4. ALGEBRAS AND MODULES

§4.1. Group Algebras

Most useful rings contain a field, and hence have a vector space structure as well as a ring structure. An **algebra** over a field F is a ring which is also a vector space over F. Examples include the algebra of polynomials over a field, and the algebra of $n \times n$ matrices over a field.

For the purposes of representation theory the most important type of algebra is a group algebra. We start with a group, such as S_3 = {I, (123), (132), (12), (13), (23)}. This has its own multiplication operation. We make it into a ring by adding group elements.

What on earth is (123) + (12)? The answer is (123) + (12). In other words we consider formal sums and differences of group elements. These are no longer in the group, of course, they are in some enlarged system where, for example, if we add 3(23) + (123) to 5(12) – 7(23) we get (123) + 5(12) – 4(23).

But if we want our system to be an algebra, say over the complex number field, we need to include such formal expressions as $\sqrt{2}\mathrm{I} - \pi(123) + \frac{17}{3}(12) - 42.(23)$, which is given here in its simplest form.

The **group algebra** of $G = \{g_1, g_2, \ldots, g_n\}$ over F is the set of all formal expressions of the form:

$$\lambda_1 g_1 + \lambda_2 g_2 + \ldots + \lambda_n g_n.$$

It is denoted by **FG**. Addition and scalar multiplication are defined in the obvious way. Multiplication of two such formal expressions is also defined in the usual way, with products $g_i g_j$ being evaluated in the group. One of the g_i, usually it is g_1, is the identity, which we will write as I instead of 1 to avoid confusion. Five times the identity would be written as 5I instead of the more confusing 51.

The dimension of FG as a vector space over F is clearly $|G|$.

Example 1: $\mathbb{C}\langle g \mid g^3 = 1\rangle = \{aI + bg + cg^2 \mid a, b, c \in \mathbb{C}\}$ and $g \in \langle g \mid g^3 = 1\rangle\}$.

In this algebra
$$\begin{aligned}(I - g)^5 &= I - 5g + 10g^2 - 10g^3 + 5g^4 - g^5 \\ &= I - 5g + 10g^2 - 10\,I + 5g - g^2 \\ &= -9\,I + 9g^2 \\ &= 9(g^2 - I).\end{aligned}$$

Except where the group is the trivial group, the group algebra is not a field as it has divisors of zero – two non-zero elements whose product is zero.

Example 2: In $\mathbb{C}S_3$, if $x = (123) - (132) + (13) - (23)$ then $x^2 = 0$.

The **centre** of an algebra is the set **Z(A)** of all elements of A that commute with every element of A. Z(A) is clearly a subalgebra of A but, as we will show, it is not in general an ideal of A.

Example 3: Consider the algebra $\mathbb{C}S_3$.
Let $z = (123) + (132) \in Z(CS_3)$.
Clearly z commutes with both (123) and (132). Moreover:

$$z(12) = (123)(12) + (132)(12) = (23) + (13) \text{ and}$$
$$(12)z = (12)(123) + (12)(132) = (13) + (23) = z(12).$$

Similarly z commutes with (13) and (23). So $z \in Z(\mathbb{C}S_3)$.
Similar calculations show that:

$$(12) + (13) + (23) \in Z(\mathbb{C}S_3).$$

Theorem 1: If G is a finite group then Z(FG) is the set of all linear combinations of the sums of each conjugacy class of G.
Proof: Let Γ be a conjugacy class and let γ be the formal sum of its elements. Conjugating γ by a group element will simply permute the elements of Γ and hence the terms of γ, which doesn't change it. So γ commutes with all the group elements and hence with all the formal linear combinations of group elements.

