

Lectures on semisimple rings and representation theory — preliminary draft

Pedro Resende

December 12, 2024

Abstract

Support notes for the MMAC course “Modules and Representations” of IST in the academic year 2024/2025. Each of the following “lectures” corresponds to a 50 minute session, or a 100 minute session in the case of the “double lectures”.

Contents

Introduction	3
Lecture 1 (double). Algebras and representations	3
1.1 Smith normal forms (conclusion)	3
1.2 More on injective modules	3
1.3 Associative algebras	6
1.4 Group algebras and representations	7
Lecture 2. Constructions of algebras	9
2.1 Endomorphisms and matrices	10
2.2 Algebra of a small category	10
2.3 Quivers	11
2.4 Tensor algebras	12
2.5 Quotients of algebras	12
Lecture 3 (double). Examples based on tensor algebras	13
3.1 Complements on previous lecture	13
3.2 The universal enveloping algebra of a Lie algebra	14
3.3 Derivations	16
Test 3 (MAP30)	16
Lecture 4. Irreducible representations	17
4.1 Representations of algebras	17
4.2 Irreducible representations and Schur’s Lemma	19

Lecture 5 (double). Semisimple modules and rings	20
5.1 Complement on simple modules	20
5.2 Semisimple modules	21
5.3 Semisimple rings	21
5.4 Example: Maschke's Theorem	23
Lecture 6 (double). Simple rings	24
6.1 Complements from previous lecture	24
6.2 Structure of simple rings	25
Lecture 7. Idempotents	29
Lecture 8 (double). Structure of semisimple rings	31
8.1 Conclusion of the previous lecture	31
8.2 Artin–Wedderburn theorem	31
8.3 More on group algebras	34
Lecture 9 (double). Characters of finite groups	35
9.1 More on group representations	35
9.2 Character theory	37
Lecture 10. Some character tables	42
10.1 Euclidean structure	42
10.2 Character tables	44
10.3 Example: character table of D_8	45
10.4 Example: character table of D_{14}	47
Lecture 11 (double). General representation theory	49
11.1 Jacobson's density theorem	50

Introduction

These notes are meant to provide an introduction to representation theory, in particular of finite groups, via the notion of semisimple ring and the theorem of Artin–Wedderburn. For further reading see [1–3].

Unless otherwise stated, the rings and ring homomorphisms in these notes are assumed to be unital.

- [1] J. A. Beachy, *Introductory lectures on rings and modules*, London Mathematical Society Student Texts, vol. 47, Cambridge University Press, Cambridge, 1999. MR1723048
- [2] D. S. Dummit and R. M. Foote, *Abstract algebra*, 3rd ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004. MR2286236
- [3] S. Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. MR1878556

Lecture 1 (double). Algebras and representations

Sections 1.1 and 1.2 conclude the material for Test 3 (MAP30). From section 1.3 onwards is the material on algebras and representation theory, which will be evaluated in Test 4 (MAP45).

1.1 Smith normal forms (conclusion)

§1. EXERCISE. Compute a Smith normal form (over \mathbb{Z}) of the matrix

$$\begin{pmatrix} 3 & 6 \\ 9 & 317 \end{pmatrix}$$

1.2 More on injective modules

When we studied projective modules we saw that one of the equivalent conditions for a module P to be projective is that every epimorphism $\varphi : M \rightarrow P$ is a retraction. There is an analogous condition for injective modules which we did not address, so let us do it now.

First we need a simple condition regarding pushouts of modules (for an arbitrary ring R), where by a *pushout square* in any category \mathcal{C} is meant the same as a pullback square in \mathcal{C}^{op} . Let A , B and C be R -modules, with

homomorphisms as follows:

$$\begin{array}{ccc} C & \xrightarrow{f} & A \\ g \downarrow & & \\ B & & \end{array}$$

Let $K \subset A \oplus B$ consist of all the pairs $(f(c), -g(c))$ with $c \in C$. By an easy application of the submodule criterium we see that K is a submodule of $A \oplus B$. Let $P = (A \oplus B)/K$ (this means that all the pairs $(f(c), 0)$ and $(0, g(c))$ are identified in the quotient), and let $q : A \oplus B \rightarrow P$ the quotient homomorphism. Letting $\iota_1 : A \rightarrow A \oplus B$ and $\iota_2 : B \rightarrow A \oplus B$ be the canonical injections, we obtain a commutative square which is easily seen to be a pushout square (exercise!):

$$\begin{array}{ccc} C & \xrightarrow{f} & A \\ g \downarrow & & \downarrow j_1 := q\iota_1 \\ B & \xrightarrow{j_2 := q\iota_2} & P \end{array}$$

(As always for universal properties, any other pushout of f and g is isomorphic to P .)

You may recall that, in any category, pullbacks are well behaved with respect to monomorphisms in the sense that the pullback of a monomorphism is itself a monomorphism. Dually, any pushout (also called a pushforward) of an epimorphism is itself an epimorphism. This holds for arbitrary categories. But for the category of R -modules we have an additional fact:

§2. LEMMA. *Any pushout of a monomorphism of R -modules is itself a monomorphism of R -modules.*

Proof. Let the following be a pushout square of R -modules:

$$\begin{array}{ccc} C & \xrightarrow{f} & A \\ g \downarrow & & \downarrow j_1 \\ B & \xrightarrow{j_2} & P \end{array}$$

Let us assume concretely, as above, that $P = (A \oplus B)/K$ and $j_i = q\iota_i$. The statement of the lemma means that if f is a monomorphism then so is j_2 (and that if g is a monomorphism so is j_1). So let us assume that f is a monomorphism, and let $b \in \ker j_2$. This means that $(0, b) = \iota_2(b) \in K$, so there must be $c \in C$ such that $(0, b) = (f(c), -g(c))$. Since f is mono, this means that $c = 0$, so $b = g(c) = 0$, and we conclude that $\ker j_2 = 0$. ■

§3. THEOREM. *The following conditions are equivalent, for any R -module Q :*

1. Q is injective.
2. Every monomorphism $\psi : Q \rightarrow M$ is a section.

Proof. The condition $1 \Rightarrow 2$ is an easy exercise, for if Q is injective and $\psi : Q \rightarrow M$ is mono then there exists a lifting μ of 1_Q as in the following diagram — the lifting is the required retraction of ψ :

$$\begin{array}{ccc} & & M \\ & \nearrow \mu & \uparrow \psi \\ Q & \xleftarrow{1_Q} & Q \end{array}$$

Now let us prove $2 \Rightarrow 1$. Assume that every monomorphism $j : Q \rightarrow P$ is a section, and consider the following diagram of R -modules, where $\psi : L \rightarrow M$ is a monomorphism:

$$\begin{array}{ccc} & & M \\ & & \uparrow \psi \\ Q & \xleftarrow{f} & L \end{array}$$

In order to show that Q is injective we will obtain a lifting F of f . Consider the pushout of f and ψ :

$$\begin{array}{ccc} P & \xleftarrow{j_1} & M \\ j_2 \uparrow & & \uparrow \psi \\ Q & \xleftarrow{f} & L \end{array}$$

Since, by §2, j_2 is a monomorphism, by hypothesis it has a retraction $\mu : P \rightarrow Q$, so making $F = \mu j_1$ we obtain the envisaged lifting of f :

$$F\psi = \mu j_1 \psi = \mu j_2 f = f. \blacksquare$$

t This characterization of injective modules leads to a surprising fact that relates injective to projective modules. Although injective modules are certainly not the same as projective modules (for instance, \mathbb{Z} is a projective \mathbb{Z} -module but it is not injective, whereas \mathbb{Q} is injective but not projective — check this as an exercise), the following property holds for any ring R :

§4. COROLLARY. *The following properties are equivalent:*

1. *All R -modules are injective.*
2. *All R -modules are projective.*
3. *Every short exact sequence of R -modules splits.*

Proof. Exercise. ■

1.3 Associative algebras

Here we recall the notion of *algebra* over a commutative ring, often termed *associative algebra* in order to distinguish it from other types of algebras, such as Lie algebras. Whenever we say only “algebra” we will be referring to associative algebras.

§5. DEFINITION. Let R be a commutative ring. By an R -algebra is meant a ring A together with a ring homomorphism $\iota : R \rightarrow A$, called the *injection of scalars*, whose image is in the center of A .

§6. DEFINITION. Given two R -algebras $A \equiv (A, \iota_A)$ and $B \equiv (B, \iota_B)$, a *homomorphism of R -algebras* $\varphi : A \rightarrow B$ is a (necessarily unital) homomorphism of rings for which the following diagram commutes (i.e., φ preserves the scalars):

$$\begin{array}{ccc}
 A & \xrightarrow{\varphi} & B \\
 \iota_A \swarrow & & \searrow \iota_B \\
 & R &
 \end{array}
 \tag{1}$$

This defines the category of R -algebras, which we denote by $R\text{-Alg}$.

§7. EXAMPLES. Let R be a commutative ring.

1. $M_n(R)$ is an R -algebra with injection of scalars $\iota : R \rightarrow M_n(R)$ given by $r \mapsto rI$ where I is the identity matrix.
2. $R[x]$ is an R -algebra with injection of scalars $\iota : R \rightarrow R[x]$ yielding the polynomial r of degree zero for each $r \in R$.

Note that in these two cases the injection of scalars is injective. In fact in the second example we always regard R concretely as a subring of $R[x]$. See appendix ?? for a brief account of the universal property of $R[x]$ and a consequence of it which has already been exploited in our study of Jordan canonical forms.

§8. NOTATION. Any R -algebra A with injection of scalars ι has a structure of R -module whose action $\cdot : R \times A \rightarrow A$ is given, for each $r \in R$ and $a \in A$, by $r \cdot a = \iota(r)a$. Usually we shall just write ra if no confusion may arise. In particular, if R is a field then A is a vector space over R , whose multiplication by scalars is given by the action.

§9. EXERCISE. Prove that a homomorphism φ of R -algebras is the same as a ring homomorphism which is equivariant with respect to the action; that is, such that for all $r \in R$ and $a \in A$,

$$\varphi(ra) = r\varphi(a).$$

§10. EXERCISE. Show that for all $r \in R$ and $a, b \in A$ the action satisfies the following additional conditions:

$$\begin{aligned} r(ab) &= (ra)b \\ r(ab) &= a(rb). \end{aligned}$$

§11. EXERCISE. Show that an R -algebra is the same thing as a ring A which is also an R -module such that the two conditions in the previous exercise hold. (Hint: define $\iota(r) = r1_A$.)

§12. EXERCISE. Let R be a commutative ring, and M an R -module. Show that $\text{End}_R(M)$ is an R -algebra. (Hint: define the action of $r \in R$ on $f \in \text{End}_R(M)$ by $(rf)(m) = rf(m)$.)

§13. NONUNITAL ALGEBRAS. The definition of an R -algebra and of R -algebra homomorphisms in terms of the action of R makes sense even if A does not have a unit. In that case the injection of scalars is not well defined, but we still have a working definition of R -algebra in terms of the action. This is the case when we define the R -algebra of an arbitrary small category, or of a general quiver (see below) because, as we shall see, the algebra we obtain is unital only when the object set of the category is finite (resp., the vertex set of the quiver is finite).

1.4 Group algebras and representations

Now let us take advantage of the fact that the students of this course already know the example of a group ring, at least for finite groups, in order to give the first example of how representations of finite groups relate to representations of an algebra. In what follows, given a ring R and a finite set X , we

denote the free R -module on X by RX , and will think of it concretely as consisting of the set of all the formal linear combinations

$$RX = \left\{ \sum_{x \in X} r_x x \mid r_x \in R \right\}.$$

§14. PROPOSITION. *Let R be a commutative ring and G a finite group with unit 1_G . The free R -module RG is an R -algebra whose unit coincides with 1_G and whose multiplication is defined by bilinear extension of the multiplication of G :*

$$\left(\sum_{g \in G} r_g g \right) \left(\sum_{h \in G} s_h h \right) = \sum_{g, h \in G} r_g s_h gh.$$

Proof. Straightforward. ■

§15. EXERCISE. Let R be a commutative ring. Show that the mapping $A \mapsto A^\times$ yields a functor $U : R\text{-Alg} \mapsto \text{Grp}$.

