# REPRESENTATIONS OF Finite and Lie Groups

Charles B Thomas

Imperial College Press

# REPRESENTATIONS OF Finite and Lie Groups

Charles B Thomas
University of Cambridge, UK

ICP
Imperial College Press

*Published by*

Imperial College Press
57 Shelton Street
Covent Garden
London WC2H 9HE

*Distributed by*

World Scientific Publishing Co. Pte. Ltd.
5 Toh Tuck Link, Singapore 596224
*USA office:* 27 Warren Street, Suite 401–402, Hackensack, NJ 07601
*UK office:* 57 Shelton Street, Covent Garden, London WC2H 9HE

**British Library Cataloguing-in-Publication Data**
A catalogue record for this book is available from the British Library.

**REPRESENTATIONS OF FINITE AND LIE GROUPS**

ISBN 1-86094-482-5
ISBN 1-86094-484-1 (pbk)

Printed in Singapore by World Scientific Printers (S) Pte Ltd

# REPRESENTATIONS OF Finite and Lie Groups

C.B. Thomas

In memory of Ali Fröhlich
(1916–2001)

# Preface

Good grief, not another book on representation theory! A cursory inspection of the small, if select, library at the Max-Planck-Institut in Bonn yields at least eight good introductory texts. These include the elegant book by J.P. Serre [J-P. Serre], against which all others should be judged. Beyond that the choice is perhaps a matter of taste - what particular slant does the author give to the subject, has she or he any special concerns? The approach chosen here is to present the elementary representation theory of finite groups in characteristic zero in a way which generalises immediately to compact topological groups. The only fresh ingredient needed is an invariant integral, which replaces taking the average by means of the sum over the group elements divided by its order. The parallel development is summarised at the end of Chapter 6; with finite groups as a special case of compact groups there is an inner product on the space of class functions under which the irreducible characters form a normal orthogonal set spanning a dense subspace. Two other topics receive special attention, exterior powers and the finite algebraic groups $SL_2(\mathbb{F}_p)$. I have long believed that the $\lambda$-structure of the representation ring $R(G)$ is a much under-used tool. Some indication of this is given in the exercises devoted to the symmetric groups $S_n$, but the applications are much wider, extending not only to the various families of simple groups of Lie type, but also to the 26 sporadic groups. As a topologist I have long been interested in $SL_2(\mathbb{F}_p)$, and Chapter 8 is intended to illustrate the general principle that in characteristic zero the representation theory of a finite algebraic group has the flavour of the theory for the corresponding group defined over $\mathbb{R}$ or $\mathbb{C}$. In contrast in the natural characteristic $p$ the model is that of a maximal compact subgroup in the complexification.

The exercises are an important part of the text, and should be attempted, not just for their own sake, but also because in a few cases the results are used in a later chapter. The book concludes with an uneven collection of hints, worked solutions and additional references. The bibliography is short and contains no more than the rival books, which I have consulted, and references to theorems mentioned in the text but not proved. The starred sections ($*$) may be omitted at a first reading.

The book has grown out of various sets of notes for a course of 16 or 24 lectures at the senior year level at Cambridge. My thanks are due to the generations of students who have attended, and interrupted, these lectures and to those who I have individually supervised. Their comments are a reminder of what a privilege it is to work in a great university. Errors inevitably remain, and are solely my responsibility.

I wrote the final version during sabbatical leave from Cambridge at the University of California at Santa Cruz, Stanford University and the Max-Planck-Institut in Bonn. I am grateful to all three institutions for their hospitality and support. I also thank Laurent Chaminade and Gabriella Frescura at Imperial College Press for their help, and most of all Michèle Bailey for typing and producing the camera-ready text.

