GROUP ALGEBRAS.

ANDREI YAFAEV

We will associate a certain algebra to a finite group and prove that it is semisimple. Then we will apply Wedderburn's theory to its study.

Definition 0.1. *Let G be a finite group. We define $F[G]$ as a set of* formal *sums*

$$u = \sum_{g \in G} \lambda_g g, \lambda_g \in F$$

endowed with two operations: addition and multiplication defined as follows.

$$\sum_{g \in G} \lambda_g g + \sum_{g \in G} \mu_g g = \sum_{g \in G} (\lambda_g + \mu_g) g$$

and

$$\sum_{g \in G} \lambda_g g \times \sum_{g \in G} \mu_h h = \sum_{g \in G, h \in G} (\lambda_h \mu_{h^{-1}g}) g$$

Note that the multiplication is induced by multiplication in G, F and linearity.

The following proposition is left to the reader.

Proposition 0.1. *The set $(F[G], +, \times)$ is a ring and is an F-vector space of dimension $|G|$ with scalar multiplication compatible with group operation. Hence $F[G]$ is an F-algebra.*

The algebra $F[G]$ is non-commutative unless the group G is comutative.

It is clear that the basis elements (elements of G) are invertible in $F[G]$.

Lemma 0.2. *The algebra $F[G]$ is a* **not** *a division algebra.*

Proof. It is easy to find zero divisors. Let $g \in G$ and let m be the order of G (the group G is finite, every element has finite order). Then

$$(1 - g)(1 + g + g^2 + \cdots + g^{m-1}) = 0$$

□

In this course we will study $F[G]$-modules, modules over the algebra $F[G]$. An important example of a $F[G]$-module is $F[G]$ itself viewed as a $F[G]$-module. We leave the verifications to the reader. This module is called a *regular* $F[G]$-module and the associated representation a *regular* representation.

Next we introduce the notion of $F[G]$-homomorphism between $F[G]$-modules.

Definition 0.2. *Let V and W be two $F[G]$-modules. A function $\phi\colon V \longrightarrow W$ is called a $F[G]$-homomorphism if it is a homomorphism from V to W viewed as modules over $F[G]$.*

That means that ϕ is F-linear and satisfies

$$\phi(gv) = g\phi(v)$$

for all $g \in G$ and $v \in V$.

We obviously have the following.

Proposition 0.3. *Let $\phi\colon V \longrightarrow W$ be a $F[G]$-homomorphism. Then $\ker(\phi)$ and $\operatorname{im}(\phi)$ are $F[G]$-submodules of V and W respectively.*

Definition 0.3. *Let G be a finite group, F a field and V a finite dimensional vector space over F. A representation ρ of G on V is a group homomorphism*

$$\rho\colon G \longrightarrow \mathrm{GL}(V)$$

A representation is called **faithful** *if $\ker(\rho) = \{1\}$.*

A representation is called **irreducible** *if the only subspaces W of V such that $\rho(G)W \subset W$ are $W = \{0\}$ and $W = V$.*

The following theorem telles us that a representation of G and an $F[G]$-module are same things.

Theorem 0.4. *Let G be a finite group and F a field. There is a one-to-one correspondence between representations of G over F and finitely generated left $F[G]$-modules.*

Proof. Let V be a (finitely generated) $F[G]$-module. Then V is a finite dimensional vectore space. Let g be in G, then, by axioms satisfied by a module, the action of g on V defines an invertible linear map which gives an element $\rho(g)$ of $\mathrm{GL}(V)$. It is trivial to check that $\rho\colon G \longrightarrow \mathrm{GL}(V)$ is a group homomorphism i.e. a representation $G \longrightarrow \mathrm{GL}(V)$.

Let $\rho\colon G \longrightarrow \mathrm{GL}(V)$ be a representation. Let $x = \sum_{g\in G} \lambda_g g$ be an element of $F[G]$ and let $v \in V$. Define

$$xv = \sum_{g\in G} \lambda_g \rho(g) v$$

It is easy to check that this defines a structure of an $F[G]$-module on V. $\square$

By definition, a morphism between two representation is a morphism of the corresponding $F[G]$-modules. Two representations are isomorphic (or equivalent) if the corresponding $F[G]$-modules are isomorphic.

