CHAPTER I: STRUCTURE THEOREMS FOR ARTINIAN ALGEBRAS

1. Introduction

We are concerned in this chapter with collecting various results about rings and their modules which will be needed in the course of this book. Our rings will all be unitary, and our modules will be, unless otherwise stated, finitely generated left ideals over the ring.

We will not give these results for arbitrary rings but rather for rings with are *left Artinian*, i.e., which have no infinite descending chains of left ideals. The basic example of a left Artinian ring is a finite dimensional algebra A over a field k. Since each ideal is a subvector space, the length of any descending chain of left ideals is bounded by the dimension of A over k.

2. Wedderburn's Theorem

For this section, let A be a unitary, left Artinian ring. For any module M over A, the socle $\operatorname{Soc}(M)$ is the submodule generated by all the simple submodules, i.e., all submodules with no non-trivial submodules. The module is called *semisimple* if $M = \operatorname{Soc}(M)$.

The Jacobson radical of a left Artinian ring A is the minimal two-sided ideal $\operatorname{Rad}(A)$ in A such that $A/\operatorname{Rad}(A)$ is semi-simple as a left module over itself. We wish to understand the structure of A in terms of $A/\operatorname{Rad}(A)$ and $\operatorname{Rad}(A)$. We begin with the structure theory of the semisimple part:

Theorem 2.1. *(Wedderburn-Artin)If R is left Artinian ring which is semisimple as a module over itself, then*

$$R = \bigoplus_{i=1}^{t} M_{n_i}(D_i),$$

where each D_i is a division ring which arises as the endomorphism ring of the unique simple module associated with the matrix block M_{n_i}. If R is simple as a ring, i.e., has no non-trivial two-sided ideals, then $t = 1$ and

$$R = M_n(D).$$

We now consider the radical in greater detail.

Definition 2.1. A primitive ideal of a ring A is the annihilator of a simple module M.

Definition 2.2. For any ring A, $\operatorname{Rad}(A)$ is the intersection of all primitive ideals.

Remark 2.1. Every maximal left ideal contains a primitive ideal, and one can show that $\operatorname{Rad}(A)$ is the intersection of all maximal left ideals.

Example 2.1. The behavior of the radical in the non-Artinian case is very different from the Artinian case. For example, the ring of integers $\mathbb{Z}$ is a non-Artinian ring. It has simple quotient modules but no simple submodules, and thus $\operatorname{Soc}(\mathbb{Z}) = 0$, so $\mathbb{Z}$ is not semisimple. $\operatorname{Rad}(\mathbb{Z}) = 0$ since the maximal (left) ideal are generated by the primes and no element is divisible by every prime. Thus we surely do not have $\mathbb{Z}/\operatorname{Rad}(\mathbb{Z})$ semisimple.

Lemma 2.1. *If A is a left Artinian ring, then*

(1) $\operatorname{Rad}(A) = \{a \in A | aS = 0 forallsimpleS\}$
(2) $\operatorname{Rad}(A)$ *is the maximal nilpotent ideal,*
(3) $\operatorname{Rad}(A)$ *is the minimal ideal J such that A/J is semisimple.*

Definition 2.3. For any A module M,

$$\operatorname{Rad}(M) = \operatorname{Rad}(A)M.$$

Lemma 2.2. *If A is left Artinian and M is a module over A, then* $\operatorname{Rad}(M)$ *is*

(1) *The minimal submodule such that $M/\operatorname{Rad}(M)$ is semisimple,*
(2) *the intersection of all maximal submodules*

Corollary 2.2.1. *Any module annihilated by* $\operatorname{Rad}(A)$ *is semisimple.*

For a left Artinian ring A there is a duality between the maximal semisimple quotient and the maximal semisimple submodule, i.e., the socle.

Lemma 2.3. *Let M be a module over a left Artinian ring A. Then* $\operatorname{Soc}(M)$ *is*

(1) *the maximal semisimple submodule,*
(2) *the sum of all minimal submodules.*

Definition 2.4. Let M be a module over a left Artinian ring. The *top* of M is

$$\operatorname{Top}(M) = M/\operatorname{Rad}(M).$$

Thus $\operatorname{Top}(M)$, as the maximal semisimple quotient, is dual to $\operatorname{Soc}(M)$, the maximal semisimple submodule.