Bonn, Michaelmas 2003

# Contents

# Chapter 1

# Introduction

Our topic is the representation theory of finite and, more generally, of compact topological groups . The latter will be defined formally later; for the moment the reader can think of a topological group as a set carrying both a topology and a group structure, which are compatible in the sense that multiplication and inversion are continuous. Examples are $SL_2(\mathbb{R})$ (non-compact) and the special unitary groups $SU_n$ (compact), both of which are important in theoretical physics. A representation of $G$ is a homomorphism of $G$ into $Aut_{\mathbb{C}}(V)$, the group of linear automorphisms of a finite dimensional vector space over the complex number $\mathbb{C}$. By choosing a basis $\{e_1 \ldots e_n\}$ of $V$ such a representation determines a homomorphism

$$\rho : G \longrightarrow GL_n(\mathbb{C}).$$

If $G$ carries a topology, we give $GL_n(\mathbb{C})$ its topology as an open subset of $\mathbb{C}^{n^2}$, and require the homomorphism $\rho$ to be continuous.

**Examples.**

(i) Let $C_r^a = \{a : a^r = 1\}$ be a cyclic group of order $r$ generated by $a$, and let $\zeta$ be some primitive $r$th root of unity. The homomorphism $\alpha_q : C_r \rightarrow U_1 \subseteq \mathbb{C}^* = \mathbb{C} - \{0\}$ which maps $a$ to $\zeta^q$ is a 1-dimensional representation of the group. Note that $\alpha_q$ is injective (we say that $\alpha_q$ is 'faithful') if and only the greatest common divisor ($gcd = (r, q)$) of $r$ and $q$ equals 1. We will see later that every representation of a finite abelian group $A$ is built up from 'irreducible' representations of this kind.

(ii) Let $G = Q_8$, the quaternion group with presentation

$$\{a, b : a^4 = 1,\ a^2 = b^2,\ b^{-1}ab = a^{-1}\}.$$

Such a 'presentation' can be regarded as a contracted multiplication table in that it tells us that each element can be written as a product $a^i b^j$, that there are eight such distinct products, and that they can be multiplied using the rule $ba^{-1} = ab$ repeatedly. [Exercise - Write out the multiplication table, and check that it corresponds to that of the basic quaternions $\{\pm 1, \pm i, \pm j, \pm k\}$ under the rule $a \leftrightarrow i, b \leftrightarrow j$.]
The map $\rho$

$$a \longmapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad b \longmapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

extends to a homomorphism of $Q_8$ into $SU_2$.

If $\mathbb{H}$ denotes the algebra of quaternions, note that $\mathbb{H}$ is 2-dimensional over $\mathbb{C}$ and that $SU_2$ may be identified with the quaternions of unit length, using the representation just defined. The group $Q_8$ also has 1-dimensional representations, obtained by composing the projection homomorphism

$$\pi : Q_8 \to C_2^{\overline{a}} \times C_2^{\overline{b}}$$

having $\mathrm{Ker}(\pi)$ equal to the subgroup generated by $a^2$, with any one of the four 1-dimensional representations mapping $\overline{a}, \overline{b}$ to $\pm 1$. We label these as $1, \alpha, \beta$ and $\alpha\beta$. Using the multiplication table we see that $Q_8$ has five conjugacy classes of elements

$$(1)\ (a^2)(a, a^{-1})(b, b^{-1})(ab, a^{-1}b).$$

Taking the trace of the representating matrices, and noting that the trace is constant on conjugacy classes, we obtain the following table

| | $1$ | $a^2$ | $a$ | $b$ | $ab$ |
|---|---|---|---|---|---|
| $1$ | $1$ | $1$ | $1$ | $1$ | $1$ |
| $\alpha$ | $1$ | $1$ | $-1$ | $1$ | $-1$ |
| $\beta$ | $1$ | $1$ | $1$ | $-1$ | $-1$ |
| $\alpha\beta$ | $1$ | $1$ | $-1$ | $-1$ | $1$ |
| $\rho$ | $2$ | $-2$ | $0$ | $0$ | $0$ |

.

We ask the reader to check three things about this square array. First and most importantly, each row can be associated unambiguously with one of the representations described. Secondly, if we add the first four entries in each column to twice the fifth we obtain 8 (equals the order $|Q_8|$) for column one and zero otherwise. Thirdly, even though the matrices describing $\rho$ are complex, the entries in the table are real. We shall see later that these are special cases of important general phenomena.