§16. PROPOSITION. *Let R be a commutative ring with unit 1_R , G a finite group, and $\eta : G \rightarrow RG$ the mapping given by $g \mapsto 1_R g$. The pair (RG, η) is a universal arrow from G to the functor U .*

Proof. We need to show the following:

1. η defines a group homomorphism $G \rightarrow (RG)^\times$;
2. For any R -algebra A and any group homomorphism $\varphi : G \rightarrow A^\times$ there is a unique homomorphism of R -algebras $\varphi^\sharp : RG \rightarrow A$ whose restriction to $(RG)^\times$ makes the diagram on the left commute:

$$\begin{array}{ccc}
 & \text{Grp} & \\
 & & \\
 G & \xrightarrow{\eta} & (RG)^\times & & RG \\
 & \searrow \varphi & \downarrow U(\varphi^\sharp) & & \downarrow \varphi^\sharp \\
 & & A^\times & & A
 \end{array}$$

The fact that η is a homomorphism of groups is immediate. For the second condition let $G = \{g_1, \dots, g_n\}$. We define φ^\sharp by

$$\varphi^\sharp(r_1 g_1 + \dots + r_n g_n) = r_1 \varphi(g_1) + \dots + r_n \varphi(g_n).$$

2.1 Endomorphisms and matrices

§19. DEFINITION. Let V be an R -module. Then $\text{End}_R(V)$ is an R -algebra with product given by composition and R -action defined by $(rf)(v) = r(f(v))$.

§20. EXERCISE. Prove that if V is a free R -module of rank $n > 1$ then $\text{End}_R(V) \cong M_n(R)$.

2.2 Algebra of a small category

§21. DEFINITION. Let C be a small category. Define the R -algebra RC to be $F_R(C_1)$ with multiplication defined by, for all $f, g \in RC$:

$$(f * g)(x) = \sum_{x=yz} f(y)g(z).$$

(This operation is called *convolution*.) Note that all the sums have only finitely many nonzero elements because the supports of f and g are finite.

§22. EXERCISE. Verify that RC is indeed an R -algebra, i.e., show that the multiplication is associative and R -bilinear as required, but that it may fail to be unital. Show that if C_0 is a finite set the algebra RC is unital with unit the function $1 : C_1 \rightarrow R$ defined by

$$1(x) = \begin{cases} 1 & \text{if } x \text{ is an identity arrow,} \\ 0 & \text{otherwise.} \end{cases}$$

Note: for associativity it may help to think of each $f \in RC$ as a formal linear combination $\sum_{x \in C_1} f(x)x$.

§23. EXAMPLE. The algebra RG of a finite group is the algebra of G regarded as a category with only one object. More generally, the construction of the algebra of a category applies to infinite groups, and also to monoids, always yielding a unital algebra.

§24. EXERCISE. Prove that for a group G the ring RG has an *involution*, by which is meant an additive map $i : RG \rightarrow RG$ such that $i(i(f)) = f$ and $i(fg) = i(g)i(f)$ for all $f, g \in G$. Hint: define it by $i(f)(x) = f(x^{-1})$.

§25. REMARK. For $R = \mathbb{C}$ the involution is usually defined by $i(f)(x) = \overline{f(x^{-1})}$, so it is an anti-linear map.

§26. FREE ALGEBRAS. Let X be a set, and X^* its free monoid. The *free R -algebra* generated by X is RX^* , usually denoted by $R\langle X \rangle$. If $|X| = n < \infty$ we write $R\langle x_1, \dots, x_n \rangle$.

§27. WARNING: Do not confuse $R\langle x_1, \dots, x_n \rangle$ with the polynomial ring $R[x_1, \dots, x_n]$ in n indeterminates. In particular, the latter is always commutative, whereas the former is not (unless $n = 1$, in which case $R[x] = R\langle x \rangle$).

§28. EXERCISE. Consider the forgetful functor $U : R\text{-Alg} \rightarrow \text{Set}$. Show that for every set X there is a universal arrow from X to U . Hint: for each set X consider the algebra $R\langle X \rangle$ and the function $\eta : X \rightarrow R\langle X \rangle$ given by $x \mapsto \delta_x$.

§29. NOTE: Often we shall identify elements generators x of a free module with the corresponding basis elements δ_x , for instance regarding the free monoid X^* as a subset of the algebra $R\langle X \rangle$. In particular, we think of elements x_1, \dots, x_n as belonging to the free algebra $R\langle x_1, \dots, x_n \rangle$, just as we do for the polynomial algebra $R[x_1, \dots, x_n]$.

2.3 Quivers

§30. DEFINITION. A *quiver* is a directed graph $Q = (I, E)$ whose set of vertices is I and whose set of edges is E . A *homomorphism of quivers* is a homomorphism of directed graphs. Often the domain and the codomain of an edge h are denoted by h' and h'' , respectively. We shall also use for quivers the same notation as for categories, namely denoting I by Q_0 and E by Q_1 , and h' by $d(h)$ and h'' by $c(h)$.

§31. FREE CATEGORY ON A QUIVER. The free category on a quiver Q , denoted by Q^* , has objects the vertices of Q and edges the paths formed by concatenating edges of Q , including the empty paths, which are the units of the category.

§32. EXERCISE. Formulate and prove the universal property of the free category of a quiver.

§33. DEFINITION. Let Q be a quiver. The R -algebra of Q , denoted by RQ , is the algebra of the free category of Q ; that is, RQ is defined to be RQ^* .

2.4 Tensor algebras

§34. DEFINITION. Let R be a commutative ring and V an R -module. The tensor algebra $T_R(V)$ is defined to be

$$T_R(V) = \bigoplus_{n=0}^{\infty} V^{\otimes n}.$$

with the required R -bilinear multiplication corresponding to the following homomorphism of R -modules,

$$T_R(V) \otimes_R T_R(V) \cong \bigoplus_{i,j=0}^{\infty} V^{\otimes i} \otimes_R V^{\otimes j} \rightarrow T_R(V)$$

which for each pair i, j is given by $V^{\otimes i} \otimes_R V^{\otimes j} \xrightarrow{\cong} V^{\otimes(i+j)} \rightarrow T_R(V)$.

§35. EXERCISE. Formulate and prove the universal property of the tensor algebra (adjunction between $R\text{-Mod}$ and $R\text{-Alg}$). Note that the canonical map $V \rightarrow T_R(V)$ that sends V to the “degree 1 component” $V^{\otimes 1}$ is injective.

§36. GRADING. The tensor algebra $T_F(L)$ is *graded* over the additive monoid $\mathbb{Z}_{\geq 0}$ in the sense that will be defined next:

§37. DEFINITION. Let A be an R -algebra, and S a semigroup. A *grading* of A over S is a direct decomposition $A = \bigoplus_{s \in S} A_s$ into R -submodules A_s such that for all $a \in A_s$ and $b \in A_t$ we have $ab \in A_{st}$.

2.5 Quotients of algebras

§38. DEFINITION. Let A be an R -algebra (possibly non-unital). By a *left ideal* of A is meant an R -submodule $J \subset A$ which is closed under multiplication by elements of A on the left. By a *right ideal* of A is meant an R -submodule $J \subset A$ which is closed under multiplication by elements of A on the right. By an *ideal* of A is meant an R -submodule $J \subset A$ which is both a left ideal and a right ideal.

§39. REMARK. If A has a unit then its three notions of ideal coincide with the same notions when we view A simply as a unital ring, because being an A -module automatically implies being an R -module due to the inclusion of scalars $\iota : R \rightarrow A$.

§40. EXERCISE. Prove that if A is an R -algebra and $I \subset A$ is an ideal of A the quotient ring A/I is itself an R -algebra.

§41. GENERATORS AND RELATIONS. If f_1, \dots, f_m are elements of

$$R\langle x_1, \dots, x_n \rangle,$$

the R -algebra presented by generators x_1, \dots, x_n and relations

$$f_1 = 0, \dots, f_m = 0$$

is

$$R\langle x_1, \dots, x_n \rangle / I,$$

where I is the ideal of A generated by f_1, \dots, f_m . This definition can be extended to any set X of generators and any subset $Y \subset R\langle X \rangle$. We shall write $\langle Y \rangle$ for the ideal generated by the set Y , or $\langle f_1, \dots, f_m \rangle$ in the case of a finite set.

§42. EXAMPLE. Let M be a monoid (or a group). The algebra RM equals $R\langle M \rangle / I$ where the ideal I is generated by the relations $\delta_{xy} = \delta_x \delta_y$ and $1 = \delta_{1_M}$.

§43. EXERCISE. Show how the algebra of a quiver can be presented by generators and relations taking the edges as generators.

§44. EXAMPLE. The Weyl algebra (over R) is

$$R\langle x, y \rangle / \langle yx - xy - 1 \rangle.$$

(This is “almost free” on x and y but subject to the commutation relation $yx - xy = 1$.)

Lecture 3 (double). Examples based on tensor algebras

Again R is a commutative ring with unit.

3.1 Complements on previous lecture

§45. EXERCISE. Show that $T_R(V)$ is an R -algebra.

§46. EXERCISE. Show that the R -algebra of a group G is graded over G .

§47. EXERCISE. Formulate a “natural” definition of R -algebra graded over a small category C and prove that RC is graded in this sense.

§48. EXERCISE. Give a presentation of RC , for a small category C , by generators and relations that uses C_1 as set of generators. Prove that this presentation indeed presents RC . Particularize for group algebras.

§49. EXERCISE. The *exterior algebra* $\bigwedge(V)$, or *Grassmann algebra*, of a vector space V over a field F , is defined to be the quotient of $T_F(V)$ by the ideal I generated by all the simple tensors of the form $x \otimes x$. The class $x \otimes y + I$ is denoted by $x \wedge y$, so in $\bigwedge(V)$ we have $x \wedge x = 0$.

1. Prove that $x \wedge y = -y \wedge x$.
2. Prove that if $\text{char } F \neq 2$ then $\bigwedge(V)$ is also the quotient of $T_F(V)$ by the ideal generated by the elements $x \otimes y + y \otimes x$.

§50. EXERCISE. The *symmetric algebra* $S(V)$ of a vector space V over a field F is defined to be the quotient of $T_F(V)$ by the ideal generated by all the differences $x \otimes y - y \otimes x$ with $x, y \in V$.

1. Prove that $S(V)$ is a commutative algebra.
2. Writing $\eta : V \rightarrow S(V)$ for the natural injection of generators, prove that any F -linear map $f : V \rightarrow A$ to a commutative F -algebra A factors uniquely through η .
3. If B is a basis of V , prove that $S(V) \cong F[B]$, where $F[B]$ is the polynomial F -algebra of polynomials written using the basis vectors as indeterminates.

3.2 The universal enveloping algebra of a Lie algebra

By a Lie algebra over a field F is meant a vector space L over F equipped with an operation

$$[-, -] : L \times L \rightarrow L,$$

called the *bracket*, which has the following properties:

1. It is bilinear,

2. $[x, x] = 0$ for all $x \in L$,
3. $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ for all $x, y, z \in L$ (Jacobi identity).

A homomorphism $f : L \rightarrow M$ of Lie algebras is a linear map that preserves the bracket:

$$f([x, y]) = [f(x), f(y)].$$

The category of Lie algebras over F is denoted by $LieAlg_F$.

§51. EXERCISE. Prove anticommutativity in any Lie algebra: $[x, y] = -[y, x]$. Prove that 2 above can be replaced by anticommutativity if $\text{char } F \neq 2$.

§52. EXAMPLE. Any F -vector space is a Lie algebra with bracket defined by $[x, y] = 0$ for all $x, y \in V$. Such Lie algebras are called *abelian*.

§53. EXAMPLE. Any F -algebra is a Lie algebra over F with the bracket defined by $[x, y] = xy - yx$. This assignment extends to a functor $L : F\text{-Alg} \rightarrow LieAlg_F$.

§54. EXAMPLE. Given an F -vector space V , the *general linear Lie algebra* $\mathfrak{gl}(V)$ is the Lie algebra obtained as above from the F -algebra $\text{End}_F(V)$. Hence, the bracket is the commutator

$$[f, g] = fg - gf,$$

where as usual the product fg is composition $f \circ g$.

§55. UNIVERSAL ENVELOPING ALGEBRAS. Let L be a Lie algebra. The *universal enveloping Lie algebra* of L is the quotient $U(L) := T_F(L)/I$ where the ideal I is generated by the relations $[x, y] = xy - yx$. Or, being fussy with the definition of the tensor algebra, the relations are $[x, y] = x \otimes y - y \otimes x$, which means we are identifying the element $[x, y] \in L$ with $x \otimes y - y \otimes x \in L^{\otimes 2}$.

§56. EXERCISE. Given a Lie algebra L and an F -algebra A , prove that the homomorphisms of Lie algebras $f : L \rightarrow L(A)$ are in a bijective correspondence with the homomorphisms of F -algebras $f^\# : U(L) \rightarrow A$. More precisely, establish an adjunction between $LieAlg_F$ and $F\text{-Alg}$.

§57. **REMARK.** Contrary to tensor algebras, it is no longer obvious that the injection of generators $L \rightarrow U(L)$ is injective. Indeed it is, so L can be regarded as being a Lie subalgebra of its universal enveloping algebra, but this is a consequence of the PBW Theorem (for Poincaré–Birkhoff–Witt), whose proof is nontrivial and lies beyond the scope of these notes.

