$.

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

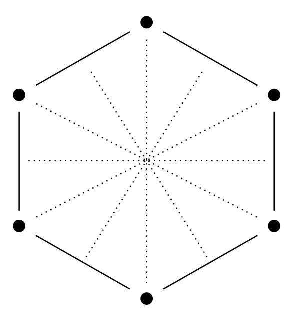


Thus, we obtain as symmetry group some sort of product between $\mathbb{Z}_4$ and $\mathbb{Z}_2$. Observe however that this product is not the usual one, our group being not abelian.

<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 $0°, \alpha°, \ldots, 6\alpha°$, 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.

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 $k = 1, \ldots, N$. But these are exactly the rotations $R_1, \ldots, R_N$ from the statement.

(2) The N symmetries with respect to the N possible symmetry axes, which are the N medians of the N-gon when N is odd, and are the $N/2$ diagonals plus the $N/2$ lines connecting the midpoints of opposite edges, when N is even. But these are exactly the symmetries $S_1, \ldots, S_N$ from the statement. □

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

THEOREM 1.8. *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:

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

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

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

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

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

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. □

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 $\rho_1, \ldots, \rho_N$ and $\sigma_1, \ldots, \sigma_N$, as follows:

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

Now when computing the products of such elements, we basically obtain the formulae in Proposition 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 $N \in \mathbb{N}$:

$\underline{N=1}$. 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:

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

$\underline{N=2}$. 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:

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

$\underline{N=3}$. 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. □

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,*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

PROPOSITION 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,*

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

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

Proof. The Cayley theorem gives an embedding as follows:

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

On the other hand, Theorem 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 $\mathbb{Z}_N$:

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

(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*

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

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

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

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

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

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

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. $\square$

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:

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

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:

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:

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

Thus χ must appear as the product of its restrictions $\chi_{|G},\chi_{|H}$, which must be both characters, and this gives the identification in the statement.

(3) This follows from (1) and (2). Alternatively, any character $\chi:G\to\mathbb{T}$ is uniquely determined by its values $\chi(g_1),\ldots,\chi(g_k)$ on the standard generators of $\mathbb{Z}_{N_1},\ldots,\mathbb{Z}_{N_k}$, which must belong to $\mathbb{Z}_{N_1},\ldots,\mathbb{Z}_{N_k}\subset\mathbb{T}$, and this gives $\widehat{G}=G$, as claimed. □

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

Proof. We have several assertions here, the idea being as follows:

(1) Given a finite abelian group G, consider indeed the group algebra $\mathbb{C}[G]$, having as elements the formal combinations of elements of G, and with involution given by:

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

This $*$-algebra is then a C^*-algebra, with norm coming by acting $\mathbb{C}[G]$ on itself, and so by the Gelfand theorem we obtain an isomorphism as follows:

$$\mathbb{C}[G]=C(X)$$

To be more precise, X is the space of the $*$-algebra characters as follows:

$$\chi:\mathbb{C}[G]\to\mathbb{C}$$

The point now is that by delinearizing, such a $*$-algebra character must come from a usual group character of G, obtained by restricting to G, as follows:

$$\chi : G \to \mathbb{T}$$

Thus we have $X = \widehat{G}$, and we are led to the isomorphism in the statement, namely:

$$\mathbb{C}[G] \simeq C(\widehat{G})$$

(2) In order to prove now the second assertion, consider the following group morphism, which is available for any finite group G, not necessarily abelian:

$$G \to \widehat{\widehat{G}} \quad , \quad g \to (\chi \to \chi(g))$$

Our claim is that in the case where G is abelian, this is an isomorphism. As a first observation, we only need to prove that this morphism is injective or surjective, because the cardinalities match, according to the following formula, coming from (1):

$$|G| = \dim \mathbb{C}[G] = \dim C(\widehat{G}) = |\widehat{G}|$$

(3) We will prove that the above morphism is injective. For this purpose, let us compute its kernel. We know that $g \in G$ is in the kernel when the following happens:

$$\chi(g) = 1 \quad , \quad \forall \chi \in \widehat{G}$$

But this means precisely that $g \in \mathbb{C}[G]$ is mapped, via the isomorphism $\mathbb{C}[G] \simeq C(\widehat{G})$ constructed in (1), to the constant function $1 \in C(\widehat{G})$, and now by getting back to $\mathbb{C}[G]$ via our isomorphism, this shows that we have indeed $g = 1$, which ends the proof. $\square$

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*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Proof. As before with Theorem 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 $<g>\subset G$ formed by the sequence of powers of g:

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

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

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

Moreover, we can choose $k\in\mathbb N$ to be minimal with this property, and with this choice, we have a set without repetitions. Thus $<g>\subset G$ is indeed a group, and more specifically a cyclic group, of order $k=ord(g)$. Finally, $ord(g)\,|\,|G|$ follows from Theorem 1.27. □

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, $G=\widehat{G}$.

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

(1) In order to prove our result, assume that G is finite and abelian. For any prime number $p \in \mathbb{N}$, let us define $G_p \subset G$ to be the subset of elements having as order a power of p. Equivalently, this subset $G_p \subset G$ can be defined as follows:

$$G_p = \left\{ g \in G \middle| \exists k \in \mathbb{N}, g^{p^k} = 1 \right\}$$

(2) It is then routine to check, based on definitions, that each G_p is a subgroup. Our claim now is that we have a direct product decomposition as follows:

$$G = \prod_p G_p$$

(3) Indeed, by using the fact that our group G is abelian, we have a morphism as follows, with the order of the factors when computing $\prod_p g_p$ being irrelevant:

$$\prod_p G_p \to G \quad , \quad (g_p) \to \prod_p g_p$$

Moreover, it is routine to check that this morphism is both injective and surjective, via some simple manipulations, so we have our group decomposition, as in (2).

(4) Thus, we are left with proving that each component G_p decomposes as a product of cyclic groups, having as orders powers of p, as follows:

$$G_p = \mathbb{Z}_{p^{r_1}} \times \ldots \times \mathbb{Z}_{p^{r_s}}$$

But this is something that can be checked by recurrence on $|G_p|$, via some routine computations, and so we are led to the conclusion in the statement.