Before leaving $Q_8$ let us present the generalised quaternion group of order $4t$, which will be useful later,

$$Q_{4t} = \{a, b : a^{2t} = 1, a^t = b^2, b^{-1}ab = a^{-1}\}.$$

In terms of the quaternion algebra $\mathbb{H}$ $a$ can be identified with $e^{\pi i/t}$ and $b$ with $j$.

Given a homorphism of $G$ into $Aut_{\mathbb{C}}(V)$ we can think of $G$ as *acting* on the vector space $V$ via the map $g.v = \rho(g)v$ for all $v \in V$. More directly we can define such an action as a (continuous) map

$$\begin{aligned} G \times V &\longrightarrow V \\ (g, v) &\longmapsto g \cdot v \end{aligned}$$

satisfying $g_1(g_2v) = (g_1g_2)v$ and $1 \cdot v = v$ for all $g_1, g_2 \in G$ and $v \in V$. At least when $G$ is finite, the $G$-action and $\mathbb{C}$-action (scalar product) on $V$ can be combined as a $\mathbb{C}[G]$-action, where $\mathbb{C}[G]$ denotes the so-called *group algebra* of the finite group $G$.

**Definition.** The ring $\mathbb{C}[G]$ consists of formal linear combinations

$$\begin{aligned} &\textstyle\sum_{g\in G} \lambda_g g, \text{ where } \lambda_g \in \mathbb{C}, \text{ and} \\ &\textstyle\sum_{g\in G} \lambda_g g + \sum_{g\in g} \mu_g g = \sum_{g\in G}(\lambda_g + \mu_g)g, \\ &\textstyle(\sum_{g\in G} \lambda_g g)(\sum_{h\in G} \mu_h h) = \sum_{k\in G} \sum_{gh=k} \lambda_g \mu_h k. \end{aligned}$$

It is a straightforward and tedious exercise to check that, with these definitions of addition and multiplication, $\mathbb{C}[G]$ is a ring, which is commutative if and only if $G$ is an abelian group. Although we are primarily interested in the complex group algebra, it is important to note that the same definition holds with $A$ equal to any commutative ring rather than $A = \mathbb{C}$. We then obtain the group ring $A[G]$, which has been much-studied both by topologists and number theorists.

**Examples.**

(i) Write out the multiplication table for the group ring $\mathbb{F}_2[C_2]$, where $\mathbb{F}_2$ is the finite field with 2 elements, and $C_2$ is a cyclic group of order 2.

(ii) If $C_p^a$ is a cyclic group of order $p$ ($p$ = prime), and $\zeta$ is a primitive $p^{\text{th}}$ root of unity (for example $\zeta = e^{2\pi i/p}$), show that the map $a \longmapsto \zeta$ extends to a homomorphism of rings $\mathbb{Z}[C_p] \to \mathbb{Z}(\zeta) \hookrightarrow \mathbb{Q}(\zeta)$, and identify its kernel.

The discussion above shows that, for finite groups $G$, complex representation theory is equivalent to the theory of the structure of finitely-generated $\mathbb{C}[G]$-modules. One of our first results will be to show that $\mathbb{C}[G]$ belongs to a very special class of *semisimple* rings, and, although we shall not adopt this approach, the whole of classical representation theory can be read as a special case of that of semisimple rings. We develop this more abstract algebra in Appendix B.

Now for some basic definitions, which can be formulated either in the language of $G$-spaces or of $\mathbb{C}[G]$-modules.

(1) The $G$-spaces $V_1$ and $V_2$ are said to be *equivalent* if there exists a $\mathbb{C}$-linear isomorphism $f : V_1 \to V_2$, compatible with the $G$-actions. This means that $f(\rho_1(g)v) = \rho_2(g)f(v)$ for all $g \in G$ and $v \in V_1$.
Note that we must distinguish carefully between $\text{Hom}_{\mathbb{C}}(V_1, V_2)$ and $\text{Hom}_{\mathbb{C}[G]}(V_1, V_2)$, and that equivalence is expressed in terms of the latter family of homomorphisms. Note also that a group homomorphism from $G$ into $Aut_{\mathbb{C}}(V)$ extends to an algebra homomorphism $\mathbb{C}[G] \to \text{Hom}_{\mathbb{C}}(V, V)$, and that conversely, given such an algebra homomorphism, we can recover $\rho$ by restricting to the elements of $G$. However injectivity of the group homomorhpism does not necessarily imply injectivity of the algebra homomorphism.