Given an $F[G]$-module V and a basis B of V as F-vector space, for $g \in G$, we will denote by $[g]_B$ the matrix of the linear transformation defined by g with respect to the basis B.

For example :

Let
$$D_8 = \{a, b : a^4 = b^2 = 1, b^{-1}ab = a^{-1}\}$$
and define a representation by
$$\rho(a) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ and } \rho(b) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
Choose B to be the canonical basis $v_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $v_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ of $V = F^2$. We have:
$$\begin{array}{cc} av_1 = -v_2 & av_2 = v_1 \\ bv_1 = v_1 & bv_2 = -v_2 \end{array}$$
This completely determines the structure of V as a $F[D_8]$-module. Conversely, by taking the matrices $[a]_B$ and $[b]_B$, we recover our representation ρ.

Another example :

Let G be the group S_n, group of permutations of the set $\{1, \ldots, n\}$. Let V be a vector space of dimension n over F (the n here is *the same* as the one in S_n). Let $\{v_1, \ldots, v_n\}$ be a basis of V. We define
$$gv_i = v_{g(i)}$$
The reader will verify that the conditions of the above proposition are verified and hence we construct a $F[G]$-module called the *permutation module.*

Let $n = 4$ and let $B = \{v_1, \ldots, v_n\}$ be a basis of F^4. Let g be the prmutation $(1, 2)$. Then
$$gv_1 = v_2, gv_2 = v_1, gv_3 = v_3, gv_4 = v_4$$
The matrix $[g]_B$ is
$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Lemma 0.5. *A representation $\rho\colon G \longrightarrow \mathrm{GL}_n(F)$ is irreducible (or simple) if and only if the corresponding $F[G]$-module is simple.*

Proof. A non-trivial invariant subspace $W \subset V$ is a non-trivial $F[G]$-submodule, and conversely. $\square$

Note that ρ being irreducible means that the only $\rho(G)$-invariant subspaces of V are $\{0\}$ and V itself.

If a representation is reducible i.e. there is a $F[G]$-submodule W of V, then we can choose a basis B of V (choose a basis B_1 of B and complete it to a basis of B) in such a way that the matrix $[g]_B$ for all g is of the form

$$\begin{pmatrix} X_g & Y_g \\ 0 & Z_g \end{pmatrix}$$

where X_g is a $\dim W \times \dim W$ matrix. Clearly, the functions $g \mapsto X_g$ and $g \mapsto Z_g$ are representations of G.

Let's look at an example. Take $G = C_3 = \{a : a^3 = 1\}$ and consider the $F[G]$-module V ($\dim V = 3$) such that

$$av_1 = v_2, av_2 = v_3, av_3 = v_1$$

(Easy exercise : check that this indeed defines an $F[G]$-module)

This is a reducible $F[G]$-module. Indeed, let $W = Fw$ with $w = v_1 + v_2 + v_3$. Clearly this is a $F[G]$-submodule. Consider the basis $B = \{w, v_2, v_3\}$ of V. Then

$$[I_3]_B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \; [a]_B = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix}$$

(For the last matrix, note that: $aw = w, av_2 = v_3, av_3 = v_1 = w - v_2 - v_3$)

Given two $F[G]$-modules, a homomorphism $\phi\colon V \longrightarrow W$ of $F[G]$-modules is what you think it is. It has a kernel and an image that are $F[G]$-submonules of V and W.

Example.

Let G be the group S_n of permutations. Let V be the permutation module for S_n and $\{v_1, \ldots, v_n\}$ a basis for V. Let $w = \sum_i v_i$ and $W = Fw$. This is a $F[G]$-module. Define a homomorphism

$$\phi\colon \sum_i \lambda_i v_i \mapsto (\sum_i \lambda_i) w$$

This is a $F[G]$-homomorphism (check !). Clearly,

$$\ker(\phi) = \{\sum \lambda_i v_i, \sum \lambda_i = 0\} \text{ and } \mathrm{im}(\phi) = W$$

We now get to the first very important result of this chapter. It says that $F[G]$-modules are semisimple.