The top of any nonzero module is nonzero, a result known as Nakayama's lemma. This is true for a module over any ring, but the proof is particularly simple when the ring is left Artinian, so we restrict ourselves to that case:

Lemma 2.4. *(Nakayama's lemma) If M is a module over a left Artinian ring A, then if*

$$\mathrm{Rad}(A)M = M,$$

we have that

$$M = 0.$$

Proof. Since A is left Artinian, $\mathrm{Rad}(A)$ is nilpotent, so there exists an integer n with $\mathrm{Rad}^n(A) = 0$. Then

$$M = \mathrm{Rad}(A)M = \mathrm{Rad}^2(A)M = \dots \mathrm{Rad}^n(A)M = 0.$$

□

As Example 2.1 of $\mathbb{Z}$ shows, in a general ring we do not have a dual result that the socle is nonzero. However, for a left Artinian ring we *do* have this dual result:

Lemma 2.5. *If M is a module over a left Artinian ring A such that $\mathrm{Soc}(M) = 0$, then $M = 0$.*

Proof. We prove the contrapositive. Suppose that $M \neq 0$. Since $\mathrm{Rad}(A)$ is nilpotent, there is a minimal i such that $\mathrm{Rad}(A)^i M = 0$, and since M is nonzero, $i \geq 1$. Then

$$\mathrm{Rad}(A)^{i-1}M$$

is annihilated by $\mathrm{Rad}(A)$ and is thus semisimple, so by the minimality of i, $\mathrm{Soc}(M)$, which contains this semisimple submodule, is nonzero. When $i = 1$, we let $\mathrm{Rad}^0(A) = A$. □

Both the radical and the socle behave well with respect to direct sums:

$$\mathrm{Rad}(\bigoplus M_i) = \bigoplus \mathrm{Rad}(M_i),$$

$$\mathrm{Soc}(\bigoplus M_i) = \bigoplus \mathrm{Soc}(M_i).$$

The duality can be extended further, by defining the radical series and the socle series.

Definition 2.5. Let $\mathrm{Rad}^0(M) = M$, let $\mathrm{Rad}^1(M) = \mathrm{Rad}(M)$ and recursively set

$$\mathrm{Rad}^{i+1}(M) = \mathrm{Rad}(\mathrm{Rad}^i(M)) = (Rad(a)^{i+1}M.$$

Let $\mathrm{Soc}^0(M) = 0$, let $\mathrm{Soc}^1(M) = \mathrm{Soc}(M)$ and recursively set

$$\mathrm{Soc}^{i+1}(M) = \{a \in M | a + \mathrm{Soc}^i(M) \in \mathrm{Soc}(M/\mathrm{Soc}^i(M))\}$$

Remark 2.2. It is clear from the definition that $\mathrm{Rad}^i(M)$ is a decreasing sequence of submodules which, since $\mathrm{Rad}(A)$ is nilpotent, stabilizes at zero. Each quotient of adjacent modules is semisimple. Dually,

$$\mathrm{Soc}(M) \subseteq \mathrm{Soc}^2(M) \subseteq \dots \mathrm{Soc}^r(M),$$

and each quotient of adjacent modules is semisimple. Since A is left Artinian it is also left Noetherian, and thus this ascending sequence stabilizes eventually, at $\mathrm{Soc}^R(M)$ for some natural number r. Since $M/\mathrm{Soc}^r(M)$ has a zero socle, it must by zero by Lemma 2.5, so the sequence stabilizes with

$$\mathrm{Soc}^r(M) = M$$

.

We now give an example with a commutative ring.