(2) The ring of linear maps $\text{Hom}_{\mathbb{C}}(V, V)$ is itself a vector space over $\mathbb{C}$ and can be given the structure of a $G$-space using the definition $gf(v) = g(f(g^{-1}v))$. Clearly the same holds when $V$ is replaced by a pair of $G$-spaces $V_1$ and $V_2$, and $\text{Hom}_{\mathbb{C}[G]}(V_1, V_2)$ coincides with the subset of invariant elements. Notation: For any $G$-space $V$, $V^G = \{v \in V : gv = v \text{ for all } g \in G\}$. Thus

$$\text{Hom}_{\mathbb{C}[G]}(V_1, V_2) = \text{Hom}_{\mathbb{C}}(V_1, V_2)^G.$$

If $G$ acts trivially on $V$, i.e. the image of $\rho$ in $Aut_{\mathbb{C}}(V)$ equals $1_n$, the identity map, we write $V^G = V$.

(3) As with ordinary vector spaces we can define sub-objects and quotient objects. A $G$-subspace of $V$ is thus a $\mathbb{C}[G]$-submodule, or a sub-vector space $W \subseteq V$ such that $gw \in W$ for all $g \in G$ and $w \in W$. Given

a $G$-homomorphism $f : V_1 \to V_2$ we note that the kernel of $f$ is a $G$-subspace of $V_1$ and that the quotient vector space $V_2/f(V_1)$ admits a $G$-action with respect to which the projection map $V_2 \to V_2/f(V_1)$ is a $G$-homomorphism.

**Definition.** The $G$-space $V$ is said to be *irreducible* if the only $G$-invariant subspaces are $\{0\}$ and $V$ itself. The space $V$ is *indecomposable* if there is no non-trivial splitting of $V$ as the direct sum of $G$-subspaces $W \oplus W'$.

**Proposition 1.1** *(Schur's Lemma) Let $V_1$ and $V_2$ be irreducible $G$-spaces. A $G$-linear map $f : V_1 \to V_2$ is either trivial or an isomorphism. In particular if $V = V_1 = V_2$, $\mathrm{Hom}_{\mathbb{C}[G]}(V, V)$ is a division ring.*

***Proof.*** Consider the kernel of a $G$-linear map $f$. Since $V_1$ is irreducible this either equals $V_1$, in which case $f$ is trivial, or equals $\{0\}$, in which case $V_1$ maps injectively onto its image. This is a submodule of $V_2$, hence either trivial or equal to $V_2$. Hence a non-trivial map $f$ must be bijective. The second claim is an immediate consequence of this. □

(4) If $V$ is a finite-dimensional $G$-space we can define a $\mathbb{C}$-linear map

$$\begin{aligned} \mathrm{Tr}_G : V &\longrightarrow V^G \text{ by} \\ v &\longmapsto \textstyle\sum_{g \in G} gv. \end{aligned}$$

The image is invariant, since pre-multiplication by $h \in G$ does no more than permute the elements $gv$ among themselves. As an important special case note that, if $f \in \mathrm{Hom}_{\mathbb{C}}(V_1, V_2)$, then $\mathrm{Tr}_G(f) \in \mathrm{Hom}_{\mathbb{C}[G]}(V_1, V_2)$.
More generally consider the composition

$$V_1' \underset{\varphi}{\longrightarrow} V_1 \underset{f}{\longrightarrow} V_2 \underset{\psi}{\longrightarrow} V_2',$$

where $\varphi, f$ and $\psi$ are all $\mathbb{C}$-linear and $\varphi, \psi$ are $G$-maps. Then $\mathrm{Tr}_G(\psi \cdot f \cdot \varphi) = \psi \cdot \mathrm{Tr}_G(f) \cdot \varphi$.