3.3 Derivations

§58. **DEFINITION.** By a *not necessarily associative* R -algebra is meant an R -module A equipped with an R -bilinear operation $- \bullet - : A \times A \rightarrow A$; or, equivalently, with a homomorphism of R -modules $A \otimes_R A \rightarrow A$.

§59. **EXAMPLES.** Associative algebras, with $a \bullet b = ab$, and Lie algebras, with $a \bullet b = [a, b]$ (the later with R a field, although one can equally define Lie algebras over more general commutative rings).

§60. **DEFINITION.** Let A be a not necessarily associative F -algebra for a field F . By a *derivation* on A is meant a homomorphism of R -modules $D : A \rightarrow A$ such that for all $a, b \in A$ the Leibniz rule is satisfied:

$$D(ab) = D(a)b + aD(b).$$

We write $\text{Der}(A)$ for the set of derivations of A .

§61. **EXAMPLE.** The usual derivative of a smooth map $f : \mathbb{R} \rightarrow \mathbb{R}$ is a derivation $\frac{d}{dx} : C^\infty(\mathbb{R}) \rightarrow C^\infty(\mathbb{R})$, where the multiplication in $C^\infty(\mathbb{R})$ is pointwise multiplication of smooth functions.

§62. **EXERCISE.** Prove that $\text{Der}(A)$ is a Lie subalgebra of $\mathfrak{gl}(A)$. But show that the product fg of two derivations might not be a derivation.

§63. **REMARK.** So we see that derivations of associative algebras, but also derivations of Lie algebras, form Lie algebras.

Test 3 (MAP30)

Lecture 4. Irreducible representations

4.1 Representations of algebras

Recall that a (finite degree) representation of an F -algebra A (for a field F) was defined to be a homomorphism of F -algebras

$$\rho : A \rightarrow M_n(F).$$

Since $M_n(F) \cong \text{End}_F(V)$ for any n -dimensional vector space V over F , we are led to the notion of a general representation of an R -algebra A on an R -module V , for any unital ring R :

§64. DEFINITION. By a *representation* of an R -algebra A (unital or non-unital) on an R -module V is meant a homomorphism (unital if A is unital) of R -algebras

$$\rho : A \rightarrow \text{End}_R(V).$$

§65. PROPOSITION.

1. A representation $\rho : A \rightarrow \text{End}_R(V)$ is “the same” as a structure of A -module on V (unital if A is unital) which is compatible with the R -module structures of both A and V in the sense given by the law

$$r(av) = (ra)v = a(rv)$$

for all $a \in A$, $r \in R$ and $v \in V$.

2. Moreover, in the unital case, this compatibility of the actions is equivalent to imposing that the action of R on V is given by

$$rv = \iota(r)v,$$

where $\iota : R \rightarrow A$ is the injection of scalars of A .

Proof. Let $\rho : A \rightarrow \text{End}_R(V)$, and consider the A -module structure defined by $av = \rho(a)(v)$. Let also $r \in R$. Then

$$a(rv) = \rho(a)(rv) = r\rho(a)(v) = r(av)$$

because $\rho(a)$ is a homomorphism of R -modules, and

$$(ra)v = \rho(ra)(v) = (r\rho(a))(v) = r(\rho(a)(v)) = r(av)$$

because ρ is also a homomorphism of R -modules (because it is one of R -algebras) and the action on the R -endomorphisms of V is defined pointwise.

Conversely, given an action of A on V satisfying the law $r(av) = (ra)v = a(rv)$, and letting $\rho : A \rightarrow \text{End}_{\mathbb{Z}}(V)$ be its representation by endomorphisms of abelian groups on V , essentially reversing the above argument we conclude that ρ is a homomorphism of R -modules (that's the condition $r(av) = (ra)v$), and that $\rho(a)$ is an R -module endomorphism (that's the condition $r(av) = a(rv)$).

Finally, in the unital case, if the two equivalent conditions hold we conclude that

$$rv = r(1_A v) = (r1_A)v = \iota(r)v,$$

and, conversely, if $rv = \iota(r)v$ we conclude that

$$(ra)v = (\iota(r)a)v = (a\iota(r))v = a(\iota(r)v) = a(rv)$$

and

$$(ra)v = (\iota(r)a)v = \iota(r)(av) = r(av). \blacksquare$$

§66. REMARK. This proposition justifies, for a **unital** R -algebra A , that we define a representation of A to be simply a left A -module — where V also becomes an R -module by change of base ring along $\iota : R \rightarrow A$. From here on we shall adopt this point of view, for simplicity, and often we will use the words “representation” and “module” interchangeably.

In addition, still in the unital case, the *category of representations* of A is defined to be $A\text{-Mod}$, a *subrepresentation* is defined to be a submodule, and an *intertwiner map* between two representations of A is just a homomorphism of the corresponding A -modules.

§67. EXAMPLES.

1. The category of representations of a Lie algebra L can be identified with $U(L)\text{-Mod}$.
2. The category of representations of a group G over a field F can be identified with $FG\text{-Mod}$.

§68. EXERCISE. Let G be a group. By a G -module over a field F is meant a vector space V over F together with an action of G on V which is *linear*; that is, such that for all $g \in G$, $\lambda \in F$ and $v, w \in V$ we have $g(\lambda v + w) = \lambda gv + gw$. Verify that this is the same as a representation $\rho : G \rightarrow GL(V)$.

4.2 Irreducible representations and Schur's Lemma

Now we introduce the very important notion of irreducible representation, and of indecomposable representation. From here on we will typically use the language of module theory, so that in general we denote rings by the letter A , assuming they are unital, and what we will say applies equally well to R -algebras A .

§69. DEFINITION. Let A be a ring and let V be a nonzero A -module.

1. The module V is *irreducible* (or *simple*) if its only submodules are 0 and V .
2. The module V is *decomposable* if it can be written as $V_1 \oplus V_2$ for two nonzero submodules of V ; otherwise it is *indecomposable*.

§70. REMARK. Clearly, any simple module is indecomposable. Give an example of an indecomposable module that is not simple.

§71. SCHUR'S LEMMA. *Let F be a commutative ring and A a nonzero F -algebra.*

1. *Any nonzero homomorphism $\varphi : V \rightarrow W$ of simple A -modules is an isomorphism.*
2. *If V is a simple A -module, then $\text{End}_A(V)$ is a division ring.*
3. *If V is a simple A -module and F is an algebraically closed field, and $\dim_F(V) < \infty$, then $\text{End}_A(V) \cong F$.*

Proof. If $\varphi : V \rightarrow W$ is nonzero then $\varphi(V)$ is a nonzero submodule of W , hence it must be W itself. Then $\ker \varphi$ cannot be the whole of V , and thus it must be $\{0\}$, so φ is an isomorphism. Therefore any nonzero $\varphi \in \text{End}_A(V)$ is invertible, so $\text{End}_A(V)$ is a division ring.

For the third part of the lemma, let us first solve the following exercise:

§72. EXERCISE. Let A be an F -algebra for some field F , and let V be a left A -module. Prove that if $T \in \text{End}_A(V)$ and $\lambda \in F$ is any eigenvalue of T (T is an F -linear map) then the eigenspace E_λ of λ is a nonzero left A -submodule.

Resolution. Let $x \in E_\lambda$ and $a \in A$. Then $T(ax) = aT(x) = a\lambda x = \lambda ax$, so $ax \in E_\lambda$. This shows that E_λ is a left A -submodule of V , and E_λ is nonzero by definition of eigenspace (it must contain an eigenvector, which by definition has to be a nonzero vector).

Now let us continue the proof of the third part of Schur's Lemma. Let $T : V \rightarrow V$ be a homomorphism of left A -modules. In particular, T is an F -linear map, so it has an eigenvalue λ because F is algebraically closed (and $\dim_F(V)$ is both finite and nonzero). By the exercise, the eigenspace E_λ is a nonzero A -submodule of V , so it coincides with V because V is simple. Hence, $T(x) = \lambda x$ for all $x \in V$. This establishes the envisaged bijective correspondence between F and $\text{End}_A(V)$, which moreover is: clearly a homomorphism of abelian groups; clearly unital; and it preserves multiplication, for if $T_1(x) = \lambda_1 x$ and $T_2(x) = \lambda_2 x$ for all $x \in V$ then $T_1 \circ T_2(x) = \lambda_1(\lambda_2 x) = (\lambda_1 \lambda_2)x$. ■

Lecture 5 (double). Semisimple modules and rings

5.1 Complement on simple modules

§73. DEFINITION. Let A be a ring. A left ideal of A which is simple as a left A -module is said to be *minimal*.

§74. LEMMA. Let L be a minimal left ideal of a ring A , and let V be a simple left A -module. If L and V are not isomorphic as left A -modules we have $LV = \{0\}$ (i.e., $L \subset \text{Ann}(V)$).

Proof. Let $v \in V$. Define $\phi : L \rightarrow V$ by for all $a \in L$

$$\phi(a) = av.$$

This is a left module homomorphism and, by Schur's lemma, it is nonzero if and only if it is an isomorphism. Therefore, if L and V are not isomorphic ϕ must be zero, and it follows that $Lv = \phi(L) = \{0\}$ for all $v \in V$, so $LV = \{0\}$. ■

5.2 Semisimple modules

§75. DEFINITION. Let A be a ring and let V be a nonzero A -module.

1. The module V is *completely reducible* (or *semisimple*) if it is a direct sum of irreducible submodules.
2. If V is a completely reducible module, any direct summand of V is called a *constituent* of V .

§76. LEMMA. Let A be a ring, V a semisimple A -module, and $\varphi : V \rightarrow W$ a surjective homomorphism of A -modules. Then W is semisimple and φ is a retraction.

Proof. Let $V = \bigoplus_{i \in I} V_i$ with each V_i irreducible. Then W is the sum of the images of the submodules $V_i \subset V$:

$$W = \sum_{i \in I} \varphi(V_i).$$

Since V_i is irreducible, the image $\varphi(V_i)$ is either 0 or isomorphic to V_i , hence itself a simple module. This shows that W is the sum of isomorphic copies of some of the constituents of V . Then for each $i, j \in I$ we must either have $\varphi(V_i) = \varphi(V_j)$ or $\varphi(V_i) \cap \varphi(V_j) = \{0\}$ due to irreducibility of the images, so W is a direct sum of isomorphic copies of some of the constituents of V . This shows both that W is semisimple and that it is a direct summand of V , so φ splits. ■

§77. NOTE. In other words, a quotient of a completely reducible module is a projection onto the direct sum of a subset of the set of constituents.

5.3 Semisimple rings

§78. DEFINITION. By a *semisimple* ring will be meant a ring A which is semisimple as an A -module; that is, A is a direct sum of minimal left ideals.

§79. THEOREM. Let A be a ring. The following conditions are equivalent.

1. Every A -module is injective (equivalently, every A -module is projective).
2. Every A -module is semisimple.

3. A is semisimple.

4. A is a direct sum of finitely many minimal left ideals.

Proof. (1) \Rightarrow (2). Assume that every A -module is injective, and let M be an A -module. Write $\text{Soc}(M)$ (this is called the *socle* of M) for the sum of all the minimal submodules of M (the simple submodules). Evidently, $\text{Soc}(M)$ is a semisimple module because it is a (necessarily direct) sum of simple modules. Since we are assuming that every module is injective, the inclusion of $\text{Soc}(M)$ into M splits, so there is a submodule $N \subset M$ such that $M = \text{Soc}(M) \oplus N$, and all we need to do is prove that $N = 0$.

Let us proceed by assuming that there is an element $n \in N \setminus \{0\}$ and obtain a contradiction. Any chain of submodules $N' \subset N$ such that $n \notin N'$ has a supremum (their union) which also does not contain n , so by Zorn's lemma there is a maximal submodule $L \subset N$ that does not contain n , and thus $L + An$ is the least submodule of N that contains both L and n . Hence, by the fourth isomorphism theorem for modules, in the quotient N/L the submodule $A(n+L)$ is simple. But all the modules are projective, so there is a decomposition $N = N_1 \oplus N_2$ such that $N_1 \cong N/L$, and thus $M = \text{Soc}(M) \oplus N_1 \oplus N_2$, which is a contradiction because N_1 has a simple submodule but $\text{Soc}(M)$ is supposed to contain all the simple submodules of M .

(2) \Rightarrow (3). Immediate.

(3) \Rightarrow (4). Suppose that A , regarded as an A -module, is completely reducible, and let $(J_i)_{i \in I}$ be a family of minimal left ideals of A such that $A = \bigoplus_{i \in I} J_i$. Then there exists a finite subset $F \subset I$ such that $1 \in \bigoplus_{j \in F} J_j$, so for every element $a \in A$ we have

$$a = a1 \in \bigoplus_{j \in F} J_j.$$

(4) \Rightarrow (1). If A is a direct sum of minimal left ideals, any free A -module is completely reducible because it is a direct sum of copies of A . Hence, since any A -module N is a quotient of a free module, it is a direct summand of a free module due to §76. This shows that every A -module is projective. ■

§80. REMARK. Semisimple rings are often called *semisimple Artinian rings*, as in [1], or *semisimple rings with minimum condition*, as in [2], because some authors use a definition of semisimple ring which is weaker than the one given in these notes.