Theorem 0.6 (Maschke's theorem)**.** *Let G be a finite group and F a field such that* $\mathrm{Char}F$ *does not divide $|G|$ (ex.* $\mathrm{Char}F = 0$*). Let V be a $F[G]$-module and U an $F[G]$-submodule. Then there is an $F[G]$-submodule W of V such that*

$$V = U \oplus W$$

In other words, $F[G]$ is a semisimple algebra.

Proof. Choose any subspace W_0 of V such that $V = U \oplus W_0$. For any $v = u + w$, define $\pi \colon V \longrightarrow V$ by $\pi(v) = u$ (i.e. π is a projection onto U). We will modify π into an $F[G]$-homomorphism. Define

$$\phi(v) = \frac{1}{|G|} \sum_{g \in G} g\pi g^{-1}(v)$$

This clearly is an F-linear morphism $V \longrightarrow V$. Furthermore, $\mathrm{im}(\phi) \subset U$ (notice that $\pi(g^{-1}v) \in U$ and as U is an $F[G]$-module, we have $g\pi(g^{-1}v) \in U$).

Claim 1. : ϕ is a $F[G]$-homomorphism.

Let $x \in G$, we need to show that $\pi(xv) = x\pi(v)$. Let, for $g \in G$, $h := x^{-1}g$ (hence $h^{-1} = g^{-1}x$). Then

$$\phi(xv) = \frac{1}{|G|} \sum_{h \in G} x(h\pi h^{-1})(v) = x \frac{1}{|G|} \sum_{h \in G} (h\pi h^{-1})(v) = x\phi(v)$$

This proves the claim.

Claim 2. : $\phi^2 = \phi$.

For $u \in U$ and $g \in G$, we have $gu \in U$, therefore $\phi(gu) = gu$. Now

$$\phi(u) = \frac{1}{|G|} \sum (g\pi g^{-1})u = \frac{1}{|G|} \sum (g\pi(g^{-1}u) = \frac{1}{|G|} \sum gg^{-1}u = \frac{1}{|G|} \sum u = u$$

Let $v \in V$, then $\phi(u) \in U$ and it follows that $\phi^2(v) = \phi(v)$, this proves the claim. We let $W := \ker(\phi)$. Then, as ϕ is a $F[G]$-homomorphism, W is a $F[G]$-module. Now, the minimal polynomial of ϕ is $x^2 - x = x(x-1)$. Hence

$$V = \ker(\phi) \oplus \ker(\phi - I) = W \oplus U$$

This finishes the proof.

$\square$

Note that without the assumption that $Char(F)$ does not divide $|G|$, the conslusion of Mashke's theorem is wrong. For example let $G = C_p = \{a : a^p = 1\}$ over $F = \mathbb{F}_p$. Then the function

$$a^j \mapsto \begin{pmatrix} 1 & 0 \\ j & 1 \end{pmatrix}$$

for $j = 0, \dots, p-1$ is a representation of G of dimension 2. We have

$$a^j v_1 = v_1 a^j v_2 = j v_1 + v_2$$

Then $U = Span(v_1)$ is a $F[G]$-submodule of V. But there is no $F[G]$-submodule W such that $V = U \oplus V$ as (easy) U is the only 1-dimensional $F[G]$-submodule of V.

Similarly, the conclusion of Maschke's theorem fails for infinite groups. Take $G = \mathbb{Z}$ and the representation

$$n \mapsto \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}$$

The proof of Maschke's theorem gives a procedure to find the complementary subspace. Let $G = S_3$ and $V = \{e_1, e_2, e_3\}$ be the permutation module. Clearly, the submodule $U = Span(v_1 + v_2 + v_3)$ is an $F[G]$-submodule. Let $W_0 = Span(v_1, v_2)$.