Example 2.2. Let k be a field and suppose $A = k[x]/(x^2) \oplus k[y]/(y^3)$. Consider A as a left module over itself. Then

$$\mathrm{Rad}(A) = (x) \oplus (y), \mathrm{Rad}^2(A) = (y^2), \mathrm{Rad}^3(A) = 0,$$

and

$$\mathrm{Soc}(A) = (x) \oplus (y^2), \mathrm{Soc}^2(A) = k[x]/(x^2) \oplus (y), \mathrm{Soc}^3(A) = A.$$

Claim 1. *Let M be a module over a left Artinian ring A. If r is the smallest integer such that $\mathrm{Soc}^r(M) = M$, then we always have $\mathrm{Rad}^i(M) \subseteq \mathrm{Soc}^{r-i}(M)$. Furthermore, $\mathrm{Rad}^i(M) \nsubseteq \mathrm{Soc}^{r-i-1}(M)$ if $i < r$, and thus $\mathrm{Rad}^{r-1}(M) \neq 0$, while $\mathrm{Rad}^r(M) = 0$.*

Proof. Since $\mathrm{Rad}(A)$, by Lemma 2.1, annihilates all simple modules and thus anhiliates the socle, we always have

$$\mathrm{Rad}(A)\,\mathrm{Soc}^j(M) \subseteq \mathrm{Soc}^{j-1}(M).$$

When $j = r$, this means that

$$\mathrm{Rad}(M) \subseteq \mathrm{Soc}^{r-1}(M),$$

and by descending induction on j, we get the first part of the claim for all $i = j - r + 1$. As for the second part of the claim, when $i = 0$, we have that $\mathrm{Rad}^0 = M$, and $\mathrm{Soc}^{r-1}(M) \nsubseteq M$ by the minimality of r. Now proceed by induction on i, assuming that $\mathrm{Rad}^i(M) \nsubseteq \mathrm{Soc}^{r-i-1}(M)$ and $i < r - 1$. Since $\mathrm{Rad}^i(M)$ is nonzero, then by Nakayama's lemma, $\mathrm{Rad}^i(M)/\mathrm{Rad}^{i+1}(M)$ is nonzero. Thus there is a submodule N_i of $\mathrm{Rad}^i(M)$ which is a complement of $\mathrm{Soc}^{r-i-1}(M) \cap \mathrm{Rad}^i(M)$, modulo Rad^{i+1}. Clearly, $\mathrm{Rad}(A)N_i \subseteq \mathrm{Rad}^{i+1}(M)$. However, it is not contained in $\mathrm{Soc}^{r-i-2}(M)$, for if it were, then $N_i + \mathrm{Soc}^{r-i-2}(M)$ would be annihilated by $\mathrm{Rad}(A)$ modulo $\mathrm{Soc}^{r-i-2}(M)$ and thus would, by definition, lie in $\mathrm{Soc}^{r-i-1}(M)$, in contradition to the choice of N_i. □

Definition 2.6. The natural number r which is the common length of the radical series and the socle series is called the *Loevy length* of the module.

Exercises:

(1) Find the radical series and the socle series for T^n, the upper triangular $n \times n$ matrices over $\mathbb{C}$. Verify that

$$\operatorname{Rad}^i(T^n) \subseteq \operatorname{Soc}^{n-i}(T^n)$$

(2) Find the radical series and the socle series for $\mathbb{Z}_{72}$. (Hint: First use the Chinese Remainder Theorem to split the ring into a direct sum.)

3. The Jordan-Holder theorem

One of the fundamental concepts of module theory is that a module is build up out of simple modules. We have already seen, in our discussion of the radical series, that we can find a descending sequence of submodules such that the quotients are all semisimple. Similarly the socle series also provides a descending sequence of submodules whose quotients are semisimple, and there are many other possible sequences. Furthermore, any such sequence of submodules can be "refined", by inserting intermediate submodules, to a sequence in which each quotient is actually simple, again in many possible ways. The point to the Jordan-Holder theorem is that if we consider the totality of simple quotients for such a refined sequence, the multiplicity of each simple is independent of various choices.

The original theorem was a theorem about groups, and the original proof was based on a theorem of Schreier, that any two descending normal sequences can be refined to sequences of the same length with the same quotients. A version of the Schreier theorem can be proven for modules, and used to prove the Jordan-Holder theorem for modules, which we give here in the version suitable for modules over a left Artinian ring.