§81. COROLLARY. Let A be a semisimple ring, and M a simple left A -module. Then $M \cong J$ for some minimal left ideal J of A .

Proof. The argument for proving (1) \Rightarrow (2) in §79 is that any left A -module is a direct sum of isomorphic copies of minimal left ideals of A , so if M is a simple module it must be isomorphic to a minimal left ideal. ■

5.4 Example: Maschke's Theorem

§82. MASCHKE'S THEOREM (18.1.1 OF [2]). *Let G be a finite group and F a field whose characteristic does not divide $|G|$. Then the group algebra FG is semisimple.*

Proof. We will show that every FG -module is injective, which is equivalent to showing that every injective homomorphism $\psi : U \rightarrow V$ of FG -modules splits. Equivalently, we show that any submodule $U \subset V$ has a direct complement, $V = U \oplus W$, which in turn is equivalent to the existence of a homomorphism of FG -modules $\pi : V \rightarrow U$ such that $\pi(u) = u$ for all $u \in U$.

First, since U is an F -linear subspace of V , there is an F -linear subspace $W_0 \subset V$ such that $V = U \oplus W_0$, and we define $\pi_0 : V \rightarrow U$ to be the corresponding projection to U . This is not necessarily the splitting we are looking for because W_0 is not necessarily a G -invariant subspace (i.e., an FG -submodule), so, equivalently, π_0 is not necessarily G -equivariant.

In order to obtain the required splitting let us begin, for each $g \in G$, by defining another map $g\pi_0g^{-1} : V \rightarrow U$: for all $v \in V$ define

$$g\pi_0g^{-1}(v) = g\pi_0(g^{-1}v).$$

Since π_0 is F -linear and both g and g^{-1} act by linear transformations, the map $g\pi_0g^{-1}$ is F -linear. Also, for each $u \in U$ we have, since U is G -invariant,

$$g\pi_0g^{-1}(u) = g\pi_0(g^{-1}u) = gg^{-1}u = u,$$

so $g\pi_0g^{-1}$ is an F -linear retraction.

Now let $n = |G|$, and let us regard n as an element of F by defining $n = 1 + \cdots + 1$ (n times). By hypothesis, $n \neq 0$ in F because the characteristic of F does not divide $|G|$. So n has an inverse n^{-1} , which we denote by $\frac{1}{n}$. Then define $\pi : V \rightarrow U$ to be the "average" of all the maps $g\pi_0g^{-1}$ over G :

$$\pi = \frac{1}{n} \sum_{g \in G} g\pi_0g^{-1}.$$

This is a sum of F -linear maps multiplied by a scalar, so it is an F -linear map. It is also a retraction onto U because for all $u \in U$ we have

$$\pi(u) = \frac{1}{n} \sum_{g \in G} g\pi_0g^{-1}(u) = \frac{1}{n} \sum_{g \in G} u = \frac{1}{n}(nu) = u.$$

Finally, let us prove that π is G -equivariant. Let $h \in G$ and $v \in V$.

$$\begin{aligned}
 \pi(hv) &= \frac{1}{n} \sum_{g \in G} g\pi_0(g^{-1}hv) \\
 &= \frac{1}{n} \sum_{g \in G} hh^{-1}g\pi_0(g^{-1}hv) \\
 &= \frac{1}{n} \sum_{g \in G, k=h^{-1}g} hk\pi_0(k^{-1}v) \\
 &= \frac{1}{n} \sum_{g \in G} hg\pi_0(g^{-1}v) \\
 &= h \frac{1}{n} \sum_{g \in G} g\pi_0(g^{-1}v) = h\pi(v).
 \end{aligned}$$

Notice that in the above derivation k ranges over all the elements of G when g does, which justifies why we could replace k by g (h is fixed). ■

§83. COROLLARY. *The complex group algebra $\mathbb{C}G$ is a semisimple ring for any finite group G .*

Lecture 6 (double). Simple rings

6.1 Complements from previous lecture

In all the previous material about semi-simple modules and algebras we have assumed that the algebras are unital. Even earlier, when studying projective modules we have made use of the fact that $\text{hom}_R(R, M) \cong M$ for any R -module M , which assumes that R has a unit. Similarly, in studying the four equivalent definitions of semisimple ring in the previous lecture, we have used the definition of free module for unital rings.

This does not mean that representation theory falls apart for nonunital algebras, but simply that some care must be taken. For instance, it is no longer true that a representation $\rho : A \rightarrow \text{End}_R(V)$ is the same thing as an A -module V , although it is true provided we add the conditions $r(av) = (ra)v = a(rv)$, as we have seen. Alternatively, such a representation can be regarded as a module, but over another algebra, known as the *unitization* of A . This type of trick is often used in the context of operator algebras, such as C^* -algebras.

§84. EXERCISE. Let A be a nonunital R -algebra, for a commutative ring R with unit.

1. Prove that the direct sum $A_1 := A \oplus R$ is a unital R -algebra with unit $(0, 1)$, with product defined by

$$(a, r)(b, s) = (ab + rb + sa, rs),$$

and injection of scalars defined by $\iota_2 : R \rightarrow A \oplus R$.

2. Prove that A_1 has the following universal property: for all unital R -algebras B and all homomorphisms of (nonunital) R -algebras $f : A \rightarrow B$ there is a unique homomorphism of unital R -algebras $f^\# : A_1 \rightarrow B$ that makes the following diagram commute, where ι is the first injection $A \rightarrow A \oplus R$:

$$\begin{array}{ccc} A & \xrightarrow{\iota_1} & A_1 \\ & \searrow f & \downarrow f^\# \\ & & B \end{array}$$

3. Prove that any A_1 -module V is the same thing as a (nonunital) representation $\rho : A \rightarrow \text{End}_R(V)$ in which V has the R -module structure given by restricting the A_1 action to R .

6.2 Structure of simple rings

§85. DEFINITION. A nonzero ring A is *simple* if it is semisimple and all its minimal left ideals are isomorphic as left A -modules.

§86. COROLLARY. *Any two simple modules over a simple ring A are isomorphic, and they are isomorphic to the minimal left ideals of A .*

Proof. Immediate from §81. ■

§87. EXAMPLE. Let Δ be a division ring, and $A = M_n(\Delta)$. Regard Δ^n as the set of column $n \times 1$ matrices with entries in Δ . Then Δ^n is a left A -module under matrix multiplication, and clearly it is simple. Now note that we have $A = J_1 \oplus \cdots \oplus J_n$ where for each $j = 1, \dots, n$ the left ideal J_j

is that of all the matrices whose entries outside the j -column are zero:

$$J_j = \left\{ \underbrace{\begin{pmatrix} 0 & \cdots & 0 & a_{1j} & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & a_{nj} & 0 & \cdots & 0 \end{pmatrix}}_{n \text{ columns}} \mid a_{ij} \in \Delta \right\}.$$

Then each J_j is isomorphic to Δ^n as a left A -module, so we see that A is a simple ring. Moreover, by §86, every simple A -module is isomorphic to Δ^n . Theorem §94 below will show that every simple ring is of this form up to isomorphism.

§88. THEOREM. *Let A be a simple ring.*

1. *For any minimal left ideals L and M there is $m \in M$ which yields an isomorphism $\varphi : L \rightarrow M$ by $\varphi(b) = bm$ for all $b \in L$. Hence, $Lm = M$.*
2. *$LA = A$.*
3. *A has no two-sided ideals except $\{0\}$ and A .*

Proof. Let L and M be minimal left ideals, and consider the retraction of left A -modules $\pi : A \rightarrow L$ (recall that L is a direct summand of A , so π is the projection). Let $\varphi : L \rightarrow M$ be an isomorphism, and let $m = \varphi(\pi(1))$. Then for all $b \in L$ we have

$$\varphi(b) = \varphi(\pi(b)) = \varphi(\pi(b1)) = b\varphi(\pi(1)) = bm.$$

Since $\varphi \circ \pi : A \rightarrow M$ is surjective, we obtain $Lm = M$. This proves (1), and (2) is an immediate consequence.

Finally, let $I \subset A$ be a two-sided ideal. This is a sum of minimal left ideals, so if $I \neq \{0\}$ we must have $IA = A$ due to (2). This proves (3). ■

§89. REMARK. So we see that simple rings share with simple modules the property that they have only two types of quotients: any epimorphism whose domain is a simple ring is either a zero homomorphism or an isomorphism.

§90. NOTATION. If A is a ring, we denote by A^{op} the ring which coincides with A as an abelian group and whose multiplication is that of A with the order reversed; that is, denoting by $x; y$ the product of x and y in A^{op} , we have $x; y = yx$.

§91. LEMMA. *Let A be a ring. Then $A^{\text{op}} \cong \text{End}_A(A)$.*

Proof. Recall the isomorphism of abelian groups $f : A \rightarrow \text{End}_A(A)$ which to each $a \in A$ assigns the unique left A -module homomorphism $f_a : A \rightarrow A$ such that $f_a(1) = a$; that is, $f_a(x) = xa$ for all $x \in A$. Then, writing $a; b$ for the product ba , we obtain

$$f_{a;b}(x) = f_{ba}(x) = xba = (xb)a = f_a(f_b(x)),$$

so we see that $f_{a;b} = f_a \circ f_b$. Therefore, f defines an (evidently unital) isomorphism of rings $f : A^{\text{op}} \rightarrow \text{End}_A(A)$. ■

§92. REMARK. Note that $A = A^{\text{op}}$ if and only if A is commutative, but there may exist isomorphisms $A \cong A^{\text{op}}$ for noncommutative rings. For instance, this happens for any *involutive* ring, by which is meant a ring A equipped with an operation $a \mapsto a^*$ that for all $a, b \in A$ satisfies $(a + b)^* = a^* + b^*$, $a^{**} = a$, and $(ab)^* = b^*a^*$. Then the mapping $a \mapsto a^*$ defines an isomorphism of rings $A \cong A^{\text{op}}$ which moreover is unital because necessarily $1^* = 1$. (Exercise: prove this.)

An example of involutive ring is the ring of square matrices $M_n(F)$ for some field F , since the operation of matrix transposition is an involution (check). Hence, $M_n(F)^{\text{op}} \cong M_n(F)$. If $F = \mathbb{C}$, another involution is the operation that to each matrix assigns its adjoint.

§93. LEMMA. *Let Δ be a division ring, and $n \in \mathbb{N}$. Then*

$$M_n(\Delta^{\text{op}}) \cong M_n(\Delta)^{\text{op}}.$$

Proof. The idea is to apply matrix transposition as in §92, but taking into account that the matrices do not necessarily have entries in a commutative ring. Let $A, B \in M_n(\Delta^{\text{op}})$, and write $T : M_n(\Delta^{\text{op}}) \rightarrow M_n(\Delta)^{\text{op}}$ for the map that assigns each matrix $A \in M_n(\Delta^{\text{op}})$ to its transpose A^t , but whose entries are now regarded as being in Δ rather than Δ^{op} . Then we have for all $i, j = 1, \dots, n$

$$\begin{aligned} T(AB)_{ij} &= (AB)_{ji} = \sum_{k=1}^n a_{jk} b_{ki} = \sum_{k=1}^n b_{ki} a_{jk} = \sum_{k=1}^n T(B)_{ik} T(A)_{kj} \\ &= (T(B)T(A))_{ij} = (T(A); T(B))_{ij}, \end{aligned}$$

so we see that matrix transposition defines a homomorphism of rings

$$T : M_n(\Delta^{\text{op}}) \rightarrow M_n(\Delta)^{\text{op}}.$$

This is evidently unital, and it is an isomorphism whose inverse is again given by matrix transposition. ■

§94. THEOREM. *Let A be a ring. The following conditions are equivalent:*

1. *A is a simple ring.*
2. *There is a division ring Δ such that $A \cong M_n(\Delta)$ as rings.*