Then $V = U \oplus W_0$ as $\mathbb{C}$-vector spaces. The projection ϕ onto U is given by

$$\phi(v_1) = 0, \ \phi(v_2) = 0, \ \phi(v_3) = v_1 + v_2 + v_3$$

The $F[G]$-homomorphism as in the proof of Maschke's theorem is given by

$$\Phi(v_i) = \frac{1}{3}(v_1 + v_2 + v_3)$$

Clearly $\ker(\Phi) = Span(v_1 - v_2, v_2 - v_3)$. The $F[G]$-submodule is then

$$W = Span(v_1 - v_2, v_2 - v_3)$$

This is the $F[G]$-submodule such that $V = U \oplus W$. Actually, you may notice that is submodule is

$$W = \{\sum \lambda_i v_i : \sum \lambda_i = 0\}$$

By applying a theorem from the previous chapter.

Corollary 0.7. *Let G be a finite group and V a $F[G]$ module where $F = \mathbb{R}$ or $\mathbb{C}$. There exist simple $F[G]$-modules $U_1, \dots, U_r$ such that*

$$V = U_1 \oplus \cdots \oplus U_r$$

In other words, $F[G]$ modules are semisimple.

Another corollary:

Corollary 0.8. *Let V be an $F[G]$-module,* Char$F$ *does not divide $|G|$. Let U be an $F[G]$ submodule of V. There is a* surjective *$F[G]$ homomorphism $V \longrightarrow U$.*

Proof. By Mascke's theorem there is an $F[G]$-submodule W such that $V = U \oplus W$. Consider $\pi\colon u + w \mapsto u$. □

We can now state Shur's lemma for $F[G]$-modules:

Theorem 0.9 (Schur's lemma)**. Suppose that F is algebraically closed.**

Let V and W be simple *$F[G]$-modules.*

1. *If $\phi\colon V \longrightarrow W$ is a $F[G]$-homomorpism, then either ϕ is a $F[G]$-isomorphism or $\phi(v) = 0$ for all $v \in V$.*
2. *If $\phi\colon V \longrightarrow W$ is a $F[G]$-isomorpism, then ϕ is a scalar multiple of the identity endomorphim I_V.*

This gives a **characterisation** of simple $F[G]$-modules and it is also a partial converse to Shur's lemma.

Proposition 0.10. *Suppose* Char$F$ *does not divide $|G|$ Let V be a non-zero $F[G]$-module and suppose that every $F[G]$-homomorphism from V to V is a scalar multiple of I_V. Then V is simple.*

Proof. Suppose that V is reducible, then by Maschke's theorem, we have

$$V = U \oplus W$$

where U and W are $F[G]$-submodules. The projection onto U is a $F[G]$-homomorphism which is not a scalar multiple of I_V (it has a non-trivial kernel !). This contradicts the assumtion. □

We now apply Shur's lemma to classifying representations of abelian groups.

In what follows, the field F is $\mathbb{C}$.

Let G be a finite abelian group and V a simple $\mathbb{C}[G]$-module. As G is abelian, we have

$$xgv = g(xv), x, g \in G$$

Therefore, $v \mapsto xv$ is a $\mathbb{C}[G]$-homomorphism $V \longrightarrow V$. As V is irreducible, Shur's lemma imples that there exists $\lambda_x \in \mathbb{C}$ such that $xv = \lambda_x v$ for all V. In particular, this implies that every subspace of V is a $\mathbb{C}[G]$-module. The fact that V is simple implies that $\dim(V) = 1$. We have proved the following:

Proposition 0.11. *If G is a finite abelian group, then every simple $\mathbb{C}[G]$-module is of dimension one.*

The basic structure theorem for finite abelian groups is the following:

Theorem 0.12 (Structure of finite abelian groups)**.** *Every finite abelian group G is a direct product of cyclic groups.*

Let

$$G = C_{n_1} \times \cdots \times C_{n_r}$$

and let c_i be a generator for C_{n_i} and we write

$$g_i = (1, \ldots, 1, c_i, 1, \ldots, 1)$$

Then

$$G =< g_1, \ldots, g_r >, g^{n_i} = 1, g_i g_j = g_j g_i$$

Let $\rho\colon G \longrightarrow \mathrm{GL}_n(\mathbb{C})$ be an irreducible representation of G. We know that $n = 1$, hence $\mathrm{GL}_n(\mathbb{C}) = \mathbb{C}^*$. There exist $\lambda_i \in \mathbb{C}$ such that

$$\rho(g_i) = \lambda_i$$

The fact that g_i has order n_i implies that $\lambda_i^{n_i} = 1$.