(5) Finally, the fact that the finite abelian groups are self-dual, $G = \widehat{G}$, follows from the structure result that we just proved, and from Theorem 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:*

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

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

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

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 $S^{N-1}_\mathbb{R} \subset \mathbb{R}^N$.

(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 $S^{N-1}_\mathbb{C} \subset \mathbb{C}^N$. □

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

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:

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

(2) We have indeed the following implications:

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

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

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

Theorem 2.3. *The following are groups of matrices,*

$$SO_N = \left\{ U \in O_N \Big| \det U = 1 \right\}$$

$$SU_N = \left\{ U \in U_N \Big| \det U = 1 \right\}$$

consisting of the rotations which preserve the orientation.

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

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

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

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*

$$\begin{CD}
SU_1 @>>> U_1\\
@AAA @AAA\\
SO_1 @>>> O_1
\end{CD}$$

are the following groups of complex numbers,

$$\begin{CD}
\{1\} @>>> \mathbb{T}\\
@AAA @AAA\\
\{1\} @>>> \{\pm 1\}
\end{CD}$$

or, equivalently, are the following cyclic groups,

$$\begin{CD}
\mathbb{Z}_1 @>>> \mathbb{Z}_\infty\\
@AAA @AAA\\
\mathbb{Z}_1 @>>> \mathbb{Z}_2
\end{CD}$$

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

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

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:*

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

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

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

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

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

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

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

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,*

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

which makes SU_2 isomorphic to the unit sphere $S^1_{\mathbb{C}} \subset \mathbb{C}^2$.

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

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

Assuming that we have $\det U = 1$, the inverse must be given by:

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

On the other hand, assuming $U \in U_2$, the inverse must be the adjoint:

$$U^{-1} = \begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix}$$

We are therefore led to the following equations, for the matrix entries:

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

Thus our matrix must be of the following special form:

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

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

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

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

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

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,*

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

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:

$$\begin{aligned}|\det(U)|^2&=\det(U)\overline{\det(U)}\\&=\det(U)\det(U^*)\\&=\det(UU^*)\\&=\det(1)\\&=1\end{aligned}$$

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

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

We know from Proposition 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:

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

Thus we have $V\in SU_2$, and so we can write, with $|a|^2+|b|^2=1$:

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

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

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

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

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*

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

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:

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

Now let us write our parameters $a,b\in\mathbb{C}$, which belong to the complex unit sphere $S^1_{\mathbb{C}}\subset\mathbb{C}^2$, in terms of their real and imaginary parts, as follows:

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

In terms of $x,y,z,t\in\mathbb{R}$, our formula for a generic matrix $U\in SU_2$ becomes the one in the statement. As for the condition to be satisfied by the parameters $x,y,z,t\in\mathbb{R}$, this comes the condition $|a|^2+|b|^2=1$ to be satisfied by $a,b\in\mathbb{C}$, which reads:

$$x^2+y^2+z^2+t^2=1$$

Thus, we are led to the conclusion in the statement. Regarding now the last assertion, recall that the unit sphere $S^3_\mathbb{R}\subset\mathbb{R}^4$ is given by:

$$S^3_\mathbb{R}=\left\{(x,y,z,t)\Big|x^2+y^2+z^2+t^2=1\right\}$$

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

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

We have therefore proved our theorem. □

As a philosophical comment here, the above parametrization of SU_2 is something very nice, because the parameters (x,y,z,t) range now over the sphere of space-time. Thus, we are probably doing some kind of physics here. More on this later.

Regarding now the group U_2, we have here a similar result, as follows:

THEOREM 2.9. *We have the following formula,*

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

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:

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

Now let us write our parameters $a,b\in\mathbb{C}$, which belong to the complex unit sphere $S^1_\mathbb{C}\subset\mathbb{C}^2$, and $d\in\mathbb{T}$, in terms of their real and imaginary parts, as follows:

$$a=x+iy\quad,\quad b=z+it\quad,\quad d=p+iq$$

In terms of these new parameters $x,y,z,t,p,q\in\mathbb{R}$, our formula for a generic matrix $U\in SU_2$, that we established before, reads:

$$U=(p+iq)\begin{pmatrix}x+iy&z+it\\ -z+it&x-iy\end{pmatrix}$$

As for the condition to be satisfied by the parameters $x,y,z,t,p,q\in\mathbb{R}$, this comes the conditions $|a|^2+|b|^2=1$ and $|d|=1$ to be satisfied by $a,b,d\in\mathbb{C}$, which read:

$$x^2+y^2+z^2+t^2=1\quad,\quad p^2+q^2=1$$

Thus, we are led to the conclusion in the statement. Regarding now the last assertion, recall that the unit spheres $S^3_\mathbb{R}\subset\mathbb{R}^4$ and $S^1_\mathbb{R}\subset\mathbb{R}^2$ are given by:

$$S^3_\mathbb{R}=\left\{(x,y,z,t)\Big|x^2+y^2+z^2+t^2=1\right\}$$

$$S^1_\mathbb{R}=\left\{(p,q)\Big|p^2+q^2=1\right\}$$

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,*

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

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

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

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

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:

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

Thus, the elements $U\in SU_2$ are precisely the matrices as follows, depending on parameters $x,y,z,t\in\mathbb{R}$ satisfying $x^2+y^2+z^2+t^2=1$:

$$U=x\begin{pmatrix}1&0\\0&1\end{pmatrix}+y\begin{pmatrix}i&0\\0&-i\end{pmatrix}+z\begin{pmatrix}0&1\\-1&0\end{pmatrix}+t\begin{pmatrix}0&i\\i&0\end{pmatrix}$$

But this gives the formula for SU_2 in the statement. □

The above result is often the most convenient one, when dealing with SU_2. This is because the Pauli matrices have a number of remarkable properties, which are very useful when doing computations. These properties can be summarized as follows:

THEOREM 2.11. *The Pauli matrices multiply according to the formulae*

$$c_2^2 = c_3^2 = c_4^2 = -1$$

$$c_2c_3 = -c_3c_2 = c_4$$

$$c_3c_4 = -c_4c_3 = c_2$$

$$c_4c_2 = -c_2c_4 = c_3$$

they conjugate according to the following rules,

$$c_1^* = c_1 \ , \ c_2^* = -c_2 \ , \ c_3^* = -c_3 \ , \ c_4^* = -c_4$$

and they form an orthonormal basis of $M_2(\mathbb{C})$, with respect to the scalar product

$$< a, b >= tr(ab^*)$$

with $tr : M_2(\mathbb{C}) \to \mathbb{C}$ being the normalized trace of 2×2 matrices, $tr = Tr/2$.