Theorem 3.1. *(Jordan-Holder) Let A be a left Artinian ring, and M a finitely generated modules. Then there is a finite descending sequence of submodules, called a composition series, such that each quotient is a simple module. The factors, called the composition factors of M, are independent of the choice of composition series.*

Example 3.1. If G is an abelian group of order n, then G can be regarded as a module for the Artinian ring $\mathbb{Z}_n$, since any element is annihilated by n. The composition factors for G are all of the form $\mathbb{Z}_p$, for $p|n$, and each factor occurs with a multiplicity equal to the multiplicity of p as a factor of n.

Exercises:

(1) A finite group is called solvable of its composition factors are all cyclic groups of order p. Every group of order less than 100 is solvable except A_5. Prove that the composition factors of a solvable group depend only on the order of the group, without regard to its structure.

(2) Find the composition factors of the group A_4.
(3) Find the composition factors of the ring $A = k[x]/(x^2) \bigoplus k[y]/(y^3)$ as a module over itself. (Hint: first divide by $\mathrm{Rad}(A)$ to find the simple modules.)

4. The Krull-Schmidt Theorem

We now want to break up our modules into the smallest units which can be treated as independent entities. The result quoted earlier in Section 2, that the socle and the radical can be calculated separately for each direct summand of a module, can serve as an indicator of the direction in which we want to move. We want to break up each module into the smallest possible direct summands.

Definition 4.1. A module M over a ring A is *decomposable* if

$$M \tilde{\to} M_2 \oplus M_2,$$

i.e., M is an internal direct sum of two submodules M_1 and M_2. The module is *indecomposable* if it is not decomposable.

For a finitely-generated module over a left Artinian ring, there is a simple theoretical procedure for breaking it up into its indecomposable direct summands: inductively subdivide each decomposable summand until all summands are indecomposable. The procedure ends after a finite number of steps because a finitely generated module over a left Artinian ring satisfies the descending chain condition and thus cannot have an infinite descending sequence of direct summands. In practical calculation it is often quite a difficult matter to break up a module into its indecomposable summands; for large modules this is frequently done by "brute force" using computer calculation. However, for theoretical considerations it usually suffices to know that the decomposition exists, even if one cannot readily display it. Not only does it exist, but it is, as the following theorem shows, essentially unique:

Theorem 4.1. *(Krull-Schmidt) Let A be a left Artinian ring, and M a finitely-generated module over A. The there is a decomposition of M as a direct sum of a finite number of indecomposable submodules,*

$$M = U_1 \oplus \cdots \oplus U_r.$$

Furthermore, if

$$M = V_1 \oplus \cdots \oplus V_s$$

is another decomposition, then $r = s$ and the factors, after permutation, will be isomorphic.

The representation theory of an Artinian ring A is the study of its finitely-generated modules, and the module homomorphisms between them. It is well-known that homomorphisms of modules behave extremely well with regard to direct sums: If $M = \bigoplus M_j$ and $N = \bigoplus N_j$ then

$$\mathrm{Hom}_A(M, N) = \bigoplus_i \bigoplus_j \mathrm{Hom}_A(M_i, N_j).$$

Thus the general study of homomorphisms between modules can be reduced to a study of homomorphism between summands.

The first step in breaking up a module into its indecomposable direct summands is to break up the ring A into its indecomposable subrings, called its *blocks*. The existence of such a decomposition is in fact a consequence of Theorem 4.1. We have had frequent occasion to consider A as a left module over itself, and we could, dually, have considered A as a right module over itself. However, considering the right module action of A on itself is equivalent to considering the action of the opposite algebra A^{op} on the left. The elements in the opposite algebra are the same with the multiplication reversed, i.e., $b \star a = ab$, and thus, if $a \in A$ and $b, c \in A^{op}$ we have the necessary module condition that

$$(c \star b) \cdot a = a(bc) = (ab)c = c \cdot (b \cdot a).$$

The separate left actions of A and A^{op} can be combined into one left action by the direct product ring $A \times A^{op}$.

When A is an algebra over a commutative ring R, which acts the same from the left and from the right, we can consider A as a left module for the tensor product ring $A \otimes_R A^{op}$, which is sometimes call the *enveloping algebra*. In fact, any ring is an algebra over $R = \mathbb{Z}$, so we will usually work with the tensor product rather than the direct product.