This completely determines ρ. Indeed, let $g = g_1^{i_1} \cdots g_r^{n_r}$, we get

$$\rho(g) = \lambda_1^{i_1} \cdots \lambda_r^{i_r}$$

As ρ is completely determined by the λ_i, we write

$$\rho = \rho_{\lambda_1, \ldots, \lambda_r}$$

We have shown:

Theorem 0.13. *Let $G = C_{n_1} \times \cdots \times C_{n_r}$. The representations $\rho_{\lambda_1, \ldots, \lambda_r}$ constructed above are irreducicible and have degree one. There are exactly $|G|$ of these representations.*

Let us look at a few examples. Let $G = C_n = \{a : a^n = 1\}$ and let $\zeta_n = e^{2\pi i/n}$. The n irreducible representations of G are the

$$\rho_{\zeta_n^i}(a^k) = \zeta_n^k$$

where $0 \leq k \leq n-1$.

Let us classify all irreducible representations of $G = C_2 \times C_2 =< a_1, a_2 >$. There are four of them, call them V_1, V_2, V_3, V_4 where V_i is a one dimensional vector space with basis v_i. We have

$$\begin{array}{cc} a_1 v_1 = v_1 & a_2 v_1 = v_1 \\ a_1 v_2 = v_2 & a_2 v_2 = -v_2 \\ a_1 v_3 = -v_3 & a_2 v_3 = v_3 \\ a_1 v_4 = -v_4 & a_2 v_4 = -v_4 \end{array}$$

Let us now turn to not necessarily irreducible representations. Let $G =< g >$ be a cyclic group of order n and V a $\mathbb{C}[G]$-module. Then V decomposes as

$$V = U_1 \oplus \cdots \oplus U_r$$

into a direct sum of irreducible $\mathbb{C}[G]$-modules. We know that every U_i has dimension one and we let u_i be a vector spanning U_i. As before we let $\zeta_n = e^{2\pi i/n}$. Then for each i there exists an integer m_i such that

$$gu_i = \zeta_n^{m_i} u_i$$

Let $B = \{u_1, \dots, u_r\}$ be the basis of V consisting of the u_i. Then the matrix $[g]_B$ is diagonal with coefficients $\zeta_n^{m_i}$.

As an exercise, the reader will classify representations of arbitrary finite abelian groups (i.e products of cyclic groups).

The statement that all irreducible representations of abelian groups have degree one has a converse.

Theorem 0.14. *Let G be a finite group such that all irreducible representations of G are of degree one. Then G is abelian.*

Proof. We can write

$$\mathbb{C}[G] = U_1 \oplus \cdots \oplus U_n$$

where each U_i is simple and hence is of degree one by assumption. Let u_i be a generator of U_i, then $\{u_1, \dots, u_n\}$ is a basis of $\mathbb{C}[G]$ as a $\mathbb{C}$-vector space.

Let g be in $\mathbb{C}[G]$, then the matrix of the action of g on $\mathbb{C}[G]$ in this basis is diagonal (because U_is are $\mathbb{C}[G]$-modules !). The regular representation of G (action of G on $\mathbb{C}[G]$ given by multiplication in G) is faithful.

Indeed, suppose $g\sum(\lambda_h h) = \sum \lambda_h h$ for all $\sum \lambda_h h \in \mathbb{C}[G]$. Then, in particular $g \cdot 1 = 1$ hence $g = 1$.

It follows that the group G is realised as a group of diagonal matrices. Diagonal matrices commute, hence G is abelian. $\square$

1. $\mathbb{C}[G]$ as a module over itself.

In this section we study the structure of $\mathbb{C}[G]$ viewed as a module over itself. We know that $\mathbb{C}[G]$ decomposes as

$$\mathbb{C}[G] = U_1 \oplus \cdots \oplus U_r$$

where the U_is are irreducible $\mathbb{C}[G]$-submodules.

As by Mashke's theorem $\mathbb{C}[G]$ is a semisimple algebra, U_is are the only simple $\mathbb{C}[G]$-modules.