PROOF. The first two assertions, regarding the multiplication and conjugation rules for the Pauli matrices, follow from some elementary computations. As for the last assertion, this follows by using these rules. Indeed, the fact that the Pauli matrices are pairwise orthogonal follows from computations of the following type, for $i \neq j$:

$$< c_i, c_j >= tr(c_ic_j^*) = tr(\pm c_ic_j) = tr(\pm c_k) = 0$$

As for the fact that the Pauli matrices have norm 1, this follows from:

$$< c_i, c_i >= tr(c_ic_i^*) = tr(\pm c_i^2) = tr(c_1) = 1$$

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.

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:

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

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

The point now, which makes the link with SO_3, and which will ultimately elucidate the structure of SO_3, is that Proposition 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 $SU_2\to SO_3$.

PROOF. We can do this in several steps, as follows:

(1) Our first claim is that the group morphism $SU_2\to GL_4(\mathbb R)$ constructed in Proposition 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:

$$\begin{aligned}<T_{U^*}(M),N> &= <U^*MU,N>\\ &= tr(U^*MUN)\\ &= tr(MUNU^*)\end{aligned}$$

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

$$\begin{aligned}<(T_U)^t(M),N> &= <M,T_U(N)>\\ &= <M,UNU^*>\\ &= tr(MUNU^*)\end{aligned}$$

Thus we have indeed $T_U^*=(T_U)^t$, which proves our $SU_2\to O_4$ claim.

(2) In order now to finish, recall that we have by definition $c_1=1$, as a matrix. Thus, the action of SU_2 on the vector $c_1\in E$ is given by:

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

We conclude that $c_1 \in E$ is invariant under SU_2, and by orthogonality the following subspace of E must be invariant as well under the action of SU_2:

$$e_1^\perp = span_\mathbb{R}(c_2, c_3, c_4)$$

Now if we call this subspace F, and we identify $F \simeq \mathbb{R}^3$ by using the basis c_2, c_3, c_4, we obtain by restriction to F a morphism of groups as follows:

$$SU_2 \to O_3$$

But since this morphism is continuous and SU_2 is connected, its image must be connected too. Now since the target group decomposes as $O_3 = SO_3 \sqcup (-SO_3)$, and $1 \in SU_2$ gets mapped to $1 \in SO_3$, the whole image must lie inside SO_3, and we are done. $\square$

The above result is quite interesting, because we will see in a moment that the morphism $SU_2 \to SO_3$ 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 $SU_2 \to O_4$, what we have in fact is a group morphism $SU_2 \to O_3$, and even $SU_2 \to SO_3$.

Proof. With notations from Proposition 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:

$$U = xc_1 + yc_2 + zc_3 + tc_4$$

$$M = ac_1 + bc_2 + cc_3 + dc_4$$

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

$$\begin{aligned}
UM &= (xc_1+yc_2+zc_3+tc_4)(ac_1+bc_2+cc_3+dc_4)\\
&= (xa-yb-zc-td)c_1\\
&+ (xb+ya+zd-tc)c_2\\
&+ (xc-yd+za+tb)c_3\\
&+ (xd+yc-zb+ta)c_4
\end{aligned}$$

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

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

Similarly, let us look now at the action $R:SU_2\curvearrowright\mathbb{R}^4$ by right multiplication, which is by definition given by the following formula:

$$R_U(M)=MU^*$$

In order to compute the matrix of this action, let us write, as before:

$$U=xc_1+yc_2+zc_3+tc_4$$

$$M=ac_1+bc_2+cc_3+dc_4$$

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

$$\begin{aligned}
MU^* &= (ac_1+bc_2+cc_3+dc_4)(xc_1-yc_2-zc_3-tc_4)\\
&= (ax+by+cz+dt)c_1\\
&+ (-ay+bx-ct+dz)c_2\\
&+ (-az+bt+cx-dy)c_3\\
&+ (-at-bz+cy+dx)c_4
\end{aligned}$$

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

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

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

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

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. □

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

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

$$SU_2 \to SO_3$$

and this map produces the Euler-Rodrigues formula

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

for the generic elements of SO_3.

PROOF. We know from the above that we have a group morphism $SU_2 \to SO_3$, given by the formula in the statement, and the problem now is that of proving that this is a double cover map, in the sense that it is surjective, and with kernel $\{\pm 1\}$.

(1) Regarding the kernel, this is elementary to compute, as follows:

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

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

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

Here P stands for "projective", and it is possible to say more about the construction $G \to PG$, which can be performed for any subgroup $G \subset U_N$. But we will not get here into this, our next goal being anyway that of proving that we have $PU_2 = SO_3$.

(3) We must prove now that the morphism $SU_2 \to SO_3$ is surjective. This is something non-trivial, and there are several advanced proofs for this, as follows:

– A first proof is by using Lie theory. To be more precise, the tangent spaces at 1 of both SU_2 and SO_3 can be explicitely computed, by doing some linear algebra, and the morphism $SU_2 \to SO_3$ follows to be surjective around 1, and then globally.