Proof. The implication (2) \Rightarrow (1) is easy and has been described in §87, so let us prove the implication (1) \Rightarrow (2). Assume that A is simple, let $A = J_1 \oplus \cdots \oplus J_n$ be the decomposition into minimal left ideals, and write J for J_1 . Recall that $\text{End}_A(J)$ is a division ring, by Schur's lemma. The (external) direct sum

$$M := \underbrace{J \oplus \cdots \oplus J}_{n \text{ times}}$$

is a left A -module isomorphic to A , so $\text{End}_A(A) \cong \text{End}_A(M)$. Let us prove that there is an isomorphism of rings

$$\text{End}_A(M) \cong M_n(\text{End}_A(J)).$$

Each $\varphi \in \text{End}_A(M)$ is a homomorphism

$$\varphi : J \oplus \cdots \oplus J \rightarrow J \oplus \cdots \oplus J.$$

Due to the universal properties of the direct sum both as product and coproduct, φ is determined uniquely by a family $\varphi_{ij} \in \text{End}_A(J)$ where $i, j = 1, \dots, n$. Concretely, φ_{ij} is the homomorphism from the j^{th} copy of J in the domain of φ to the i^{th} copy in the codomain. If $\psi \in \text{End}_A(M)$ and we name components $\psi_{ij} \in \text{End}_A(J)$ similarly, the composition $\psi \circ \varphi$ is the homomorphism whose component $(\psi \circ \varphi)_{ij}$ for each $i, j = 1, \dots, n$ is given by

$$(\psi \circ \varphi)_{ij} = \sum_{k=1}^n \psi_{ik} \circ \varphi_{kj}.$$

In other words, there is a homomorphism of rings that sends each $\varphi \in \text{End}_A(M)$ to the matrix $(\varphi_{ij}) \in M_n(\text{End}_A(J))$, which is unital because the identity homomorphism in $\text{End}_A(M)$ is mapped to the $n \times n$ identity matrix with entries in $\text{End}_A(J)$. So we have concluded that

$$\text{End}_A(A) \cong M_n(\text{End}_A(J)).$$

Hence, defining $\Delta = \text{End}_A(J)^{\text{op}}$, from §91 and §93 we obtain

$$A \cong \text{End}_A(A)^{\text{op}} \cong \text{End}_A(M)^{\text{op}} \cong M_n(\text{End}_A(J))^{\text{op}} \cong M_n(\Delta). \quad \blacksquare$$

§95. THEOREM. Let F be an algebraically closed field, and let A be a finite dimensional F -algebra. The following conditions are equivalent:

1. A is a simple ring.
2. $A \cong M_n(F)$ as F -algebras.

Proof. Adaptation of the proof of §94 by taking into account the isomorphism of rings $\text{End}_A(J) \cong F$ for any simple A -module J , which holds because A is finite dimensional and thus so is J (cf. Schur's Lemma in §71). ■

Lecture 7. Idempotents

§96. DEFINITION. The *center* of a ring A , denoted by $Z(A)$, is the set of elements $a \in A$ such that $ab = ba$ for all $b \in A$.

§97. EXERCISE. Show that $Z(A)$ is a commutative subring of A .

§98. DEFINITION. Let A be a ring.

1. An element e in A is called an *idempotent* if $e^2 = e$.
2. Idempotents e and f are *orthogonal* if $ef = fe = 0$; in particular, orthogonal idempotents commute.
3. A set E of idempotents is *orthogonal* if e and f are orthogonal for all $e \neq f$ in E .
4. A *partition* of an idempotent f is a finite orthogonal set of nonzero idempotents $\{e_1, \dots, e_n\}$ such that $e_1 + \dots + e_n = f$.
5. An idempotent e is *primitive* if it cannot be written as a sum of two nonzero orthogonal idempotents.
6. The idempotent e is a *primitive central idempotent* of A if it is a primitive idempotent of the subring $Z(A)$ (it cannot be written as a sum of nonzero orthogonal idempotents $e, f \in Z(A)$).

§99. EXAMPLE. Let X be a set and A the commutative ring of real valued functions on X . A function $f \in A$ is an idempotent if and only if $f(x)^2 = f(x)$ for all $x \in X$, which means either $f(x) = 0$ or $f(x) = 1$; that is, f is the characteristic function χ_Y of a subset $Y \subset X$. The product of two such functions corresponds to the intersection of subsets, $\chi_Y \chi_Z = \chi_{Y \cap Z}$, and orthogonal projections correspond to disjoint subsets. The ring identity is the function with constant value 1, and a partition of the identity corresponds precisely to a partition of X by nonempty subsets. The primitive idempotents are the characteristic functions of singleton subsets, so they correspond bijectively with the points of X .

§100. EXERCISE. Let A be a ring such that $A = B \oplus C$ (internal direct sum) for two additive subgroups $B, C \subset A$ such that $b^2 \in B$ for all $b \in B$ and $c^2 \in C$ for all $c \in C$ (for instance, B and C could be subrings). Show that the components of 1 in B and C are orthogonal idempotents.

Resolution. Let f and g be the elements of B and C , respectively, such that $1 = f + g$. Then

$$g^2 = (1 - f)^2 = 1 - f - f + f^2 = g - f + f^2,$$

so

$$g^2 - g = f^2 - f.$$

But $f^2 - f \in B$ and $g^2 - g \in C$, so $f^2 - f = g^2 - g = 0$. This shows that both f and g are idempotents. Then

$$fg = f(1 - f) = f - f^2 = f - f = 0 \quad \text{and} \quad gf = (1 - f)f = f - f^2 = 0.$$

So $\{f, g\}$ is a partition of 1. ■

§101. EXERCISE. Let $e \in A$ be an idempotent such that the cyclic left module Ae equals a direct sum of left submodules $J \oplus K$. Show that the components of e in J and K are orthogonal idempotents.

Resolution. Let f and g be the unique elements of J and K , respectively, such that $e = f + g$. Then $f \in J \oplus K = Ae$, so f equals ae for some $a \in A$, and thus $fe = ae^2 = ae = f$. Therefore

$$f = fe = f(f + g) = f^2 + fg.$$

But $f^2 \in J$ and $fg \in K$, so these are the components of f in the direct sum; that is, $f = f^2$ and $fg = 0$. Similarly we prove that $g^2 = g$ and $gf = 0$ by letting $g = be$ for some $b \in A$, and computing

$$g = be = be^2 = ge = g(f + g) = gf + g^2,$$

where $gf \in J$ and $g^2 \in K$. Hence, f and g are orthogonal idempotents. ■

§102. EXERCISE. Let A be a ring, and let $\{e_1, \dots, e_n\}$ be a partition of 1. Prove that A is a direct sum of left ideals

$$A = J_1 \oplus \cdots \oplus J_n$$

where $J_i = Ae_i$ for each $i = 1, \dots, n$.

§103. EXERCISE. Prove the converse of the previous exercise: any decomposition of A as a direct sum of left ideals $J_1 \oplus \cdots \oplus J_n$ arises as in the previous exercise from a partition of 1.

§104. EXERCISE. Let Δ be a division ring, let $n \in \mathbb{N}$, let $A = M_n(\Delta)$, and let I be the identity matrix (the 1 of A). Prove the following assertions:

1. $Z(A) = \{\alpha I \mid \alpha \in Z(\Delta)\}$, and $Z(A)$ is a field isomorphic to $Z(\Delta)$ (so if Δ is a field we have $Z(A) \cong \Delta$).
2. The only central idempotent in A is I (in particular, I is a primitive central idempotent).

Lecture 8 (double). Structure of semisimple rings

8.1 Conclusion of the previous lecture

Exercises 102–104.

8.2 Artin–Wedderburn theorem

Let A be a semisimple ring. For each isomorphism class $i = \{J_1, \dots, J_s\}$ (as left A -modules) of minimal left ideals of A , we can form its sum $A_i =$

$J_1 + \cdots + J_s = J_1 \oplus \cdots \oplus J_s$, and thus obtain a decomposition of A by left ideals

$$A = A_1 \oplus \cdots \oplus A_r$$

where r is the number of isomorphism classes of minimal left ideals of A and any two minimal left ideals of A are isomorphic as left modules if and only if they are contained in the same component A_i .

§105. DEFINITION. Using the above notation, each component A_i of a semisimple ring A will be called a *Wedderburn component* of A , and the direct decomposition $A_1 \oplus \cdots \oplus A_r$ is the *Wedderburn decomposition* of A .

§106. REMARK. A simple ring is the same as a semisimple ring which has exactly one Wedderburn component.

§107. THEOREM. *Let A be a semisimple ring, and let $A = A_1 \oplus \cdots \oplus A_r$ be its Wedderburn decomposition. Then*

1. A_i is a two-sided ideal of A for all $i = 1, \dots, r$,
2. There is a unique partition of 1 by central idempotents z_1, \dots, z_r in A such that each $A_i = z_i A$ for all $i = 1, \dots, r$,
3. A_i is a simple ring with unit z_i , for all $i = 1, \dots, r$,
4. A is isomorphic to the direct product of simple rings $A_1 \times \cdots \times A_r$.

Proof. Let us prove (1). Each A_i is a left ideal, so let us prove that it is also a right ideal. Let $a \in A$ and $m \in A_i$. Let $a = a_1 + \cdots + a_r$ be the decomposition of a over the Wedderburn components of A ; that is, $a_j \in A_j$ for each $j = 1, \dots, r$. Then

$$ma = ma_1 + \cdots + ma_r,$$

and thus $ma_j \in A_j$ for all $j = 1, \dots, r$. Let $j \neq i$, and consider the direct decompositions of A_i and A_j into minimal left submodules:

$$\begin{aligned} A_i &= J_1 \oplus \cdots \oplus J_s, \\ A_j &= K_1 \oplus \cdots \oplus K_t. \end{aligned}$$

Then $m = m_1 + \cdots + m_s$ for unique components $m_k \in J_k$, and $a_j = b_1 + \cdots + b_t$ for unique components $b_l \in K_l$, so

$$ma_j = \sum_{k=1}^s \sum_{l=1}^t m_k b_l,$$

and $m_k b_l \in K_l$ for each k and l . But $j \neq i$ implies that J_k and K_l are not isomorphic, and thus by §74 we must have $m_k b_l = 0$. Hence, for all $j \neq i$ we have $ma_j = 0$, and thus $ma \in A_i$, showing that A_i is a two-sided ideal.

Let us prove (2). Recall from §102 and §103 that there is a unique partition $1 = z_1 + \cdots + z_r$ such that $A_i = Az_i$ for each $i = 1, \dots, r$. But the A_i 's are also right ideals, and by the same reasoning of §102 and §103 the partition of 1 over the direct decomposition is also such that $A_i = z_i A$ for all $i = 1, \dots, r$, and thus $z_i a = a$ for all $a \in A_i$. Since for $j \neq i$ and $a \in A_j$ we must have $az_i = z_i a = 0$, it follows that each z_i is a central idempotent.

Let us prove (3). Being an ideal, each A_i is also a subring. The condition $A_i = Az_i$ shows that for all $a \in A_i$ we have $az_i = a$ because there must be $b \in A_i$ such that $a = bz_i$, and thus $az_i = bz_i^2 = bz_i = a$. Similarly, the condition $A_i = z_i A$ shows that for all $a \in A_i$ we have $z_i a = a$, so A_i is a ring with unit z_i . Since, by construction, all the minimal left submodules of A_i are isomorphic, we conclude that A_i is a simple ring.

Finally, let us prove (4). Let $a, b \in A$, and write

$$a = a_1 + \cdots + a_r \quad \text{and} \quad b = b_1 + \cdots + b_r$$

for the unique decompositions into Wedderburn components. Since, as we have seen, $a_i b_j = 0$ for all $i \neq j$, it follows that

$$ab = a_1 b_1 + \cdots + a_r b_r.$$

Therefore A is isomorphic to the direct product of rings $A_1 \times \cdots \times A_r$. ■

§108. COROLLARY (ARTIN–WEDDERBURN THEOREM). *Let A be a ring. The following conditions are equivalent:*

1. A is semisimple.
2. $A \cong M_{n_1}(\Delta_1) \times \cdots \times M_{n_r}(\Delta_r)$ for some choice of integers $n_i \in \mathbb{N}$ and division rings Δ_i , $i = 1, \dots, r$.

Moreover, the numbers n_i are unique, and the division rings Δ_i are unique up to isomorphism (up to permutations of factors in the Wedderburn decomposition of A).

§109. COROLLARY (SPECIAL ARTIN–WEDDERBURN THEOREM). *Let F be an algebraically closed field, and A be a finite dimensional F -algebra. The following conditions are equivalent:*

1. A is a semisimple ring.
2. $A \cong M_{n_1}(F) \times \cdots \times M_{n_r}(F)$ for a unique choice of integers $n_i \in \mathbb{N}$.

§110. EXERCISE. Give an example of a finite dimensional \mathbb{C} -algebra which is not semisimple.

8.3 More on group algebras

From the Special Artin–Wedderburn Theorem (§109) and Maschke’s theorem (§82) we immediately obtain:

§111. COROLLARY. *Let G be a finite group. Then*

$$\mathbb{C}G \cong M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C})$$

for a unique choice of $r, n_1, \dots, n_r \in \mathbb{N}$.