Then we have seen that *every* irreducible $\mathbb{C}[G]$-module is isomorphic to one of the U_is. In particular there are only finitely many of them.

Let's look at examples.

Take $G = C_3 = \{a : a^3 = 1\}$ and let $\omega = e^{2i\pi/3}$. Define

$$v_0 = 1 + a + a^2$$
$$v_1 = 1 + \omega^2 a + \omega a^2$$
$$v_3 = 1 + \omega a + \omega^2 a^2$$

Let $U_i = Span(v_i)$. One checks that

$$av_i = \omega^i v_i$$

and U_is are $\mathbb{C}[G]$-submodules. It is not hard to see that v_1, v_2, v_3 form a basis of $\mathbb{C}[G]$ and hence

$$\mathbb{C}[G] = U_0 \oplus U_1 \oplus U_2$$

direct sum of irreducible $\mathbb{C}[G]$-modules.

Look at D_6. It contains $C_3 =< a >$. Define:

$$v_0 = 1 + a + a^2, \quad w_0 = v_0 b$$
$$v_1 = 1 + \omega^2 a + \omega a^2, \quad w_1 = v_1 b$$
$$v_3 = 1 + \omega a + \omega^2 a^2, \quad w_2 = v_2 b$$

As before, $< v_i >$ are $< a >$-invariant and

$$av_0 = v_0, \; aw_0 = v_0$$
$$bv_0 = w_0, \; bw_0 = v_0$$

It follows that $Span(u_0, w_0)$ is a $\mathbb{C}[G]$ modules. It is not simple, indeed, it is the direct sum $U_0 \oplus U_1$ where $U_0 = Span(u_0 + w_0)$ and $U_1 = Span(u_0 - w_1)$ and they are simple submodules.

Notice that the irreducible representation of degree one corresponding to U_0 is the trivial one : sends a and b to 1. The one corresponding to U_1 sends a to 1 and b to -1.

Next we get :

$$av_1 = \omega w_2, \; aw_2 = \omega^2 w_2$$
$$bv_1 = w_2, \; bw_2 = v_1$$

Therefore $U_2 = Span(v_1, w_2)$ is $\mathbb{C}[G]$-module. It is an easy exercise to show that it is irreducible.

The corresponding two-dimensional representation is

$$a \mapsto \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}$$

and

$$b \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Lastly

$$av_2 = \omega^2 w_1, \ aw_1 = \omega w_1$$
$$bv_2 = w_1, \ bw_1 = v_2$$

Hence $U_3 = Span(v_2, w_1)$ is a $\mathbb{C}[G]$-module and one shows that it is irreducible. In fact the morphism ϕ that sends $v_1 \longrightarrow w_1$ and $w_2 \longrightarrow v_2$ is $\mathbb{C}[G]$-isomorphism (you need to chack that $\phi(av) = a\phi(v)$ and $\phi(bv) = b\phi(v)$ for all $v \in \mathbb{C}[G]$).

Therefore the representations U_2 and U_3 are isomorphic. We have

$$\mathbb{C}[G] = U_0 \oplus U_1 \oplus U_2 \oplus U_3$$

with $\dim U_0 = \dim U_2 = 1$ and corresponding representations are non-isomorphic. And $\dim U_2 \cong \dim U_3 = 2$ and the corresponding representations are isomorphic.

We have completely classified all irreducible representations of $\mathbb{C}[D_6]$ and realised them explicitly as sumbmodules of $\mathbb{C}[D_6]$.

1.1. **Wedderburn decomposition revisited.** We now apply the results we proved for semisimple modules to the group algebra $\mathbb{C}[G]$. View $\mathbb{C}[G]$ as a module over itself (regular module). By Maschke's theorem, this module is semisimple. There exist r distinct simple modules S_i and integers n_i such that

$$\mathbb{C}[G] = S_1^{n_1} \oplus \cdots \oplus S_r^{n_r}$$

We have

$$\mathbb{C}[G]^{op} = \mathrm{End}_{\mathbb{C}[G]}(\mathbb{C}[G]) = M_{n_1}(\mathrm{End}(S_1)) \oplus \cdots \oplus M_{n_r}(\mathrm{End}(S_r))$$

As S_i is simple and $\mathbb{C}$ is algebraically closed, $\mathrm{End}(S_i) = \mathbb{C}$. By taking the opposite algebra, we get

$$\mathbb{C}[G] = M_{n_1}(\mathbb{C}) \oplus \cdots \oplus M_{n_r}(\mathbb{C})$$

(note that $\mathbb{C}^{op} = \mathbb{C}$ because $\mathbb{C}$ is commutative.)