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

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

In the case $b=0$ the only equation which is left is $q=0$, and reminding that we must have $p\in i\mathbb{R}$, we do have solutions, namely two of them, as follows:

$$V=\pm\begin{pmatrix}i&0\\0&i\end{pmatrix}$$

(8) In the remaining case $b\neq 0$, the first equation reads $b\bar{q}\in\mathbb{R}$, so we must have $q=\lambda b$ with $\lambda\in\mathbb{R}$. Now with this substitution made, the second equation reads $p-\bar{p}=\lambda(a-\bar{a})$, and since we must have $p\in i\mathbb{R}$, this gives $2p=\lambda(a-\bar{a})$. Thus, our equations are:

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

Getting back now to our problem about finding fixed points, assuming $|a|^2+|b|^2=1$ we must find $\lambda\in\mathbb{R}$ such that the above numbers p,q satisfy $|p|^2+|q|^2=1$. But:

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

Thus, we have again two solutions to our fixed point problem, given by:

$$\lambda=\pm\frac{1}{\sqrt{1-Re(a)^2}}$$

(9) Summarizing, we have proved that any rotation $U\in Im(SU_2\to SO_3)$ has an axis, and with the direction of this axis, corresponding to a pair of opposite points on the sphere $S^2_\mathbb{R}\subset\mathbb{R}^3$, being given by the above formulae, via $S^2_\mathbb{R}\subset S^3_\mathbb{R}=SU_2$.

(10) In order to finish, we must argue that any rotation $U\in SO_3$ has an axis. But this follows for instance from some topology, by using the induced map $S^2_\mathbb{R}\to S^2_\mathbb{R}$. Now since $U\in SO_3$ is uniquely determined by its rotation axis, which can be regarded as a point of $S^2_\mathbb{R}/\{\pm1\}$, 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 $SU_2/\{\pm1\}$, 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:

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 $\det U=\pm1$, and in the case $\det U=-1$, we have:

$$\det(-U)=(-1)^3\det U=-\det U=1$$

Thus, assuming $\det U=-1$, we can therefore rescale U into an element $-U\in SO_3$, and this leads to the conclusion in the statement. □

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. □

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:

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. □

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 $N \in \mathbb{N}$:

$\underline{N=1}$. 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:

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

$\underline{N=2}$. 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:

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

$\underline{N=3}$. 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 $\mathbb{R}^N$.

(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*

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

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

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

with the convention $\mathbb Z_\infty=\mathbb T$, at $s=\infty$.

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

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

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:*

$$|H_N^s|=s^NN!$$

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:

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

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. $\square$

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:

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

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. $\square$

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 $d = 1$. □

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*

$$H_N^{sd} = \left\{ U \in H_N^s \Big| (\det U)^d = 1 \right\}$$

along with 34 exceptional examples.

Proof. This is something quite advanced, and we refer here to the paper of Shephard and Todd [87], and to the subsequent literature on the subject. □

3e. Exercises

Exercises:

EXERCISE 3.12.

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:*

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

If this happens only for the rows, or only for the columns, the matrix is called row-stochastic, 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 $M\mathbb{I}_N = \mathbb{I}_N M = \lambda\mathbb{I}_N$.*

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:

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

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

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

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

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

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

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

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

The unitary bistochastic matrices are stable under a number of operations, and in particular under taking products, and we have the following result:

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

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

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

Proof. Let us pick a 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:

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

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

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

$$P^{N-1}_{\mathbb{C}} = (\mathbb{C}^N - \{0\})\big/ < x = \lambda y >$$

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

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

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 $\mathbb{T}^{N-1} \subset P^{N-1}_{\mathbb{C}}$ satisfies $\mathbb{T}^{N-1} \cap U\mathbb{T}^{N-1} \neq \emptyset$.*

PROOF. These equivalences are all elementary, as follows:

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

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

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:

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

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

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

(2) $\implies$ (3) This is clear, because $\mathbb{T}^{N-1} \subset P^{N-1}_{\mathbb{C}}$ 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 $\mathbb{T}^{N-1} \subset P^{N-1}_{\mathbb{C}}$ 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

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" $\bar{\mathbb{C}}^N$ is the usual space $\mathbb{C}^N$, with its standard basis $\{e_1,\ldots,e_N\}$, with a chosen sign $\varepsilon=\pm1$, and a chosen involution on the indices:*

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

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

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

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

Thus, up to a base change, the super-identity is as follows, where $N=2p+q$ and $\varepsilon=\pm1$, with the 1_q block at right disappearing if $\varepsilon=-1$:

$$J=\begin{pmatrix}0&1\\ \varepsilon1&0_{(0)}\\ &&\ddots\\ &&&0&1\\ &&&\varepsilon1&0_{(p)}\\ &&&&&1_{(1)}\\ &&&&&&\ddots\\ &&&&&&&1_{(q)}\end{pmatrix}$$

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

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

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

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

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

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

PROOF. These results are both elementary, as follows:

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

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

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

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

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

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

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

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

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

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

Regarding now Sp_N, we have the following result:

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

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

consists of the SU_2 patterned matrices,

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

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

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

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

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. □

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:

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*

$$H_N^{sd} = \left\{ U \in H_N^s \Big| (\det U)^d = 1 \right\}$$

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. □

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:

$$\begin{array}{ccc} K_N & \longrightarrow & U_N \\ \uparrow & & \uparrow \\ H_N & \longrightarrow & O_N \end{array}$$

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*

$$G_N^d = G_N \cap K_N \quad , \quad G_N^r = G_N \cap O_N$$

$$G_N^u =< G_N, K_N > \quad , \quad G_N^s =< G_N, O_N >$$

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*

$$\begin{array}{ccccc}
K_N & \rightarrow & G_N^u & \rightarrow & U_N \\
\uparrow & & \uparrow & & \uparrow \\
G_N^d & \rightarrow & G_N & \rightarrow & G_N^s \\
\uparrow & & \uparrow & & \uparrow \\
H_N & \rightarrow & G_N^r & \rightarrow & O_N
\end{array}$$

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:

$$G_N =< G_N^d, G_N^r > \quad , \quad G_N = G_N^u \cap G_N^s$$

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.