Note that $\mathbb{C}G$ is a complex vector space of dimension $|G|$, but each Wedderburn component $M_{n_i}(\mathbb{C})$ has dimension n_i^2 , and thus

$$|G| = n_1^2 + \cdots + n_r^2.$$

Also, $Z(\mathbb{C}G)$ has dimension r . The latter is easy to see because the center of each Wedderburn component $M_{n_i}(\mathbb{C})$ is isomorphic to \mathbb{C} , and thus the center of $\mathbb{C}G$ is isomorphic to \mathbb{C}^r . In terms of block diagonal matrices, $\mathbb{C}G$ is isomorphic to the ring of complex block diagonal matrices

$$\begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ & & \ddots & \\ 0 & 0 & \cdots & A_r \end{pmatrix}$$

where for each $k = 1, \dots, r$ the matrix A_k is of dimension $n_k \times n_k$, and $Z(\mathbb{C}G)$ is isomorphic to the subring of $\mathbb{C}G$ such that, for each $k = 1, \dots, r$, the matrix A_k is a scalar matrix $\lambda_k I_k$ with $\lambda_k \in \mathbb{C}$, where I_k is the $n_k \times n_k$ identity matrix.

§112. THEOREM. *Let G be a finite group whose complex group algebra is*

$$\mathbb{C}G \cong M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C}).$$

Then r (the number of Wedderburn components of $\mathbb{C}G$) equals the number of conjugacy classes of G .

Proof. Let $\mathcal{K}_1, \dots, \mathcal{K}_s$ be the distinct conjugacy classes of G . For each i let

$$X_i = \sum_{g \in \mathcal{K}_i} g \in \mathbb{C}G.$$

Note that the set $\{X_1, \dots, X_s\}$ is linearly independent. Moreover, the condition $h^{-1}\mathcal{K}_i h = \mathcal{K}_i$ implies that $h^{-1}X_i h = X_i$ for all $i = 1, \dots, s$, so $X_i \in Z(\mathbb{C}G)$. In order to conclude that $r = s$ we only need to prove that the X_i 's span $Z(\mathbb{C}G)$. Let then $X = \sum_{g \in G} \alpha_g g$ be an arbitrary element of $Z(\mathbb{C}G)$, for coefficients $\alpha_g \in \mathbb{C}$. Centrality implies that $h^{-1}Xh = X$ for all $h \in G$, so

$$\sum_{g \in G} \alpha_g h^{-1}gh = \sum_{g \in G} \alpha_g g.$$

But as g ranges over G so does $h^{-1}gh$, and the coefficient of g in the left hand side summation is $\alpha_{hgh^{-1}}$, so we conclude that $\alpha_{hgh^{-1}} = \alpha_g$ for all $h \in G$. This means that the function $\alpha : G \rightarrow \mathbb{C}$ is a *class function* (i.e., constant in each conjugacy class; we shall revisit this below), so X is a linear combination of the X_i 's. ■

§113. COROLLARY. *Let B be a finite abelian group. Then $\mathbb{C}B \cong \mathbb{C}^{|B|}$.*

Proof. This is immediate because any matrix ring $M_n(\mathbb{C})$ is noncommutative if and only if $n > 1$, and the number of conjugacy classes is $|B|$, so

$$\mathbb{C}B \cong \overbrace{\mathbb{C} \times \dots \times \mathbb{C}}^{|B| \text{ times}}. \quad \blacksquare$$

Lecture 9 (double). Characters of finite groups

9.1 More on group representations

Since any complex representation of a finite group G is completely reducible (why?), it follows that any finite dimensional left $\mathbb{C}G$ -module V is a finite direct sum of simple submodules $V = V_1 \oplus \dots \oplus V_s$, so choosing an appropriate basis of V we obtain a matrix representation

$$\pi : G \rightarrow GL_n(\mathbb{C})$$

where $n = \dim V$ and for each $g \in G$ the matrix $\pi(g)$ is a block diagonal matrix

$$\begin{pmatrix} \pi_1(g) & 0 & \cdots & 0 \\ 0 & \pi_2(g) & \cdots & 0 \\ & & \ddots & \\ 0 & 0 & \cdots & \pi_s(g) \end{pmatrix}$$

with each $\pi_i(g)$ being a square matrix of dimension $m_i \times m_i$ where m_i is the dimension of V_i . So the degree of the representation is the sum $n = m_1 + \cdots + m_s$.

In such a basis, then, π factors through a product of linear groups, so we can regard it as a map

$$\pi : G \rightarrow GL_{m_1}(\mathbb{C}) \times \cdots \times GL_{m_s}(\mathbb{C}).$$

Then each projection $\pi_i : GL_{m_1}(\mathbb{C}) \times \cdots \times GL_{m_s}(\mathbb{C}) \rightarrow GL_{m_i}(\mathbb{C})$ gives us the irreducible representation

$$\pi_i \circ \pi : G \rightarrow GL_{m_i}(\mathbb{C}),$$

which is a matrix representation corresponding to the simple $\mathbb{C}G$ -module V_i .

Moreover, the irreducible representations of G correspond, up to isomorphism, precisely to the projections of $\mathbb{C}G$ onto its Wedderburn components:

§114. COROLLARY. *Let G be a finite group whose complex group algebra is*

$$\mathbb{C}G \cong M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C}).$$

Then G has precisely r distinct isomorphism classes of irreducible representations, each corresponding to one of the r projections

$$\pi_i : \mathbb{C}G \rightarrow M_{n_i}(\mathbb{C}).$$

So any simple direct component (= minimal submodule) of a $\mathbb{C}G$ -module V must have complex dimension n_i for some $i = 1, \dots, r$.

§115. FACT. It can also be shown that the degree of each irreducible representation (i.e., each n_i) is a divisor of $|G|$ (cf. Theorem 18.2.12 of [2], which is proved only in section 19).

§116. COROLLARY. *Let B be an abelian group. The irreducible representations of B are all of degree 1, they are group homomorphisms $\pi : B \rightarrow \mathbb{C}^\times$ and there are exactly $|B|$ many of them corresponding to the projections $\mathbb{C}B \cong \mathbb{C}^{|B|} \rightarrow \mathbb{C}$.*

§117. COROLLARY. *Let G be a finite group. The irreducible representations of G with degree 1 (i.e., the homomorphisms $\pi : G \rightarrow \mathbb{C}^\times$) correspond bijectively to the irreducible representations of the abelianization of G ,*

$$\pi : G/[G, G] \rightarrow \mathbb{C}^\times,$$

so there are exactly $|G/[G, G]|$ isomorphism classes of irreducible representations of G with degree 1.

Proof. This follows immediately from the universal property of the abelianization, which establishes a bijection between homomorphisms $G \rightarrow B$ to abelian groups B and homomorphisms $G/[G, G] \rightarrow B$. ■

9.2 Character theory

The following is a streamlined version of the material of sections 18.3 and 19.1 of [2]. Contrary to the approach in [2], here for simplicity the underlying field will always be \mathbb{C} .

In the remainder of this note all the representations will be assumed to be of finite degree, and G always denotes a finite group.

§118. DEFINITION. By a (complex valued) *class function* on G is meant a function $f : G \rightarrow \mathbb{C}$ that is constant on each conjugacy class: $f(g^{-1}xg) = f(x)$ for all $x, g \in G$ (cf. §112).

§119. PROPOSITION.

1. *The set \mathcal{C} of all the class functions is a linear subspace of the space \mathbb{C}^G of all the complex valued functions on G .*
2. *A basis of \mathcal{C} is formed by the characteristic functions of the conjugacy classes; that is, a basic class function equals 1 on a given class and 0 on all the others.*
3. *Hence, \mathcal{C} has dimension r , where r is the number of conjugacy classes.*

Proof. Clear, due to §112. ■

§120. REMARK. Since G is a basis of $\mathbb{C}G$, each class function f is the restriction to G of the unique linear map $f : \mathbb{C}G \rightarrow \mathbb{C}$ such that

$$f\left(\sum_{g \in G} \alpha_g g\right) = \sum_{g \in G} \alpha_g f(g).$$

Hence, class functions will also be regarded as linear maps on $\mathbb{C}G$, so the linear space \mathcal{C} of class functions can be identified with a linear subspace of the dual space $(\mathbb{C}G)^*$.

§121. DEFINITION.

1. If $\varphi : G \rightarrow GL(V)$ is a representation, the *character* of φ is the function

$$\chi : G \rightarrow \mathbb{C}$$

defined by $\chi(g) = \text{tr } \varphi(g)$ for each $g \in G$.

2. The character χ is *reducible* or *irreducible* according to whether φ is a reducible or irreducible representation, respectively, and the *degree* of χ is the degree of φ (i.e., the dimension of V).

§122. NOTE. $\text{tr}(T)$ (or just $\text{tr } T$) is the trace of a complex linear transformation $T : V \rightarrow V$; that is, $\text{tr}(T)$ is the sum of the complex eigenvalues of T (repeated in the sum according to their multiplicities) or, equivalently, the sum of the diagonal entries of any matrix representation of T .

§123. EXAMPLE. Consider the canonical permutation representation of S_n on the set $X = \{1, \dots, n\}$. Each permutation $\sigma : X \rightarrow X$ extends uniquely to a linear isomorphism $\sigma^\# : \mathbb{C}^n \rightarrow \mathbb{C}^n$ which in the canonical basis is represented by a permutation matrix (i.e., a matrix whose entries are either 0 or 1 and which has exactly one 1 in each row and in each column). This defines a representation $\pi : S_n \rightarrow M_n(\mathbb{C})$. Letting χ be the associated character, for each $\sigma \in S_n$ the value $\chi(\sigma)$ is the number of fixed points of σ .

§124. EXAMPLE. A representation $\pi : D_{2n} \rightarrow M_2(\mathbb{C})$ is obtained by specifying

$$\begin{aligned} \pi(r) &= \begin{pmatrix} \cos 2\pi/n & -\sin 2\pi/n \\ \sin 2\pi/n & \cos 2\pi/n \end{pmatrix} \\ \pi(s) &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

The corresponding character satisfies

$$\begin{aligned}\chi(r) &= 2 \cos 2\pi/n \\ \chi(s) &= 0\end{aligned}$$

§125. MORE EXAMPLES OF CHARACTERS. See section 18.3 of [2].

§126. LEMMA.

1. Any two equivalent representations of G have the same character.
2. The character of any representation of G is a class function.
3. For any character χ , the value $\chi(1)$ is the degree of χ .

Proof. 1. By definition, $\varphi, \psi : G \rightarrow GL_n(\mathbb{C})$ are equivalent matrix representations if and only if for each $g \in G$ the matrices $\varphi(g)$ and $\psi(g)$ are similar, so they have the same trace.

2. If $x, g \in G$ and $\varphi : G \rightarrow GL_n(\mathbb{C})$ is a representation,

$$\operatorname{tr} \varphi(g^{-1}xg) = \operatorname{tr}(\varphi(g)^{-1}\varphi(x)\varphi(g)) = \operatorname{tr} \varphi(x).$$

3. $\chi(1)$ is the trace of an identity matrix, so it equals the degree of χ . ■

§127. FACT. An immediate fact follows from the previous lemma, namely that there exist at most r distinct irreducible characters (below we shall see that there are exactly r of them), since there are exactly r equivalence classes of irreducible representations.

§128. PROPOSITION. Let V_1 and V_2 two finite dimensional $\mathbb{C}G$ -modules with characters χ_1 and χ_2 , respectively. Then the character of $V_1 \oplus V_2$ is $\chi_1 + \chi_2$.

Proof. For some choice of bases of V_1 and V_2 let

$$\varphi_1 : G \rightarrow M_{n_1}(\mathbb{C}) \quad \text{and} \quad \varphi_2 : G \rightarrow M_{n_2}(\mathbb{C})$$

be the corresponding matrix representations. Then the matrix representation $\varphi : G \rightarrow M_{n_1+n_2}(\mathbb{C})$ afforded by the module $V_1 \oplus V_2$, with respect to the union of the two bases, is by block diagonal matrices

$$\begin{pmatrix} \varphi_1(g) & 0 \\ 0 & \varphi_2(g) \end{pmatrix}$$

and thus the character of φ is given by

$$\chi(g) = \operatorname{tr} \varphi(g) = \operatorname{tr} \varphi_1(g) + \operatorname{tr} \varphi_2(g) = \chi_1(g) + \chi_2(g). \quad \blacksquare$$

§129. COROLLARY. *The character of a representation is the sum of the (irreducible) characters of the constituents appearing in a direct sum decomposition.*

§130. NOTATION. Suppose

$$\mathbb{C}G \cong M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C}),$$

and let M_1, \dots, M_r be the simple $\mathbb{C}G$ -modules that correspond, respectively, to the irreducible representations $\pi_i : \mathbb{C}G \rightarrow M_{n_i}(\mathbb{C})$ for each $i = 1, \dots, r$. Any finite dimensional $\mathbb{C}G$ -module V is a direct sum of copies of the M_i 's, and each M_i appears in the decomposition with a certain multiplicity $a_i \in \mathbb{N}$; that is,

$$V \cong \overbrace{M_1 \oplus \cdots \oplus M_1}^{a_1 \text{ times}} \oplus \cdots \oplus \overbrace{M_r \oplus \cdots \oplus M_r}^{a_r \text{ times}}.$$

Henceforth let us abbreviate this by

$$a_1 M_1 \oplus \cdots \oplus a_r M_r.$$

Hence, letting χ_i be the irreducible character corresponding to each M_i , and χ the character corresponding to V , we obtain

$$\chi = a_1 \chi_1 + \cdots + a_r \chi_r,$$

and any such sum of irreducible characters is the character of some representation.