Each S_i becomes a $M_{n_i}(\mathbb{C})$-module. Indeed, S_i is a $\mathbb{C}[G] = M_{n_1}(\mathbb{C}) \oplus \cdots \oplus M_{n_r}(\mathbb{C})$-module and $M_{n_i}(\mathbb{C})$ is a subalgebra of $\mathbb{C}[G]$. As a $M_{n_i}(\mathbb{C})$-module, S_i is also simple. Indeed, suppose that S_i' is a non-trivial $M_{n_i}(\mathbb{C})$-submodule of S_i. Then, $0 \oplus \cdots 0 \oplus S_i' \oplus \cdots \oplus 0$ is a non-trivial $\mathbb{C}[G]$-submodule of S_i.

We have seen in the previous chapter that simple $M_{n_i}(\mathbb{C})$-modules are isomorphic to $\mathbb{C}^{n_i}$ (column vector modules). It follows that $\dim_{\mathbb{C}}(S_i) = n_i$ and as $\dim_{\mathbb{C}} \mathbb{C}[G] = |G|$, we get the following very important relation

$$|G| = \sum_{i=1}^{r} n_i^2$$

The integers n_is are precisely the degrees of all possible irreducible representations of G.

In addition, for any finite group there is always an irreducible one dimensional representation : the trivial one. Therefore we always have $n_1 = 1$.

Using this relation we already can determine the degrees of all irreducible representations of certain groups. For abelian groups they are always one.

For D_6 : $6 = 1 + 1 + 2^2$. We recover what we proved above.

For D_8 we have $8 = 1 + 1 + 1 + 1 + 2^2$ hence four one-dimensional ones (exercise : determine them) and one two dimensional (determine it !).

Same for Q_8.

We will now determine the integer r : the number of isomorphism classes of irreducible representations.

Definition 1.1. *Let G be a finite group. The centre $Z(\mathbb{C}[G])$ of the group algebra $\mathbb{C}[G]$ is defined by*

$$Z(\mathbb{C}[G]) = \{z \in \mathbb{C}[G] : zr = rz \text{ for all } r \in \mathbb{C}[G]\}$$

The centre $Z(G)$ of the group G is defined similarly:

$$Z(G) = \{g \in G : gr = rg \text{ for all } r \in G\}$$

We have:

Lemma 1.1.

$$\dim Z(\mathbb{C}[G]) = r$$

Proof. Write $\mathbb{C}[G] = M_{n_1}(\mathbb{C}) \oplus \cdots \oplus M_{n_r}(\mathbb{C})$. Now, the centre of each $M_{n_i}(\mathbb{C})$ is $\mathbb{C}$ and there are r factors, hence $Z(\mathbb{C}[G]) = \mathbb{C}^r$. □

Recall that a conjugacy class of $g \in G$ is the set

$$\{x^{-1}gx : x \in G\}$$

and G is a disjoint union of conjugacy classes.

We show:

Theorem 1.2. *The number r of irreducible representations is equal to the number of conjugacy classes.*

Proof. We calculate the dimension of $Z(\mathbb{C}[G])$ in a different way. Let $\sum_{g\in G} \lambda_g g$ be an element of $Z(\mathbb{C}[G])$. By definition, for any $h \in G$ we have

$$h(\sum_{g\in G} \lambda_g g)h^{-1} = \sum_{g\in G} \lambda_g g$$

We have

$$h(\sum_{g\in G} \lambda_g g)h^{-1} = \sum_{g\in G} \lambda_{hgh^{-1}} g$$

Therefore $\lambda_g = \lambda_{hgh^{-1}}$ and therefore the function λ_g is constant on conjugacy classes. Hence the centre is generated by the

$$\{\sum_{g\in K} g : K \text{ conjugacy class}\}$$

But this family is also free because conjugacy classes are disjoint hence it is a basis for $Z(\mathbb{C}[G])$. This finishes the proof. $\square$

For example we recover the fact that irreducible representations of abelian groups are one dimensional : each conjugacy class consists of one element.