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:

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:

$$\begin{aligned}
[(g\otimes h)(g\otimes h)^*]_{ia,jb} &= \sum_{kc}(g\otimes h)_{ia,kc}((g\otimes h)^*)_{kc,jb}\\
&= \sum_{kc}(g\otimes h)_{ia,kc}\overline{(g\otimes h)_{jb,kc}}\\
&= \sum_{kc}g_{ik}h_{ac}\bar{g}_{jk}\bar{h}_{bc}\\
&= \sum_k g_{ik}\bar{g}_{jk}\sum_c h_{ac}\bar{h}_{bc}\\
&= \delta_{ij}\delta_{ab}
\end{aligned}$$

(3) This simply follows from the fact that if $g\in U_N$ is unitary, then so is its complex conjugate, $\bar{g}\in U_N$, and this due to the following formula, obtained by conjugating:

$$g^*=g^{-1}\implies g^t=\bar{g}^{-1}$$

(4) This is clear as well, because if $g\in U_N$ is unitary, and $V\in U_N$ is another unitary, then we can spin g by this unitary, and we obtain a unitary as follows:

$$VgV^*\in U_N$$

Thus, our operations are well-defined, and this leads to the above conclusions. □

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

PROPOSITION 5.3. *We have the following formulae, regarding characters*

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

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:

$$Tr(diag(g,h))=Tr(g)+Tr(h) \quad , \quad Tr(g\otimes h)=Tr(g)Tr(h)$$

$$Tr(\bar{g})=\overline{Tr(g)} \quad , \quad Tr(VgV^*)=Tr(g)$$

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

$$\begin{aligned}Tr(g\otimes h)&=\sum_{ia}(g\otimes h)_{ia,ia}\\&=\sum_{ia}g_{ii}h_{aa}\\&=Tr(g)Tr(h)\end{aligned}$$

Regarding now the third formula, this is clear from definitions, by conjugating. Finally, regarding the fourth formula, this can be established as follows:

$$Tr(VgV^*)=Tr(gV^*V)=Tr(g)$$

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

Assume now that we are given a 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:*

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

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

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

and with the convention that $u^{\otimes\emptyset}$ is the trivial representation $1:G\to U_1$.

Here are a few examples of such Peter-Weyl representations, namely those coming from the colored integers of length 2, to be often used in what follows:

$$u^{\otimes\circ\circ}=u\otimes u \quad , \quad u^{\otimes\circ\bullet}=u\otimes\bar{u}$$

$$u^{\otimes\bullet\circ}=\bar{u}\otimes u \quad , \quad u^{\otimes\bullet\bullet}=\bar{u}\otimes\bar{u}$$

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

Proposition 5.5. *The characters of Peter-Weyl representations are given by*

$$\chi_{u^{\otimes k}} = (\chi_u)^k$$

with the colored powers of a variable χ being by definition given by

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

and with the convention that $\chi^\emptyset$ equals by definition 1.

Proof. This follows indeed from the additivity, multiplicativity and conjugation formulae established in Proposition 5.3, via the conventions in Definition 5.4. □

Given a closed subgroup $G \subset U_N$, we would like to understand its Peter-Weyl representations, and compute the expectations of the characters of these representations. In order to do so, let us formulate the following key definition:

Definition 5.6. *Given a 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

$$Hom(u,v) = \left\{ T \in M_{M \times N}(\mathbb{C}) \Big| T u_g = v_g T, \forall g \in G \right\}$$

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:

$$\begin{aligned}(S\otimes T)(u_g\otimes w_g)&=Su_g\otimes Tw_g\\&=v_gS\otimes t_gT\\&=(v_g\otimes t_g)(S\otimes T)\end{aligned}$$

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

$$\begin{aligned}Tu_g=v_gT&\implies u_g^*T^*=T^*v_g^*\\&\implies T^*v_g=u_gT^*\end{aligned}$$

(4) This is just 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. □

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

Step 2. We prove now that the above algebras $A_i \subset A$ are in a direct sum position, in the sense that we have a non-unital $*$-algebra sum decomposition, as follows:
$$A = A_1 \oplus \ldots \oplus A_k$$

As with any direct sum question, we have two things to be proved here. First, by using the formula $p_1+\ldots+p_k=1$ and the projection equations $p_i^2=p_i^*=p_i$, we conclude that we have the needed generation property, namely:

$$A_1+\ldots+A_k=A$$

As for the fact that the sum is indeed direct, this follows as well from the formula $p_1+\ldots+p_k=1$, and from the projection equations $p_i^2=p_i^*=p_i$.

Step 3. Our claim now, which will finish the proof, is that each of the $*$-subalgebras $A_i=p_iAp_i$ 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. $\square$

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:

$$pu_g p = u_g p \quad , \quad \forall g \in G$$

Thus, we are in need of a technical linear algebra result, stating that for a projection $P \in M_N(\mathbb{C})$ and a unitary $U \in U_N$, the following happens:

$$PUP = UP \implies PU = UP$$

(5) But this can be established with some C^*-algebra know-how, as follows:

$$\begin{aligned}
tr[(PU - UP)(PU - UP)^*] &= tr[(PU - UP)(U^*P - PU^*)] \\
&= tr[P - PUPU^* - UPU^*P + UPU^*] \\
&= tr[P - UPU^* - UPU^* + UPU^*] \\
&= tr[P - UPU^*] \\
&= 0
\end{aligned}$$

Indeed, by positivity this gives $PU - UP = 0$, as desired.

(6) With these preliminaries in hand, let us decompose the algebra $End(u)$ as in Theorem 5.9, by using the decomposition $1 = p_1 + \ldots + p_k$ into minimal projections. If we denote by $u_i \subset u$ the subrepresentation coming from the vector space $V_i = Im(p_i)$, then we obtain in this way a decomposition $u = u_1 + \ldots + u_k$, as in the statement. □

In order to formulate our second Peter-Weyl theorem, 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:*

$$C_v = \left\{ f \circ v \Big| f \in M_M(\mathbb{C})^* \right\}$$

In other words, by delinearizing, $C_\nu \subset C(G)$ is the following linear space:

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

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:

$$C_v \subset < g_{ij} >$$

(3) By definition of the Peter-Weyl representations, as arbitrary tensor products between the fundamental representation u and its conjugate $\bar{u}$, we have:

$$< g_{ij} >= \sum_k C_{u^{\otimes k}}$$

(4) Now by putting together the observations (2,3) we conclude that we must have an inclusion as follows, for certain exponents $k_1, \ldots, k_p$:

$$C_v \subset C_{u^{\otimes k_1} \oplus \ldots \oplus \pi^{\otimes k_p}}$$

By using now the functoriality result from (1), we deduce from this that we have an inclusion of representations, as follows:

$$v \subset u^{\otimes k_1} \oplus \ldots \oplus u^{\otimes k_p}$$

Together with Theorem 5.10, this leads to the conclusion in the statement. □

As a conclusion to what we have so far, the problem to be solved is that of splitting the Peter-Weyl representations into sums of irreducible representations.