Conversely, if $\lambda_1 g_1 + \lambda_2 g_2 + \ldots + \lambda_n g_n \in Z(FG)$ then conjugating it by $g \in G$ leaves it unchanged.
Hence:

$$\lambda_1 g^{-1} g_1 g + \lambda_2 g^{-1} g_2 g + \ldots \lambda_n g^{-1} g_n g$$
$$= \lambda_1 g_1 + \lambda_2 g_2 + \ldots + \lambda_n g_n.$$

Since these are formal expressions we may equate corresponding coefficients, and so clearly conjugate elements have the same coefficient. We may take this out as a common factor from all the terms in a given conjugacy class and end up with a linear combination of the sums of the elements in the respective conjugacy classes.

In fact if the conjugacy classes are $\Gamma_1, \Gamma_2, \ldots, \Gamma_n$ and if γ_i is the formal sum of the elements of Γ_i, then

$\{\gamma_1, \gamma_2, \ldots, \gamma_n\}$ is a basis for Z(FG). ✋☺

Corollary: The dimension of Z(FG) over F is the number of conjugacy classes in G.

§4.2. Modules

The scalars in a vector space must come from a field. But we'd like to have 'vector spaces' in which the scalars come from a ring. We can do so, provided we call them something other than vector spaces, and provided we don't expect all the theory of vector spaces to apply in this new environment.

One important difference will be the fact that if the ring is non-commutative then it's important, if we have to multiply by two scalars in succession, in which order we multiply them. The right hand side of the equation $(\lambda\mu)\mathbf{v} = \lambda(\mu\mathbf{v})$ has $\mathbf{v}$ multiplied first by μ and then by λ whereas it is more natural to have them multiply in the order given, reading from left to right. We are in a similar situation to what we were with functions, and we solve it the same way – we write our scalars on the right. The expression

$\mathbf{v}\lambda$ may look a little strange and unfamiliar but you'll get used to it, especially as we'll be dropping the convention that vectors appear in bold type.

Let R be a ring. A (right) **R-module** is a 'vector space' over the ring R. Just go through all the vector space axioms and write the scalars on the right. The crucial one is:

$$v(\lambda\mu) = (v\lambda)\mu$$

which looks like an associative law.

Examples 2:
(1) Vector spaces over F are F-modules, where F is a field.
(2) Abelian groups are $\mathbb{Z}$-modules.
(3) Every ring R is a right R-module.

Submodules and **quotient modules** are defined as for groups or rings. One important difference is that while G/H is only defined when H is a normal subgroup of the group, G, and R/I is only defined when I is a 2-sided ideal of the ring R, M/N is defined whenever N is a submodule of M.

Examples 3:
(1) For F-modules (vector spaces over F), the submodules are the subspaces.
(2) For $\mathbb{Z}$-modules (abelian groups), the submodules are the subgroups.
(3) Considering R as a right R-module, the submodules are the right ideals.

If M, N are R-modules the map f:M $\rightarrow$ N is a **homomorphism** if it is an abelian group homomorphism and (mr)f = (mf)r for all m $\in$ M, r $\in$ *R*. **Kernels**, **images** and **isomorphisms** are defined as for vector spaces.

In some ways modules behave just like vector spaces. One important difference is that the vector space theorem that enables dimension to be well-defined does not hold in general. It does, however, for finitely generated modules over a division ring (a ring that satisfies all the field axioms except, possibly, the commutative law for multiplication).

Another elementary, but important fact about vector spaces is that if $\lambda\mathbf{v} = 0$ then $\mathbf{v} = \mathbf{0}$ or $\lambda = 0$**.** In modules in general we can have non-zero elements, *r*, for which m*r* = 0 for many ring elements, not just zero.

The **annihilator** of a subset X of an R-module M is defined to be:

$$\mathbf{A(X)} = \{a \in R \mid xa = 0 \text{ for all } x \in X\}.$$

Example 4: If M = $\mathbb{R}^2$, and R is the ring of all 2 $\times$ 2 matrices over $\mathbb{R}$, then M is an R-module by the usual definition of multiplying a row vector by a matrix.
If X = {(*x*, 0)} then A(X) is the set of 2 $\times$ 2 matrices of the form $\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$.