By what we have seen before, we know that D_6 has three conjugacy classes, D_8 has five.

1.2. **Conjugacy classes in dihedral groups.** We can in fact determine completely conjugacy classes in dihedral groups.

Let G be a finite group and for $x \in G$, let us denote by x^G the conjugacy class of x. Let

$$C_G(x) = \{g \in G : gx = xg\}$$

This is a subgroup of G called the centraliser of x. We have

$$|x^G| = |G : C_G(x)| = \frac{|G|}{|C_G(x)|}$$

We have the followin relation (standard result in group theory). Let $x_1, \ldots, x_m$ be representatives of conjugacy classes in G.

$$|G| = |Z(G)| + \sum_{x_i \notin Z(G)} |x_i^G|$$

Let us now turn to the dihedral group

$$G = D_{2n} = \{a, b : a^n = b^2 = 1, b^{-1}ab = a^{-1}\}$$

Suppose that n is odd.

Consider a^i for $1 \leq i \leq n-1$. Then $C(a^i)$ contains the group generated by a: obviously $aa^ia^{-1} = a^i$. It follows that

$$|a^G| = |G : C_G(a)| \leq 2 = |G :< a > |$$

On the other hand $b^{-1}a^ib = a^{-i}$ so $\{a^i, a^{-i}\} \subset {a^i}^G$. As n is odd $a^i \neq a^{-i}$ ($a^{2i} = 1$ implies that $n = 2i$ but n is odd).

It follows that $|{a^i}^G| \geq 2$ hence

$$|{a^i}^G| = 2 \ C_G(a^i) =< a > \ \ {a^i}^G = \{a^i, a^{-i}\}$$

Next $C_G(b)$ contains 1 and b. As $b^{-1}a^ib = a^{-i}$ and $a^i \neq a^{-i}$, therefore a^i and a^ib do not commute with b. Therefore $C_G(b) = \{1, b\}$. It follows that $|b^G| = n$ and we have

$$b^G = \{b, ab, \ldots, a^{n-1}b\}$$

(notice that all elements of G are $\{1, a, a^2, \ldots, a^{n-1}, b, ab, \ldots, a^{n-1}b\}$)

We have determined all conjugacy classes in the case n is odd.

Proposition 1.3. *The dihedral group D_{2n} with n odd has exactly $\frac{n+3}{2}$ conjugacy classes and they are*

$$\{1\}, \{a, a^{-1}\}, \ldots, \{a^{(n-1)/2}, a^{-(n-1)/2}\}, \{b, ab, \ldots, a^{n-1}b\}$$

Suppose $n = 2m$ is even.

We have $a^m = a^{-m}$ such that $b^{-1}a^mb = a^{-m} = a^m$ and the centraliser of a^m contains both a and b, hence

$$C_G(a^m) = G$$

The conjugacy class of a^m is just a^m.

As before ${a^i}^G = \{a^i, a^{-i}\}$ for $1 \leq i \leq m-1$.

We have

$$a^jba^{-j} = a^{2j}b, \ a^jba^{-j} = a^{2j+1}b$$

It follows that

$$b^G = \{a^{2j}b : 0 \leq j \leq m-1\} \text{ and } (ab)^G = \{a^{2j+1}b : 0 \leq j \leq m-1\}$$

We proved:

Proposition 1.4. *In D_{2n} for $n = 2m$ even, there are exactly $m+3$ conjugacy classes, they are*

$$\{1\}, \{a^m\}, \{a^i, a^{-i}\} \text{ for } 1 \leq i \leq m-1,$$
$$\{a^{2j}b : 0 \leq j \leq m-1\} \text{ and } (ab)^G = \{a^{2j+1}b : 0 \leq j \leq m-1\}$$

In particular, we know the number of all irreducible representations of D_{2n}.