**Proposition 1.2** *(Maschke's Theorem) Let $W$ be a $G$-subspace of the finite-dimensional $G$-space $V$ over the complex numbers. There exists a complementary $G$-subspace $W'$ such that $V \cong W \bigoplus W'$.*

***Proof.*** Decompose $V$ as a direct sum $W \bigoplus W'$ over the complex numbers $\mathbb{C}$, and let $\pi : V \to W$ be the $\mathbb{C}$-linear projection map onto $W$. Thus $\pi(v) = v$ for all $v \in W$. We can average $\pi$ over the elements of the finite group $G$ by setting

$$\varphi = \frac{1}{|G|}\mathrm{Tr}_G(\pi)$$

obtaining a pair of $G$-homomorphisms

$$\begin{tikzcd} 0 \arrow[r] & W \arrow[r, shift left, "j"] & V, \arrow[l, shift left, "\varphi"] \end{tikzcd}$$

such that $j$ is the inclusion, and $\varphi \cdot j = \mathrm{Id}_W$. It is now easy to see that there is a $G$-splitting of $V$ as

$$V \text{ as } W \oplus \ker(\varphi),$$

so that we can take $W' = \ker(\varphi)$. From the definitions, $jW \cap \ker(\varphi) = \{0\}$, and for an arbitrary element $v \in V, v - \varphi(v) \in \ker(\varphi)$. □

Simple though its proof is, Maschke's Theorem is fundamental to representation theory. We note in passing that it holds for representation spaces over an arbitrary field $k$ provided either that the characteristic of $k$ does not divide $|G|$, the order of $G$, or that the characteristic equals 0. We may use it for example to study representations of a finite $p$-group of order $p^t$ over an extension field of $\mathbb{F}_q (q \neq p)$.

**Definition.** Let $R$ be a ring. The $R$-module $V$ is said to be *semisimple* if every $R$-submodule is a direct summand. The ring $R$ itself is said to be semisimple, if $1 \neq 0$, and $R$ is semisimple as a left module over itself.

We state the next group of results in terms of semisimple rings rather than in terms of the special case $\mathbb{C}[G]$.

Throughout we assume that all the rings $R$ which we consider contain a multiplicative identity $1 = 1_R$. Although not strictly necessary we will also make this assumption in Appendix B.

**Proposition 1.3** *The following two conditions are equivalent on a (finitely generated) $R$-module $V$:*

*(1) $V$ is a (finite) direct sum of irreducible $R$-modules,*
*(2) Every submodule of $V$ is a direct summand.*

***Proof.*** Let $V = \bigoplus_{i \in I} V_i$, $W \subseteq V$ and $J$ be a maximal subset of the indexing set $I$ such that the sum $W + \bigoplus_{j \in J} V_j$ is direct. We claim that this sum $V^*$ equals $V$, that is contains each summand $V_i$, $i \in I$. The intersection $V^* \cap V_i = \{0\}$ or $V_i$ because $V_i$ is irreducible. In the former case we can adjoin $i$ to $J$, and $J$ is not maximal. Hence $V_i \subseteq V^*$.

We next show that if (2) holds, $V$ is a sum of irreducible $R$-modules, with the sum not necessarily direct. An intermediate result is that every non-zero $R$-module contains an irreducible $R$-module. Let $v \in V, v \neq 0$, and consider the submodule $Rv$. The kernel of the homomorphism $R \to Rv$ is a left ideal $L$ in $R$, contained in a maximal ideal $M \neq R$. Then $M/L$ is a maximal submodule of $R/L$, and hence $Mv$ is a maximal submodule of $Rv$, not equal to $Rv$. We have isomorphisms

$$R/L \xrightarrow{\sim} Rv$$
$$M/L \xrightarrow{\sim} Mv,$$

and since (2) holds $V = Mv \oplus M'$ for some submodule $M'$. Furthermore

$$Rv = Mv \oplus (M' \cap Rv),$$

because every element $x \in Rv$ decomposes uniquely as $x = \alpha v + x'$, with $\alpha \in M$, $x' \in M'$, $x' = x - \alpha v \in Rv$. The maximality of $Mv$ in $Rv$ implies that $M' \cap Rv$ is irreducible.