Clearly if $X \subseteq Y$ then $A(X) \supseteq A(Y)$ and it's easy to show that A(X) is always a right ideal of R. If X is a submodule we can do even better.

Theorem 2: If N is a submodule of the R-module M then A(N) is a 2-sided ideal of R.
Proof: Checking that it is a left ideal suppose $\alpha \in A(X)$ and $r \in R$. Let $n \in N$.
Then $n(r\alpha) = (nr)\alpha$. Now $nr \in N$ since N is a submodule, and α annihilates all the elements of N. ✋☺

As for groups or rings we define an **endomorphism** to be homomorphism from a module to itself. The set of all R-module endomorphisms of M is $\mathbf{End_R(M)}$, a subring of the ring of all abelian group endomorphisms of M, denoted by **End(M)**.

Theorem 3: If M is an R-module, R/A(M) is isomorphic to a submodule of End(M).
Proof: Right multiplication by an element of R is a module endomorphism. The function that maps that element to the corresponding endomorphism is a ring homomorphism, and so the result follows from the First Isomorphism Theorem for rings. ✋☺

Note that for every ring R an abelian group M can be made into an R-module by simply defining every scalar product to be zero, in which case every element of M has the whole of R as its annihilator. Such modules are

called trivial. That is, the R-module M is **trivial** if A(M) = R. In the same way every abelian group G can be made into a ring by defining every product to be zero. Such rings are called zero rings. That is, a ring is a **zero ring** if it is a trivial R-module ie $R^2 = 0$. Remember that R^2 doesn't just contain all the squares – it contains all sums of products of elements of R.

At the other end of the spectrum we have faithful modules. M is **faithful** if A(M) = 0. If you think that there must be some connection between trivial and faithful modules and trivial and faithful representations you're on the right track – there is.

M is an **irreducible** module if it is non-trivial and 0 and M are its only submodules. The main part of the definition is the bit about 0 and M being the only submodules. The non-trivial condition is just a technical restriction that plays a similar role to the condition that rules out the number 1 being a prime even though 1 is its only (positive) divisor.

The next theorem shows that irreducible modules can be generated by a single element, and in fact every non-zero element is a generator. Notice where that technical condition of non-triviality plays a vital role at the end of the proof.

Theorem 4: If M is irreducible and $0 \neq m \in M$ then

$$M = mR.$$

Proof: Suppose M is irreducible and $0 \neq m \in M$.
Now $mR = \{mr \mid r \in R\}$ is a submodule.

Then $mR = 0$ or $mR = M$.
Also $A = \{x \mid xR = 0\}$ is a submodule. This is a bit like an annihilator, but instead of being a subset of R it's a subset of M. Since M is irreducible, $A = 0$ or $A = M$.

Suppose $mR \neq M$. Then $mR = 0$ and so $m \in A$.
But $m \neq 0$ so $A \neq 0$. It follows that $A = M$.
But that would mean that M is trivial, which the definition of irreducibility rules out. So we get a contradiction, and hence $mR = M$. ✋☺

A fundamental theorem is the following, called Schur's Lemma. It will be used later to show that every non-zero element of a certain ring of homomorphisms has an inverse.

Theorem 5 (SCHUR'S LEMMA): If M, N are irreducible R-modules and $f:M \to N$ is a module homomorphism then $f = 0$ or it is an isomorphism (and so has an inverse).
Proof: If $f \neq 0$ then $\ker f = M$ and $\text{im } f = 0$. ✋☺
Corollary: If M is an irreducible R-module then $\text{End}_R(M)$ is a **division ring**, that is a ring that satisfies all the axioms of a field with the exception of the commutative law for multiplication.

Theorem 6: If M is an irreducible R-module, where R contains the field of complex numbers, and $f:M\to M$ is an R-module isomorphism, then there exists $\lambda \in \mathbb{C}$ with

$$mf = m\lambda \text{ for all } m \in M.$$

Proof: f is a vector space isomorphism and so has an eigenvalue λ. Because there's a corresponding eigenvector, the kernel of $f - \lambda I$ is a non-zero submodule of M so is M. ✋☺

§4.3. Representation Modules

Representation modules provide an alternative perspective on group representations. Every representation of a group G over a field F gives rise to a corresponding module over the group algebra FG. Conversely, every module over FG gives rise to a representation.