5c. 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 $\Gamma = \widehat{G}$, 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,

$$\int_G g = \delta_{g1}$$

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

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. □

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:

$$((id \otimes \varphi^{*k})v)_{i_0 i_{k+1}} = \sum_{i_1 \ldots i_k} M_{i_0 i_1} \ldots M_{i_k i_{k+1}} = (M^k)_{i_0 i_{k+1}}$$

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

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

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

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

Now since v is unitary we have $||v|| = 1$, and so $||M|| \leq 1$. Thus the last Cesàro limit converges, and equals the orthogonal projection onto the 1-eigenspace of M:

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^n M^k = P$$

Thus our initial Cesàro limit converges as well, to $\tau(P)$, as desired. □

The point now is that when the linear form $\varphi \in C(G)^*$ from the above result is chosen to be faithful, we obtain the following finer result:

Proposition 5.16. *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 $Fix(v) = \left\{\xi \in \mathbb{C}^n \middle| v\xi = \xi\right\}$.

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 $Fix(v)$.

"⊃" This is clear, and for any φ, because we have the following implication:

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

"⊂" Here we must prove that, when φ is faithful, we have:

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

For this purpose, assume that we have $M\xi = \xi$, and consider the following function:

$$f = \sum_i \left(\sum_j v_{ij}\xi_j - \xi_i \right) \left(\sum_k v_{ik}\xi_k - \xi_i \right)^*$$

We must prove that we have $f = 0$. Since v is unitary, we have:

$$\begin{aligned} f &= \sum_{ijk} v_{ij}v_{ik}^*\xi_j\bar{\xi}_k - \frac{1}{N}v_{ij}\xi_j\bar{\xi}_i - \frac{1}{N}v_{ik}^*\xi_i\bar{\xi}_k + \frac{1}{N^2}\xi_i\bar{\xi}_i \\ &= \sum_j |\xi_j|^2 - \sum_{ij} v_{ij}\xi_j\bar{\xi}_i - \sum_{ik} v_{ik}^*\xi_i\bar{\xi}_k + \sum_i |\xi_i|^2 \\ &= ||\xi||^2 - < v\xi, \xi > - \overline{< v\xi, \xi >} + ||\xi||^2 \\ &= 2(||\xi||^2 - Re(< v\xi, \xi >)) \end{aligned}$$

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

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

Now since φ is faithful, this gives $f = 0$, and so $v\xi = \xi$, as claimed. □

We can now formulate a main result, as follows:

THEOREM 5.17. *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 $Fix(v) = \left\{ \xi \in \mathbb{C}^n \middle| v\xi = \xi \right\}$.

PROOF. We can prove this from what we have, in several steps, as follows:

(1) Let us first go back to the general context of Proposition 5.15. 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:

$$\int_\varphi*\varphi=\varphi*\int_\varphi=\int_\varphi$$

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 $\int_G=\int_\varphi$:

$$\left(\int_G\otimes id\right)\Delta=\left(id\otimes\int_G\right)\Delta=\int_G(.)1$$

But this is exactly the left and right invariance formula we were looking for.

(5) Finally, in order to prove the uniqueness assertion, assuming that we have two invariant integrals $\int_G,\int_G'$, we have, according to the above invariance formula:

$$\left(\int_G\otimes\int_G'\right)\Delta=\left(\int_G'\otimes\int_G\right)\Delta=\int_G(.)1=\int_G'(.)1$$

Thus we have $\int_G=\int_G'$, and this finishes the proof. □

Summarizing, we can now integrate over G. As a first application, we have:

THEOREM 5.18. *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:

$$\begin{aligned}\int_G\chi_v&=Tr(P)\\&=\dim(Im(P))\\&=dim(Fix(v))\end{aligned}$$

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

$$\begin{aligned}\int_G \chi^k &= \int_G \chi_u^k \\ &= \int_G \chi_{u^{\otimes k}} \\ &= \dim(Fix(u^{\otimes k}))\end{aligned}$$

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

As a key remark now, the integration formula in Theorem 5.17 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*

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

depending on a colored integer $k = e_1 \ldots e_k$, are called polynomial integrals over G.

As a first observation, the knowledge of these integrals is the same as the knowledge of the integration functional over G. Indeed, since the coordinate functions $g \to g_{ij}$ separate the points of G, we can apply the Stone-Weierstrass theorem, and we obtain:

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

Thus, by linearity, the computation of any functional $f : C(G) \to \mathbb{C}$, and in particular of the integration functional, reduces to the computation of this functional on the polynomials of the coordinate functions $g \to g_{ij}$ and their conjugates $g \to \bar{g}_{ij}$.

By using now Peter-Weyl theory, everything reduces to algebra, as follows:

Theorem 5.20. *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*

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

valid for any colored integer $k = e_1 \ldots e_k$ and any multi-indices i, j, where D_k is a linear basis of $Fix(u^{\otimes k})$, the associated generalized Kronecker symbols are given by

$$\delta_\pi(i) = < \pi, e_{i_1} \otimes \ldots \otimes e_{i_k} >$$

and $W_k = G_k^{-1}$ is the inverse of the Gram matrix, $G_k(\pi, \sigma) = < \pi, \sigma >$.