Just as the submodules of A under the left action of A on itself are left ideals, so the submodules of A under the action of $A \otimes_R A^{op}$ are (two-sided) ideals. If we apply Theorem 4.1 to A as a module over its enveloping algebra, then

$$A = \bigoplus_{i=1}^{t} B_i,$$

where the B_i are ideals. Each B_i is thus a subalgebra of A, since it is isomorphic to the quotient

$$A / \bigoplus_{j \neq 1} B_j.$$

Thus the *blocks* of A are its indecomposable subalgebras.

To each subalgebra B_i is associated its identity element e_i. As an element of A, e_i is an idempotent, i.e., $e_i \cdot e_i = e_i$. Because of the direct sum, the distinct idempotents are orthogonal, $e_i \cdot e_j = 0$ for $j \neq i$. This then implies that each e_i lies in the center $Z(A)$ of the ring A, since, as identity element, it commutes with every element of B_i and it annihilates every element of B_j of every $j \neq i$.

Definition 4.2. An idempotent e_i in a ring A is called *centrally primitive* if it lies in $Z(A)$ and it cannot be written as the sum of two orthogonal central idempotents.

This should be distinquished carefully from the following concept:

Definition 4.3. An idempotent e_i in a ring A is called *primitive* if it cannot be written as the sum of two orthogonal idempotents.

A centrally primitive idempotent is not necessary primitive, as Example 4.3 below will show.

Definition 4.4. A set of orthogonal idempotents is called *complete* if the sum of all the idempotents is the identity.

Before we return to the study of indecomposable modules over A there is one more important point to make about the centrally primitive idempotents. If 1_A is the identity element of the unitary ring A, then the sset of centrally primitive idempotents is complete, i.e.,

$$1_A = \sum_{i=1}^{t} e_i.$$

A decomposition of the ring A induces a decomposition of all the modules. Assume that we have decomposed A into blocks B_i as above, with centrally primitive idempotents e_i, and let M be any A-module. for any $m \in M$ we have

$$m = 1_A \cdot m = \sum_{i=1}^{t} e_i \cdot m.$$

Thus we in fact have a direct sum decomposition of M into submodules e_iM, each of which is a module for the subalgebra B_i. Let us denote e_iM by M_i.

Lemma 4.1. *Let M and N be modules over an Artin ring A, which has a decomposition into blocks as $A = \bigoplus B_i$. If $i \neq j$, then*

$$\mathrm{Hom}_A(M_i, N_j) = 0.$$

Thus

$$\mathrm{Hom}_A(M, N) = \bigoplus \mathrm{Hom}_{B_i}(M_i, N_i).$$

Proof. Take $f \in \mathrm{Hom}_A(M_i, N_j)$, and $m_i = e_i \cdot m \in M_i$. Then

$$f(m_i) = f(e_i \cdot m_i) = e_i \cdot f(m_i) = e_i \cdot e_j \cdot f(m_i) = 0.$$

□

Thus the representation theory of a left Artinian ring can be reduced to considering the representation theory of each of its blocks independently. In general algebra representation theory one usually begins with an indecomposable algebra. In the representation theory of a finite group algebra, the situation is more complicated because the group ties the different blocks together, but in fact most purely representation theorectical results are usually states as results on blocks and the subject is occasionally called *block theory*.

Let us consider three standard examples, which we will use frequently in this chapter and the next.

Example 4.1. (Quotients of Euclidean rings) Let E be a Euclidean ring. Then E is commutative, it is an integral domain, and every ideal is principal. Choose an arbitrary element a of E, and let A be the quotient of E by the ideal (a) generated by a. Since E is a unique factorization domain, the element a can be written as

$$a = u \cdot p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r},$$

where u is a unit and the p_i are ireducible elements of E. The Euclidean rings we will generally use are $\mathbb{Z}$ and $k[x]$ for a field k.

The quotient ring A has only a finite number $\tau(a)$ of ideals, with

$$\tau(a) = \Pi(\alpha_i + 1),$$

and is thus clearly Artinian. Applying the Chinese Remainder Theorem for rings, we obtain a decomposition of A into blocks:

$$A = \bigoplus B_i$$

with

$$B_i \tilde{\to} \bigoplus E/(p_i)^{\alpha_i}.$$

Each subring B_i is a local commutative ring, i.e., it has a unique maximal ideal, and A itself is called semilocal, being a direct sum of local rings. Then $\mathrm{Rad}(B_i)$ is (p_i), the unique maximal ideal, and $\mathrm{Soc}(B_i)$ is $(p_i^{\alpha_i - 1})$.