There is in fact a 1-1 correspondence between representations of G over F and FG-modules. The ones we're interested in are the representations on finite-dimensional vector spaces and these correspond to FG-modules that are finite-dimensional over F.

If $\rho:G\to End_F(V)$ is a representation of G then $\mathbf{V[\rho]}$ is the FG-module on V by defining

$$v.(\Sigma x_i g_i) = v.(\Sigma\, x_i(g_i\rho)).$$

Conversely, if M is an FG-module then $\boldsymbol{\rho[M]}:G\to End_F(M)$ is the representation defined by $m(g.\rho[M]) = mg$.

Since $M[\rho[M]] = M$ and $\rho[V[\rho]] = \rho$, there's a 1-1 correspondence between representations of G over F and FG-modules.

Properties of the representation translate smoothly to the corresponding module, usually using the same terminology.

The representation $\rho: G \to End_F(V)$ is **irreducible** if and only if $V[\rho]$ is an irreducible FG-module, in other words, if $V[\rho]$ has no subspaces invariant under all $g\rho$.

The representation $\rho: G \to End_F(V)$ is **faithful** if and only if $V[\rho]$ is a faithful FG-module.

Representations $\rho: G \to End_F(U)$ and $\sigma: G \to End_F(V)$ are **equivalent** if and only if $U[\rho] \cong V[\rho]$ as FG-modules.

§4.4. The Wedderburn Structure Theorem

The Wedderburn Structure Theorem is an important classification theorem that shows that if F is an algebraically closed field then a nil-semi-simple algebra over F, with descending chain condition on right ideals, is isomorphic to a direct sum of matrix algebras of the form $M_n(F)$. Here $\mathbf{M_n(F)}$ denotes the algebra of all $n \times n$ matrices over F.

It doesn't matter if you don't know what these properties of the algebra or the field are. An important special case is the case where the field is $\mathbb{C}$, the field of complex numbers, and the algebra is $\mathbb{C}G$, the group algebra of a finite group. We don't provide a proof here.

Theorem 7 (WEDDERRBURN STRUCTURE THEOREM – Special Case):
Let G be a finite group. Then:
(1) $\mathbb{C}G \cong R_1 \oplus R_2 \oplus \ldots \oplus R_k$ for some k where each R_i is isomorphic to $M_{n_i}(\mathbb{C})$ the ring of $n_i \times n_i$ matrices over $\mathbb{C}$.
(2) Every irreducible $\mathbb{C}G$-module is isomorphic to a minimal right ideal of some R_i, considered as an $\mathbb{C}G$-module.
(3) Minimal right ideals of the same R_i are isomorphic as modules and those corresponding to different R_i are non isomorphic.
Proof: The proof is contained in my *Ring Theory* Notes. ✋

Corollary: $\Sigma n_i^2 = |G|$.

Example 5: $\mathbb{C}S_3 \cong \mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C})$
This is because the only solutions to $\Sigma n_i^2 = 6$ are 1,1,1,1,1,1 and 1,1,2.
The first case implies that $\mathbb{C}S_3$ is commutative which is clearly not the case.

Theorem 8: Let G be a finite group. Then the number of irreducible representations of G over $\mathbb{C}$ is the number of conjugacy classes of G.
Proof: $\mathbb{C}G \cong M_{n_1}(\mathbb{C}) \oplus \ldots \oplus M_{n_k}(\mathbb{C})$ where k is the number of irreducible representations by Theorem 7. The centre of $\mathbb{C}G$ is the direct sum of the centres of the direct summands and the centre of each summand has dimension 1, consisting of the scalar matrices. Hence the

centre of $\mathbb{C}G$ has dimension k. But this is the number of conjugacy classes. 👌☺