Let $V_0 \subseteq V$ be the sum of all irreducible submodules of $V$. If $V_0 \neq V$, $V = V_0 \oplus W$ with $W \neq \{0\}$, and there exists an irreducible submodule of $W$, contradicting the definition of $V_0$.

Passage from sum to direct sum is achieved by the same trick as in the proof that (1) $\Rightarrow$ (2), i.e. take the maximal direct sum in $V$ and show that it contains each $V_i$. We leave this as an exercise. □

**Proposition 1.4** *Every submodule and every quotient module of a semisimple module is semisimple; also every finitely generated $R$-module over a semisimple ring $R$ is semisimple.*

***Proof.*** Let $U$ be a submodule of $W$ a submodule of $V$. Since $V$ is semisimple $V$ splits as $U \oplus U'$. If $w \in W$ $w$ decomposes uniquely as $w = u + u'$ with $u \in U$, $u' \in U'$. But $u' = w - u$ also belongs to $W$, so that $W = U \oplus (U' \cap W)$. Hence $U$ is a direct summand of $W$. For the quotient module $V/W$ we have a splitting $V = W \oplus W'$, with $W'$ semisimple and isomorphic to $V/W$. Finally every module over a semisimple ring is semisimple, since it may be expressed as the quotient of a free module

$F$ over $R$. As a sum of copies of the underlying ring $F$ is semisimple by Proposition 1.3. □

Our aim is to show that an irreducible module $V$ can give rise to a kind of duality between the original ground ring $R$ and the ring $S = \mathrm{End}_R(V) = \mathrm{Hom}_R(V, V)$. This is sometimes called the *double centraliser condition.*

Let $V$ be a semisimple $R$-module, i.e. a direct sum of irreducible (hence "simple") $R$-modules. As above let $S = \mathrm{End}_R(V)$. We can regard $V$ as an $S$-module with scalar multiplication defined by

$$(\varphi, v) \mapsto \varphi(v)$$

for $\varphi \in S$ and $v \in V$. Each $\alpha \in R$ induces an $S$-homomorphism $f_\alpha : V \to V$ via the rule $f_\alpha(v) = \alpha v$. This is an $S$-map, because of the module condition $\varphi(\alpha v) = \alpha\varphi(v)$. Hence there is a homomorphism of rings

$$\begin{aligned} R &\longrightarrow \mathrm{End}_S(V) \\ \alpha &\longmapsto f_\alpha, \end{aligned}$$

and we would like to know the size of the image.

**Proposition 1.5** *Let $V$ be semisimple over $R$, $S = \mathrm{End}_R(V)$ and $f \in \mathrm{End}_S(V)$. For an arbitrary element $v \in V$ we can find $\alpha \in R$ such that $\alpha v = f(v)$.*

***Proof.*** Using the semi-simplicity of $V$ write $V = Rv \oplus W$ with projection map $\pi : V \to Rv, \pi \in \mathrm{Hom}_R(V, V) = S$.
Since $f$ is given to be an $S$-map, $f(v) = f(\pi v) = \pi f(v)$, which must belong to the submodule $Rv$. □

Using a diagonal trick one can generalise 1.5 from one to finitely many elements of $V$.

**Proposition 1.6** *Let $V$ be irreducible over $R$, $S = \mathrm{End}_R(V)$, $f \in \mathrm{End}_S(V)$. Let $v_1 \ldots v_n$ be elements of $V$. Then we can find an element $\alpha \in R$ such that $\alpha v_i = f(v_i)$ for $i = 1, 2, \ldots, n$.*

***Proof.*** Consider the product map

$$\begin{aligned} &f^{(n)} : V^n \to V^n \\ &(v_1 \ldots v_n) \mapsto (f(v_1) \ldots f(v_n)), \end{aligned}$$

and write $S' = \mathrm{End}_R(V^n)$. As in elementary linear algebra, the ring $S'$ can be identified with the ring of $n \times n$ matrices with coefficients in $S$. The