Each B_i is uniserial as an ring, having a unique descending series of ideals. Every indecomposable module for B_i is isomorphic to a quotient of B_i by a power of p_i, although the proof of this highly intuitive result is not easy, being essentially equivalent to the proof that every abelian p-group is a direct sum of cyclic subgroups. Thus B_i has α_i nonzero indecomposable modules. The general modules for A will be direct sums of these indecomposables.

Example 4.2. (Upper triangular block matrices) Let n and r be integers with $n \geq r$ and let ν be a partition $(n_1, \dots, n_r)$ of n, i.e.,

$$n = n_1 + \dots + n_r.$$

Define R_ν to be the ring consisting of the upper triangular $n \times n$ matrices over a field k with blocks of dimensions $n_i \times n_i$ down the diagonal. Define an ideal J to consist of all the matricies whose entries in the diagonal blocks are all zero. Clearly $R_\nu / J = \bigoplus M_{n_i}(k)$ is semisimple. Furthmore, a careful calculations will show that $J^r = 0$. The only ideal in a left Artinian ring which is both nilpotent and has a semisimple quotient is the radical. Thus $J = \operatorname{Rad}(R_\nu)$, and the ring is left Artinian. The socle is the $n_1 \times n_r$ block matrix in the upper right hand corner. Each column of that block is a simple module of dimension n_1, and the socle is the direct sum of those columns.

The ring R_ν acts on the n-dimensional vector space $V = k^n$, viewed as a set of column matrices. Any R_ν-submodule of V is a vector subspace of V. We wish to know which of the vector subspaces of V are indecomposable R_ν-modules.

We first note that V has a decomposition as a direct sum of vector subspaces V_i of dimension n_i corresponding to the various blocks. We claim that the indecomposable submodules are all of the form

$$W_i = V_1 \oplus V_2 \oplus \cdots \oplus V_i$$

for some $i \leq r$. More generally, all indecomposable modules are isomorphic to W_i/W_j for $i > j$.

Example 4.3. Let G be any finite group, and let k be a field. The group algebra of G over k is defined in the usual way, i.e., to be a k-vector space with the elements of G as basis elements, and the multiplication extended linearly (i.e., by using the distributive law and collecting coefficients) from the multiplication in G.

Maschke's theorem states that if $char(k)$ does not divide $|G|$, then kG is semisimple. If k contains a $|G|$-th root of unity, then in fact

$$kG \tilde{\to} \bigoplus_{i=1}^{t} M_{n_i}(k),$$

where the n_i are the degrees of the irreducible representations of G. Each block has a unique indecomposable module, which is a simple module of dimension n_i. The block itself has dimension n_i^2 as a vector space over k.

If $char(k) || G|$, then the situation is much more interesting. We assume that $|G| = p^a \cdot m$, where $p = char(k)$ and (p, m). We further assume that the field k contains an m-th root of unity. If that is so, then

$$kG / \operatorname{Rad}(kG) \tilde{\to} \bigoplus_{j=1}^{s} M_{n'_j}(k),$$

and we say that k is a *splitting field* for G. Since kG is a finite dimensional algebra over a field, it is left Artinian and decomposes into a finite number of blocks.

It is possible to find an integral domain R with a unique maximal ideal m, such that $R/M \tilde{\to} k$ and the quotient field K of R has characteristic zero. This ring will have the further property that idempotents in kG lift to idempotents in RG, and that central idempotents lift uniquely to central idempotents. Let f_j be a block idempotent of kG, i.e., a centrally primitive idempotent. Thus it lifts uniquely to RG, which is a subring of KG. In KG it decomposes into a sum of centrally primitive idempotents. Thus each block idempotents of kG is the reduction modulo m of a sum of block idempotents from KG.