PROOF. We know from Peter-Weyl theory that the integrals in the statement form altogether the orthogonal projection P^k onto the following space:

$$Fix(u^{\otimes k}) = span(D_k)$$

Consider now the following linear map, with $D_k = \{\xi_k\}$ being as in the statement:

$$E(x) = \sum_{\pi \in D_k} < x, \xi_\pi > \xi_\pi$$

By a standard linear algebra computation, it follows that we have $P = WE$, where W is the inverse of the restriction of E to the following space:

$$K = span\left(T_\pi \Big| \pi \in D_k\right)$$

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:

$$\begin{aligned} T \in Hom(v, w) &\iff Tv = wT \\ &\iff \sum_j T_{aj} v_{ji} = \sum_b w_{ab} T_{bi}, \forall a, i \end{aligned}$$

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

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

With these formulae in hand, both inclusions follow from the unitarity of v, w. □

We can now formulate our third Peter-Weyl theorem, as follows:

THEOREM 5.22 (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

$$<a,b>=\int_G ab^*$$

where $\int_G$ is the Haar integration over G.

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

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

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*

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

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:

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

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:

$$\begin{aligned}\int_G\chi_v\chi_v^* &= \sum_{ij}\int_G v_{ii}v_{jj}^*\\ &= \sum_i\frac{1}{N}\\ &= 1\end{aligned}$$

Here we have used the fact, coming from Theorem 5.22, that the integrals $\int_G v_{ij}v_{kl}^*$ form the orthogonal projection onto the following vector space:

$$Fix(v\otimes\bar v)\simeq End(v)=\mathbb C1$$

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 $\chi_u\in\widehat{G}$. □

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

6a.

6b.

6c.

6d.

6e. Exercises

Exercises:

Exercise 6.1.

Exercise 6.2.

Exercise 6.3.

Exercise 6.4.

Exercise 6.5.

Exercise 6.6.

Exercise 6.7.

Exercise 6.8.

Bonus exercise.

CHAPTER 7

7a.

7b.

7c.

7d.

7e. Exercises

Exercises:

EXERCISE 7.1.

EXERCISE 7.2.

EXERCISE 7.3.

EXERCISE 7.4.

EXERCISE 7.5.

EXERCISE 7.6.

EXERCISE 7.7.

EXERCISE 7.8.

Bonus exercise.

CHAPTER 8

8a.

8b.

8c.

8d.

8e. Exercises

Exercises:

Exercise 8.1.

Exercise 8.2.

Exercise 8.3.

Exercise 8.4.

Exercise 8.5.

Exercise 8.6.

Exercise 8.7.

Exercise 8.8.

Bonus exercise.

Part III

Lie algebras

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

CHAPTER 9

9a.

9b.

9c.

9d.

9e. Exercises

Exercises:

Exercise 9.1.

Exercise 9.2.

Exercise 9.3.

Exercise 9.4.

Exercise 9.5.

Exercise 9.6.

Exercise 9.7.

Exercise 9.8.

Bonus exercise.

CHAPTER 10

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.

Bonus exercise.

CHAPTER 11

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.

Bonus exercise.

CHAPTER 12

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.

Bonus exercise.

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

CHAPTER 13

13a.

13b.

13c.

13d.

13e. Exercises

Exercises:

Exercise 13.1.

Exercise 13.2.

Exercise 13.3.

Exercise 13.4.

Exercise 13.5.

Exercise 13.6.

Exercise 13.7.

Exercise 13.8.

Bonus exercise.

CHAPTER 14

14a.

14b.

14c.

14d.

14e. Exercises

Exercises:

EXERCISE 14.1.

EXERCISE 14.2.

EXERCISE 14.3.

EXERCISE 14.4.

EXERCISE 14.5.

EXERCISE 14.6.

EXERCISE 14.7.

EXERCISE 14.8.

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. Śniady, Integration with respect to the Haar measure on unitary, orthogonal and symplectic groups, *Comm. Math. Phys.* **264** (2006), 773–795.

[17] A. Connes, Noncommutative geometry, Academic Press (1994).

[18] P. Deligne, Catégories tannakiennes, in "Grothendieck Festchrift", Birkhauser (1990), 111–195.

[19] P. Di Francesco, Meander determinants, *Comm. Math. Phys.* **191** (1998), 543–583.

[20] P. Diaconis and M. Shahshahani, On the eigenvalues of random matrices, *J. Applied Probab.* **31** (1994), 49–62.

[21] P.A.M. Dirac, Principles of quantum mechanics, Oxford Univ. Press (1930).

[22] M.P. do Carmo, Differential geometry of curves and surfaces, Dover (1976).

[23] S. Doplicher and J. Roberts, A new duality theory for compact groups, *Invent. Math.* **98** (1989), 157–218.

[24] V.G. Drinfeld, Quantum groups, Proc. ICM Berkeley (1986), 798–820.

[25] R. Durrett, Probability: theory and examples, Cambridge Univ. Press (1990).

[26] A. Einstein, Relativity: the special and the general theory, Dover (1916).

[27] M. Enock and J.M. Schwartz, Kac algebras and duality of locally compact groups, Springer (1992).

[28] P. Etingof, S. Gelaki, D. Nikshych and V. Ostrik, Tensor categories, AMS (2016).

[29] L.C. Evans, Partial differential equations, AMS (1998).

[30] L. Faddeev, N. Reshetikhin and L. Takhtadzhyan, Quantization of Lie groups and Lie algebras, *Leningrad Math. J.* **1** (1990), 193–225.

[31] W. Feller, An introduction to probability theory and its applications, Wiley (1950).

[32] E. Fermi, Thermodynamics, Dover (1937).

[33] R.P. Feynman, R.B. Leighton and M. Sands, The Feynman lectures on physics, Caltech (1963).

[34] P. Flajolet and R. Sedgewick, Analytic combinatorics, Cambridge Univ. Press (2009).

[35] W. Fulton, Algebraic topology, Springer (1995).

[36] W. Fulton and J. Harris, Representation theory, Springer (1991).

[37] C. Godsil and G. Royle, Algebraic graph theory, Springer (2001).

[38] H. Goldstein, C. Safko and J. Poole, Classical mechanics, Addison-Wesley (1980).

[39] J.M. Gracia-Bondía, J.C. Várilly and H. Figueroa, Elements of noncommutative geometry, Birkhäuser (2001).