§131. LEMMA. *Two finite degree irreducible representations of a finite group G are equivalent if and only if they have the same character.*

Proof. Let the Wedderburn decomposition of $\mathbb{C}G$ be as follows:

$$\mathbb{C}G \cong M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C}). \quad (2)$$

Let us write A for the algebra $M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C})$. Then r is the number of equivalence classes of irreducible representations of A (and of G) and, as we have seen, there are at most r distinct irreducible characters. Let

$$\chi_1, \dots, \chi_r \in (\mathbb{C}G)^*$$

be the irreducible characters of G that correspond to the r irreducible representations that are the r projections

$$\pi_i : A \rightarrow M_{n_i}(\mathbb{C})$$

with $1 = 1, \dots, r$, respectively, and consider the following r idempotents of A :

$$\begin{aligned} z_1 &= (I, 0, 0, \dots, 0, 0), \\ z_2 &= (0, I, 0, \dots, 0, 0), \\ &\vdots \\ z_r &= (0, 0, \dots, 0, I). \end{aligned}$$

These are r central idempotents of A that form a linearly independent set, so they yield a basis of $Z(A)$. Let us write z^1, \dots, z^r for the dual basis; that is, each linear map $z^i : Z(A) \rightarrow \mathbb{C}$ is uniquely defined for all $j \neq i$ by

$$z^i(z_i) = 1 \quad \text{and} \quad z^i(z_j) = 0.$$

Now note that for each $i \neq j = 1, \dots, r$ we have

$$\chi_i(z_i) = n_i \quad \text{and} \quad \chi_i(z_j) = 0.$$

In other words, for each $i = 1, \dots, r$, the restriction $\chi'_i : Z(\mathbb{C}G) \rightarrow \mathbb{C}$ of the irreducible character $\chi_i : \mathbb{C}G \rightarrow \mathbb{C}$ satisfies

$$\chi'_i = n_i z^i.$$

Hence, the maps χ'_i form a basis of the dual space $(Z(\mathbb{C}G))^*$, which has dimension r , so all the irreducible characters χ_1, \dots, χ_r are linearly independent, and thus distinct. ■

§132. COROLLARY. *The irreducible characters of G form a basis of the complex vector space \mathcal{C} of complex valued class functions on G .*

Proof. Since \mathcal{C} has dimension r , and there are r linearly independent irreducible characters, which are class functions, the conclusion follows. ■

§133. NOTE. The set of characters consists of all the linear combinations of irreducible characters

$$a_1\chi_1 + \dots + a_r\chi_r$$

with coefficients taken from $\mathbb{Z}_{\geq 0}$, whereas the space of all the class functions consists of all the complex linear combinations of irreducible characters. This leads to the following generalization of §131, now applying to arbitrary finite degree representations rather than just irreducible ones.

§134. THEOREM. *Two finite degree representations of a finite group G are equivalent if and only if they have the same character.*

Proof. We have already seen that equivalent representations yield equal characters, so only the converse implication needs to be proved. Let

$$V \cong a_1 M_1 \oplus \cdots \oplus a_s M_r$$

where each M_i is a simple $\mathbb{C}G$ -module, and $M_i \not\cong M_j$ for all $i \neq j$, and $a_i \in \mathbb{Z}_{\geq 0}$. Similarly, let

$$W \cong b_1 M_1 \oplus \cdots \oplus b_s M_r$$

with $b_i \in \mathbb{Z}_{\geq 0}$. Letting χ_1, \dots, χ_r be the irreducible characters respectively corresponding to the simple modules M_1, \dots, M_r , the characters corresponding to V and W are respectively

$$a_1 \chi_1 + \cdots + a_r \chi_r \quad \text{and} \quad b_1 \chi_1 + \cdots + b_r \chi_r.$$

If these characters are equal then, since $\{\chi_1, \dots, \chi_r\}$ is a linearly independent set, it follows that $a_i = b_i$ for all $i = 1, \dots, r$, so $V \cong W$. ■

Lecture 10. Some character tables

In this lecture, when beginning to look at the examples of character tables, follow any order that you please. Perhaps the most instructive example to start with is that of the dihedral group D_8 .

10.1 Euclidean structure

Let $\theta, \psi : G \rightarrow \mathbb{C}$ be class functions. Define

$$\langle \theta, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \theta(g) \overline{\psi(g)}.$$

It is easily seen that this defines a complex inner product (i.e., a positive definite Hermitian sesquilinear form) on the vector space of class functions: for $\alpha, \beta \in \mathbb{C}$

1. $\langle \alpha\theta_1 + \beta\theta_2, \psi \rangle = \alpha\langle \theta_1, \psi \rangle + \beta\langle \theta_2, \psi \rangle$,
2. $\langle \theta, \psi \rangle = \overline{\langle \psi, \theta \rangle}$
(so also $\langle \theta, \alpha\psi_1 + \beta\psi_2 \rangle = \overline{\alpha}\langle \theta, \psi_1 \rangle + \overline{\beta}\langle \theta, \psi_2 \rangle$),

3. $\langle \theta, \theta \rangle \geq 0$,
4. If $\langle \theta, \theta \rangle = 0$ then $\theta = 0$.

(This is the canonical inner product on $\mathbb{C}^{|G|}$ divided by $|G|$.)

§135. LEMMA. *Let M_1, \dots, M_r be the simple modules of $\mathbb{C}G$ (one per isomorphism class), and let z_1, \dots, z_r be the primitive orthogonal central idempotents of $\mathbb{C}G$ such that z_i acts as the identity on M_i , and let χ_i be the irreducible character afforded by M_i . Then*

$$z_i = \frac{\chi_i(1)}{|G|} \sum_{g \in G} \chi_i(g^{-1})g.$$

Moreover, for any character ψ and $g \in G$ we have $\psi(g^{-1}) = \overline{\psi(g)}$, and $\psi(g)$ is a sum of roots of 1 in \mathbb{C} .

Proof. See propositions 13 and 14 of section 18.3 of [2]. ■

Using the previous results, after a bit of work one proves the following (see theorems 15 and 16 of section 18.3 of [2]):

§136. THEOREM (FIRST ORTHOGONALITY RELATION FOR GROUP CHARACTERS). *The irreducible characters of G form an orthonormal basis (with respect to the inner product defined above).*

§137. THEOREM (SECOND ORTHOGONALITY RELATION FOR GROUP CHARACTERS). *Letting χ_1, \dots, χ_r be the irreducible group characters of G , for all $x, y \in G$ we have*

$$\sum_{i=1}^r \chi_i(x) \overline{\chi_i(y)} = \begin{cases} |C_G(x)| & \text{if } x \text{ and } y \text{ are conjugate in } G \\ 0 & \text{otherwise.} \end{cases}$$

§138. EXERCISE. Show that the product of two characters is itself a character. (Suggestion: if θ and ψ are the characters afforded by $\mathbb{C}G$ -modules V and W , show that $\theta\psi$ is the character afforded by $V \otimes_{\mathbb{C}} W$ — cf. Proposition 17 of section 18.3 of [2].)

10.2 Character tables

The information about characters can be conveniently recorded in a *character table*, as in the following example for $Z_2 = \langle x \mid x^2 = 1 \rangle$. The columns are labeled by representatives of the conjugacy classes and the rows are labelled by irreducible characters, so character tables are square matrices. But there is an additional row (“sizes”) which records the size of the conjugacy class of each representative:

classes:	1	x
sizes:	1	1
χ_1	1	1
χ_2	1	-1

§139. EXAMPLE. The character table of $Z_3 = \langle x \mid x^3 = 1 \rangle$ is, given a primitive cubic root ζ of 1 (so $\zeta^2 = \bar{\zeta}$),

classes:	1	x	x^2
sizes:	1	1	1
χ_1	1	1	1
χ_2	1	ζ	ζ^2
χ_3	1	ζ^2	ζ

§140. EXAMPLE. The character table of S_3 is:

classes:	1	(1 2)	(1 2 3)
sizes:	1	3	2
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

Notice that the left column of any character table lists the degrees of each character. So, for instance, we see in this example that the three irreducible characters of S_3 have degrees 1, 1, and 2, respectively. Taking into account that $S_3 \cong D_6$, the character χ_3 is easy to understand in terms of the representation of D_{2n} in §124:

$$\begin{aligned} \pi((1\ 2\ 3)) &= \begin{pmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{pmatrix} \\ \pi((1\ 2)) &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

Let us use the table to confirm that the norm of χ_3 is 1:

$$\begin{aligned} \|\chi_3\|^2 &= \langle \chi_3, \chi_3 \rangle \\ &= \frac{1}{6} \sum_{\sigma \in S_3} |\chi_3(\sigma)|^2 \\ &= \frac{1}{6} (d_1 |\chi_3(1)|^2 + d_2 |\chi_3((1\ 2))|^2 + d_3 |\chi_3((1\ 2\ 3))|^2), \end{aligned}$$

where d_1 , d_2 and d_3 are the sizes of the conjugacy classes of 1, (1 2) and (1 2 3), which are listed in the character table. So

$$\|\chi_3\|^2 = \frac{1}{6} (|\chi_3(1)|^2 + 3|\chi_3((1\ 2))|^2 + 2|\chi_3((1\ 2\ 3))|^2) = \frac{1}{6}(4 + 2 \times 1) = 1.$$

§141. REMARK. Non-isomorphic groups can have the same character table. This is the case for D_8 and Q_8 , for instance. For these and other examples see section 19.1 of [2].

10.3 Example: character table of D_8

Let us compute the character table for D_8 . First we need to compute the conjugacy classes. Since $Z(D_8) = \{1, r^2\}$, there are exactly two singleton conjugacy classes, namely $\mathcal{O}_1 = \{1\}$ and $\mathcal{O}_{r^2} = \{r^2\}$. Since $\langle r \rangle \leq C_{D_8}(r)$ and r is not central, Lagrange's theorem forces $|C_{D_8}(r)| = 4$, so

$$|\mathcal{O}_r| = |D_8 : C_{D_8}(r)| = 2.$$

Then, noting that

$$sr s^{-1} = sr s = s^2 r^{-1} = r^3,$$

we conclude that $\mathcal{O}_r = \{r, r^3\}$. Now consider s . Its centralizer satisfies

$$\langle s \rangle \leq C_{D_8}(s),$$

so again by Lagrange's theorem the order of the centralizer must be either 2 or 4 (it cannot be 8 because s is not central). Since both 1 and r^2 commute with s , it follows that the order of the centralizer is 4, and thus $|\mathcal{O}_s| = 2$. Let us compute a conjugate of s :

$$r s r^{-1} = s r^{-2} = s r^2.$$

Hence, $\mathcal{O}_s = \{s, s r^2\}$. There are only two elements of D_8 to account for, sr and sr^3 , which are not central, so the remaining conjugacy class is $\mathcal{O}_{sr} =$

$\{sr, sr^3\}$. Hence, we have found five conjugacy classes, with orders 1, 1, 2, 2, and 2. Then there are five equivalence classes of irreducible representations, and thus

$$\mathbb{C}D_8 \cong M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_5}(\mathbb{C})$$

with $\sum_{i=1}^5 n_i^2 = 8$. The only possibility is to have four n_i 's equal to 1 and the other equal to 2, so we conclude that D_8 has, up to equivalence of representations, four irreducible representations of degree 1 and one irreducible representation of degree 2. One representation of degree 1 is the trivial representation $G \rightarrow \mathbb{C}^\times$, whose character χ_1 satisfies $\chi_1(g) = 1$ for all $g \in D_8$ (note that for any finite group there is such a trivial irreducible character of degree one). The irreducible representation of degree 2 is the usual matrix representation ρ by $\pi/2$ rotations and a reflection:

$$\rho(r) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \rho(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

The matrices of the other representatives of conjugacy classes are:

$$\rho(r^2) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \quad \rho(sr) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

This gives us the following incomplete character table, where χ_5 is the only irreducible character of degree 2, corresponding to the representation π :

classes:	1	r	r^2	s	sr
sizes:	1	2	1	2	2
χ_1	1	1	1	1	1
χ_2	1				
χ_3	1				
χ_4	1				
χ_5	2	0	-2	0	0

Another obvious irreducible representation of degree 1 sends r to 1 and s to -1 , for it is immediate that this respects the relations of D_8 (in fact the same would be true for any D_{2n}). The corresponding character χ_2 is given in the following table:

classes:	1	r	r^2	s	sr
sizes:	1	2	1	2	2
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1				
χ_4	1				
χ_5	2	0	-2	0	0

(The fact that $\chi_1 \neq \chi_2$ ensures that the two irreducible representations are not equivalent.) Another irreducible representation of degree 1 can be obtained by letting both r and s correspond to a rotation of π in the complex plane; in other words, both r and s are assigned to $-1 \in \mathbb{C}^\times$, corresponding to the irreducible character χ_3 :

classes:	1	r	r^2	s	sr
sizes:	1	2	1	2	2
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	-1	1	-1	1
χ_4	1				
χ_5	2	0	-2	0	0

(At each stage verify that the first orthogonality relations are satisfied, and that the norm of each line is 1 — remember that the sizes of the conjugacy classes must be accounted for.) There is only one irreducible character missing from our table, again of degree 1. Note that the assignments $r \mapsto -1$ and $s \mapsto 1$ also respect the relations of D_8 , so we conclude the character table:

classes:	1	r	r^2	s	sr
sizes:	1	2	1	2	2
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	-1	1	-1	1
χ_4	1	-1	1	1	-1
χ_5	2	0	-2	0	0

§142. EXERCISE. Revisit Exercise §140 seeing S_3 as the dihedral group D_6 , using similar ideas as those which we used for D_8 .