The procedure for finding the blocks is as follows: Let X be the $t \times t$ character table over K. (For those unfamiliar with character tables, there will be a fuller discussion of this material in a later chapter.) Let N be the diagonal matrix with the degrees n_i of the irreducible characters χ_i down the diagonal, and let M be the diagonal matrix with the number m_j of elements in conjugacy class C_j down the diagonal. Compute

$$W = N^{-1} \cdot X \cdot M.$$

(Let $\hat{C}_j \in Z(kG)$ be the sum of the elements in class C_j. Then the entry w_{ij} in W is the scalar in block $B_i \tilde{\to} M_{n_i}(K)$ to which $\hat{C}_j$ is mapped under the projection onto the ith block.)

Now reduce the matrix W modulo p, using the fact that all pth roots of unity go to 1. Each set of identical rows corresponds to a block of kG, whose dimension is the sum of the dimensions of the corresponding blocks of KG.

We now illustrate this situation for the dihedral group D_5. Let ζ be a 5th root of unity in K. Then

$$X = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 \\ 2 & A & B & 0 \\ 2 & B & A & 0 \end{bmatrix}, W = \begin{bmatrix} 1 & 2 & 2 & 5 \\ 1 & 2 & 2 & -5 \\ 1 & A & B & 0 \\ 1 & B & A & 0 \end{bmatrix},$$

where $A = \zeta + \zeta^4$ and $B = \zeta^2 + \zeta^3$.

• Case 1: $char(k) \neq 2, 3$. The degrees of the irreducible characters are (1,1,2,2), so

$$kG \tilde{\to} k \oplus k \oplus M_2(k) \oplus M_2(k).$$

The four blocks have dimensions (1,1,4,4).

• Case 2: $char(k) = 2$. The first two rows of W are identical, modulo 2, so there are now three blocks, with dimensions (2,4,4).

$$kG \tilde{\to} k[x]/(x^2) \oplus M_2(k) \oplus M_2(k).$$

• Case 3: $char(k) = 5$. In this case, $\zeta \equiv 1$ and $5 \equiv 0$, so all the rows of W reduce to (1,2,2,0), and thus there is a single block. We will only develop the language of basis graphs, which will allow us to describe the structure of this block, in the next chapter. We will mention that

$$kG / \operatorname{Rad}(kG) \tilde{\to} k \oplus k,$$

so that in this case the block idempotent e decomposes into two noncentral primitive idempotents e_1 and e_2. This decomposition is not at all unique. It is easy to find units u in kG such that $u^{-1}e_1u$ is neither equal to e_1 nor to e_2. Then

$$e = u^{-1}e_1u + u^{-1}e_2u$$

is a different decomposition of e as a sum of orthogonal primitive idempotents.

The following result is useful in constructing units with required properties:

Theorem 4.2. *(Skolem-Noether) Let k be a field, and $A = M_n(k)$ a matrix algebra over k. Then every automorphism of A is inner, i.e., it can be given as conjugation by a unit of A.*

Exercises:

(1) Consider $\mathbb{Z}_{24}$ as a module over $\mathbb{Z}_{144}$. Decompose it into a sum of indecomposable summands. For each summand M_i calculate $\mathrm{Rad}(M_i)$, $\mathrm{Soc}(M_i)$, and $\mathrm{Top}(M_i)$.

(2) Verify that the submodules W_i defined in Example 4.2 is cyclic, i.e., generated by a single element, and that any element with a non-zero component in V_i is a generator. Use this to show that the W_i are indecomposable by showing that if there is a decomposition

$$W_i = X \oplus Y,$$

then one of the two components much contain a generator of the entire module.

(3) Calculate the dimensions of the blocks of S_3 for splitting fields of characteristic 2, 3, and 5, given that

$$X = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & -1 \\ 2 & -1 & 0 \end{bmatrix}, N = diag(1,1,2), andM = diag(1,2,3).$$

(4) Consider the mapping of $M_2(k)$ to itself which sends

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \to \begin{bmatrix} d & c \\ b & a \end{bmatrix}.$$

Prove that it is an automorphism of $M_2(k)$ and calculate the unit u such the mapping is equivalent to conjugation by u.

References:

- Rowen, Chapters 13-15, 22.
- Thevenaz, Chapter 1, Section 1.