[40] D.J. Griffiths, Introduction to electrodynamics, Cambridge Univ. Press (2017).

[41] D.J. Griffiths and D.F. Schroeter, Introduction to quantum mechanics, Cambridge Univ. Press (2018).

[42] D.J. Griffiths, Introduction to elementary particles, Wiley (2020).

[43] P. Griffiths and J. Harris, Principles of algebraic geometry, Wiley (1994).

[44] L.C. Grove, Classical groups and geometric algebra, AMS (2002).

[45] G.H. Hardy and E.M. Wright, An introduction to the theory of numbers, Oxford Univ. Press (1938).

[46] J. Harris, Algebraic geometry, Springer (1992).

[47] R. Hartshorne, Algebraic geometry, Springer (1977).

[48] A. Hatcher, Algebraic topology, Cambridge Univ. Press (2002).

[49] R.A. Horn and C.R. Johnson, Matrix analysis, Cambridge Univ. Press (1985).

[50] K. Huang, Introduction to statistical physics, CRC Press (2001).

[51] J.E. Humphreys, Introduction to Lie algebras and representation theory, Springer (1972).

[52] J.E. Humphreys, Linear algebraic groups, Springer (1975).

[53] M. Idel and M.M. Wolf, Sinkhorn normal form for unitary matrices, *Linear Algebra Appl.* **471** (2015), 76–84.

[54] K. Ireland and M. Rosen, A classical introduction to modern number theory, Springer (1982).

[55] N. Jacobson, Basic algebra, Dover (1974).

[56] M. Jimbo, A q-difference analog of $U(\mathfrak{g})$ and the Yang-Baxter equation, *Lett. Math. Phys.* **10** (1985), 63–69.

[57] V.F.R. Jones, Index for subfactors, *Invent. Math.* **72** (1983), 1–25.

[58] V.F.R. Jones, On knot invariants related to some statistical mechanical models, *Pacific J. Math.* **137** (1989), 311–334.

[59] V.F.R. Jones, Subfactors and knots, AMS (1991).

[60] V.F.R. Jones, Planar algebras I (1999).

[61] C. Kassel, Quantum groups, Springer (1995).

[62] T. Kibble and F.H. Berkshire, Classical mechanics, Imperial College Press (1966).

[63] M. Kumar, Quantum: Einstein, Bohr, and the great debate about the nature of reality, Norton (2009).

[64] G. Landi, An introduction to noncommutative spaces and their geometry, Springer (1997).

[65] S. Lang, Algebra, Addison-Wesley (1993).

[66] S. Lang, Abelian varieties, Dover (1959).

[67] P. Lax, Linear algebra and its applications, Wiley (2007).

[68] P. Lax, Functional analysis, Wiley (2002).

[69] B. Lindstöm, Determinants on semilattices, *Proc. Amer. Math. Soc.* **20** (1969), 207–208.

[70] F. Lusztig, Introduction to quantum groups, Birkhäuser (1993).

[71] S. Majid, Foundations of quantum group theory, Cambridge Univ. Press (1995).

[72] S. Malacarne, Woronowicz's Tannaka-Krein duality and free orthogonal quantum groups, *Math. Scand.* **122** (2018), 151–160.

[73] Y.I. Manin, Quantum groups and noncommutative geometry, Springer (2018).

[74] V.A. Marchenko and L.A. Pastur, Distribution of eigenvalues in certain sets of random matrices, *Mat. Sb.* **72** (1967), 507–536.

[75] M.L. Mehta, Random matrices, Elsevier (2004).

[76] S. Montgomery, Hopf algebras and their actions on rings, AMS (1993).

[77] M.A. Nielsen and I.L. Chuang, Quantum computation and quantum information, Cambridge Univ. Press (2000).

[78] P. Petersen, Linear algebra, Springer (2012).

[79] D.E. Radford, Hopf algebras, World Scientific (2011).

[80] W. Rudin, Principles of mathematical analysis, McGraw-Hill (1964).

[81] W. Rudin, Real and complex analysis, McGraw-Hill (1966).

[82] W. Rudin, Fourier analysis on groups, Dover (1972).

[83] D.V. Schroeder, An introduction to thermal physics, Oxford Univ. Press (1999).

[84] J.P. Serre, A course in arithmetic, Springer (1973).

[85] J.P. Serre, Linear representations of finite groups, Springer (1977).

[86] I.R. Shafarevich, Basic algebraic geometry, Springer (1974).

[87] G.C. Shephard and J.A. Todd, Finite unitary reflection groups, *Canad. J. Math.* **6** (1954), 274–304.

[88] M.E. Sweedler, Hopf algebras, W.A. Benjamin (1969).

[89] P. Tarrago and M. Weber, Unitary easy quantum groups: the free case and the group case, *Int. Math. Res. Not.* **18** (2017), 5710–5750.

[90] J.R. Taylor, Classical mechanics, Univ. Science Books (2003).

[91] D.V. Voiculescu, K.J. Dykema and A. Nica, Free random variables, AMS (1992).

[92] J. von Neumann, Mathematical foundations of quantum mechanics, Princeton Univ. Press (1955).

[93] S. Weinberg, Foundations of modern physics, Cambridge Univ. Press (2011).

[94] S. Weinberg, Lectures on quantum mechanics, Cambridge Univ. Press (2012).

[95] D. Weingarten, Asymptotic behavior of group integrals in the limit of infinite rank, *J. Math. Phys.* **19** (1978), 999–1001.

[96] H. Weyl, The theory of groups and quantum mechanics, Princeton Univ. Press (1931).

[97] H. Weyl, The classical groups: their invariants and representations, Princeton Univ. Press (1939).

[98] H. Weyl, Space, time, matter, Princeton Univ. Press (1918).

[99] E. Wigner, Characteristic vectors of bordered matrices with infinite dimensions, *Ann. of Math.* **62** (1955), 548–564.

[100] S.L. Woronowicz, Compact matrix pseudogroups, *Comm. Math. Phys.* **111** (1987), 613–665.

Index