10.4 Example: character table of D_{14}

This was not seen in the lecture, but students should go through this example, too.

Similarly to any dihedral group, there are two irreducible representations of degree 1, namely the trivial one that assigns every group element to 1 (which exists for every finite group), and the irreducible representation $\rho : D_{14} \rightarrow \mathbb{C}^\times$ defined by $\rho(r) = 1$ and $\rho(s) = -1$. In order to move further, let us compute the conjugacy class \mathcal{O}_g for each $g \in D_{14}$. The reasoning is again based on computing centralizers and applying Lagrange's theorem, so now we shall abbreviate a bit.

$|\mathcal{O}_r| = 2$ (this is true for any D_{2n} , $n \geq 3$). A conjugate of r is $sr s = r^6$, so $\mathcal{O}_r = \{r, r^6\}$.

Since $\langle r \rangle$ is cyclic of prime order, the centralizers of all the powers r^2, \dots, r^5 have order 7, so again the orbits of these elements have order 2. Hence, $\mathcal{O}_{r^2} = \{r^2, r^5\}$ because $sr^2s = r^5$, and $\mathcal{O}_{r^3} = \{r^3, r^4\}$ because $sr^3s = r^4$.

Next, we consider the centralizer of s : since in D_{14} the reflection s commutes with no power of r , and also with no element of the form sr^k with $k = 1, \dots, 6$, $C_{D_{14}}(s) = \{1, s\}$, so $|\mathcal{O}_s| = 7$. Hence, \mathcal{O}_s consists of all the seven elements of order 2.

Summarizing, there are 5 conjugacy classes:

- $\mathcal{O}_1 = \{1\}$
- $\mathcal{O}_r = \{r, r^6\}$
- $\mathcal{O}_{r^2} = \{r^2, r^5\}$
- $\mathcal{O}_{r^3} = \{r^3, r^4\}$
- $\mathcal{O}_s = \{s, sr, sr^2, sr^3, sr^4, sr^5, sr^6\}$

Since two of the irreducible characters must have degree 1, the squares of the remaining three irreducible characters must add up to 12, so they are all of degree 2. This leads us to the first incomplete character table:

classes:	1	r	r^2	r^3	s
sizes:	1	2	2	2	7
χ_1	1	1	1	1	1
χ_2	1	1	1	1	-1
χ_3	2				
χ_4	2				
χ_5	2				

The remaining three irreducible representations can be based on rotation and permutation matrices, the “standard” one being

$$\rho_3(r) = \begin{pmatrix} \cos(2\pi/7) & -\sin(2\pi/7) \\ \sin(2\pi/7) & \cos(2\pi/7) \end{pmatrix} \quad \rho_3(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

The two other irreducible representations can be obtained by duplicating and triplicating the rotation “speed”:

$$\rho_4(r) = \begin{pmatrix} \cos(4\pi/7) & -\sin(4\pi/7) \\ \sin(4\pi/7) & \cos(4\pi/7) \end{pmatrix} \quad \rho_4(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$\rho_5(r) = \begin{pmatrix} \cos(6\pi/7) & -\sin(6\pi/7) \\ \sin(6\pi/7) & \cos(6\pi/7) \end{pmatrix} \quad \rho_5(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Note that as the powers of r range from $1 = r^0$ to r^6 and then back to 1 the representation ρ_3 performs one full rotation, whereas ρ_4 and ρ_5 perform two and three full rotations, respectively. So the intuition behind these being nonequivalent representations resembles that of single, double and triple loops being distinct in the fundamental group of the 1-sphere. The quickest way to confirm that the representations are not equivalent is to verify that their characters are different:

classes:	1	r	r^2	r^3	s
sizes:	1	2	2	2	7
χ_1	1	1	1	1	1
χ_2	1	1	1	1	-1
χ_3	2	$2 \cos(2\pi/7)$	$2 \cos(4\pi/7)$	$2 \cos(6\pi/7)$	0
χ_4	2	$2 \cos(4\pi/7)$	$2 \cos(8\pi/7)$	$2 \cos(12\pi/7)$	0
χ_5	2	$2 \cos(6\pi/7)$	$2 \cos(12\pi/7)$	$2 \cos(18\pi/7)$	0

This becomes more visible if we choose all angles to lie in the upper half plane:

classes:	1	r	r^2	r^3	s
sizes:	1	2	2	2	7
χ_1	1	1	1	1	1
χ_2	1	1	1	1	-1
χ_3	2	$2 \cos(2\pi/7)$	$2 \cos(4\pi/7)$	$2 \cos(6\pi/7)$	0
χ_4	2	$2 \cos(4\pi/7)$	$2 \cos(6\pi/7)$	$2 \cos(2\pi/7)$	0
χ_5	2	$2 \cos(6\pi/7)$	$2 \cos(2\pi/7)$	$2 \cos(4\pi/7)$	0

§143. EXERCISE. Verify that ρ_4 and ρ_5 are indeed representations (check that the defining relations are respected), and that they are irreducible.

§144. EXERCISE. Verify that the following defines an irreducible representation of D_{14} :

$$\rho(r) = \begin{pmatrix} \cos(2\pi/7) & \sin(2\pi/7) \\ -\sin(2\pi/7) & \cos(2\pi/7) \end{pmatrix} \quad \rho(s) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

To which of the representations ρ_3 , ρ_4 , or ρ_5 is it equivalent? Describe an explicit isomorphism of modules that proves the equivalence.

§145. EXERCISE. Can you generalize the D_{14} example so as to describe the character table of any dihedral group D_{2p} for a prime p ?

Lecture 11 (double). General representation theory

In this lecture we see some representation theory that goes beyond semisimple algebras.

11.1 Jacobson's density theorem

Suppose $A \cong M_{n_1}(\Delta_1) \times \cdots \times M_{n_r}(\Delta_r)$ is a semisimple ring, with each Δ_i being a division ring. Then A has r equivalence classes of irreducible representations, each of which corresponding to one of the projections π_1, \dots, π_r :

$$\pi_i : M_{n_1}(\Delta) \times \cdots \times M_{n_r}(\Delta) \rightarrow M_{n_i}(\Delta).$$

Since each projection is surjective, we conclude that any irreducible representation of A is given by a surjective homomorphism

$$\rho : A \rightarrow M_n(\Delta).$$

§146. EXAMPLE. If $A = M_2(F) \times M_3(F)$ for a field F , a simple A -module is F^2 . For each pair of linearly independent vectors $x_1, x_2 \in F^2$ and each pair of vectors $y_1, y_2 \in F^2$ there is a unique F -linear transformation $T : F^2 \rightarrow F^2$ such that $T(x_1) = y_1$ and $T(x_2) = y_2$. Equivalently, there is a unique matrix $B \in M_2(F)$ such that $Bx_1 = y_1$ and $Bx_2 = y_2$, so there is an element $a \in A$, for instance $a = (B, 0)$, such that $ax_1 \rightarrow y_1$ and $ax_2 = y_2$. This is a way of “explaining” why the irreducible representation $\pi_1 : A \rightarrow M_2(F)$ is surjective. However, this property is more general than the context of semisimple rings would suggest, as we will see now.

§147. JACOBSON'S DENSITY THEOREM. *Let A be a ring, V a simple A -module, and D the division ring $\text{End}_A(V)$. Let x_1, \dots, x_n be linearly independent elements of V (over D). Then for all $y_1, \dots, y_n \in V$ there is $a \in A$ such that $ax_i = y_i$ for all $i = 1, \dots, n$.*

Proof. The proof is by induction on n .

The base case is $n = 1$, where the list of linearly independent elements consists of a single element $x_1 \neq 0$. Then the cyclic submodule $Ax_1 \subset V$ has to coincide with V because V is simple. In particular, there is $a \in A$ such that $ax_1 = y_1$.

Now assume that $n \in \mathbb{Z}_{>1}$ and that the theorem holds for all integers in $\{1, \dots, n-1\}$. Let x_1, \dots, x_n be linearly independent elements of V and let $y_1, \dots, y_n \in V$. Let us first prove (using the induction hypothesis) the following statement:

(*) There exist $a_1, \dots, a_n \in A$ such that $a_i x_i \neq 0$ and $a_i x_j = 0$ for all $i, j = 1, \dots, n$ and $i \neq j$.

Let us assume that (*) is false and derive a contradiction. Writing X for the set $\{x_1, \dots, x_n\}$, the assumption that (*) is false means that there is at least one subset $X' \subset X$ containing $n-1$ elements such that whenever $ax' = 0$ for all $x' \in X'$ then necessarily $ax = 0$ for the element $x \in X \setminus X'$. Without loss of generality, let us suppose that $X' = \{x_1, \dots, x_{n-1}\}$, and let us assume that

(**) for all $a \in A$ the condition $ax_1 = \dots = ax_{n-1} = 0$ implies $ax_n = 0$.

This assumption allows us to define a homomorphism of A -modules

$$\varphi : V^{n-1} \rightarrow V$$

as we will see now. For each $(z_1, \dots, z_n) \in V^{n-1}$ the induction hypothesis ensures that there is $a \in A$ such that

$$ax_i = z_i \text{ for all } i = 1, \dots, n-1.$$

Moreover, if there is any other $a' \in A$ such that

$$a'x_i = z_i \text{ for all } i = 1, \dots, n-1,$$

then $(a - a')x_i = 0$ for all $i = 1, \dots, n-1$, and thus the assumption (**) entails $(a - a')x_n = 0$, so $ax_n = a'x_n$. Hence, we can take any such $a \in A$ and obtain a well defined homomorphism by the formula

$$\varphi(z_1, \dots, z_n) = ax_n.$$

Now for each $i = 1, \dots, n-1$ define $\xi_i \in D$ by composing the injection $\iota_i : V \rightarrow V^{n-1}$ with φ :

$$\xi_i = \varphi \iota_i : V \rightarrow V.$$

Then

$$\begin{aligned} \varphi(z_1, \dots, z_{n-1}) &= \varphi(z_1, 0, \dots, 0) + \dots + \varphi(0, \dots, 0, z_{n-1}) \\ &= \xi_1 z_1 + \dots + \xi_{n-1} z_{n-1}. \end{aligned}$$

But then, choosing $(z_1, \dots, z_{n-1}) = (x_1, \dots, x_{n-1})$ and $a = 1$, we obtain

$$x_n = 1x_n = \varphi(x_1, \dots, x_{n-1}) = \xi_1 x_1 + \dots + \xi_{n-1} x_{n-1},$$

which implies that the elements x_1, \dots, x_n are linearly dependent. This is a contradiction that resulted from negating the condition (*), so (*) is true.

Finally, using (*), let us finish the proof. For each $i, j = 1, \dots, n-1$ let a_i be such that $a_i x_i \neq 0$ and $a_i x_j = 0$ if $i \neq j$. Since $a_i x_i \neq 0$, there is $b_i \in A$ such that $b_i(a_i x_i) = y_i$ because V is a simple module (using similar reasoning to that of the induction base). Let

$$a = b_1 a_1 + \dots + b_n a_n.$$

Then for each $i = 1, \dots, n$ we have

$$ax_i = b_1 a_1 x_i + \dots + b_n a_n x_i = b_i a_i x_i = y_i,$$

thus concluding the proof. ■