Noncommutative algebra

Aryaman Maithani

October 15, 2024

Contents

Introduction

This document is a compilation of facts about noncommutative rings. The motivation is to understand facts about finite algebras over a field, e.g., $k[G]$ for a finite group G.

The facts are stated without proofs. The sequence of the theorems may seem funny. These are *not* in logical order. For example, we begin the sections on simple and semisimple rings by stating the structure theorem for these rings. The abstract facts that follow later would then be easy consequences of the structure theorem. However, in practice, one goes the other way around in proving the structure theorem (possibly even using theorems from later subsections). The hope is that the organisation here makes it an easy reference to get to the relevant facts.

Parts I and II are definitions and theorems about general noncommutative algebra. We first begin by stating all the relevant definitions in Part I, followed by the theorems in Part II.

Part III focuses on facts about the group ring $k[G]$. The relevant definitions and notions for this object are introduced in the first section there.

Part I

Definitions

Rings throughout will be unital but not necessarily commutative. All modules will also be unital. We assume familiarity with basic notions of (left/right) artinian and noetherian rings and modules. For example, a left artinian ring is left noetherian. A module has finite length iff it is both artinian and noetherian.

For this section, A will denote an arbitrary ring.

Note that a *left* A-module M is (by definition) an abelian group M with a multiplication $A \times M \to M$ satisfying certain properties. This is precisely the data of an abelian group M and a ring homomorphism

$$\rho\colon A \to \mathrm{End}_{\mathbb{Z}}(M).$$

For this reason, we may think of ρ (or M) as a representation of A. The annihilator of M is defined as $\ker(\rho)$ and denoted as $\mathrm{ann}_A(M)$.

We have that $\rho(a)$ is the left-multiplication (or homothety) map. We denote this by a_M, i.e.,

$$\begin{aligned} a_M\colon M &\to M \\ m &\mapsto a \cdot m. \end{aligned}$$

Note that $a_M \in \mathrm{End}_{\mathbb{Z}}(M)$ but this is not necessarily an A-module homomorphism.

Definition 0.1. If M is a left A-module, the commutant is defined as $A' \coloneqq \mathrm{End}_A(M)$, and the bicommutant as $A'' \coloneqq \mathrm{End}_{A'}(M)$.

There is a (well-defined) ring homomorphism $\lambda_M\colon A \to A''$ given by $a \mapsto a_M$.

Note that M is a left A'-module with the multiplication $A' \times M \to M$ given by $(\varphi, m) \mapsto \varphi(m)$. Thus, the bicommutant is well-defined. Moreover, each homothety a_M (for $a \in A$) is an element of the bicommutant $\mathrm{End}_{A'}(M)$ since $a_M \circ \varphi = \varphi \circ a_M$ for $a \in A$ and $\varphi \in A'$.

Definition 0.2. Let R be a commutative ring. An R-algebra is a (possibly noncommutative) ring A with a ring homomorphism $\rho\colon R \to \mathrm{center}(A)$.

In particular, whenever we talk about a k-algebra (for a field k), we have that k lies in the center of A. Note that even though we may have a natural ring homomorphism $\mathbb{C} \hookrightarrow \mathbb{H}$, the division ring $\mathbb{H}$ is *not* a $\mathbb{C}$-algebra.

Definition 0.3. A (nonzero) module is simple if it has exactly two submodules.

The two submodules are then zero and the module itself.

Definition 0.4. An A-module M is faithful if $\mathrm{ann}_A(M)$ is zero. Equivalently, if λ_M is injective.

Definition 0.5. A module M is semisimple if any of the following equivalent conditions hold:

- every submodule of N has a direct sum complement, i.e., every inclusion $N \hookrightarrow M$ splits;
- every short exact sequence of the form $0 \to N \to M \to L \to 0$ splits;
- M is the sum of its simple submodules;
- M is the direct sum of a family of simple modules.

A ring A is (left) semisimple if A is a semisimple as a left module over A.

Semisimplicity is a symmetric notion: A is left semisimple iff A is right semisimple.

Definition 0.6. A (nonzero) ring A is simple if A is is semisimple and has only one isomorphism class of simple left ideals.

The definition above is more restrictive than found in some books. Also note that being simple (or even weakly-simple) as a ring is weaker than being simple as a left-module over itself. See Theorem 1.1.

Definition 0.7. A (nonzero) ring A is weakly-simple if A has exactly two two-sided ideals.

See Theorems 1.3 and 1.4 for the implications.

Definition 0.8. A (nonzero) ring A is primitive if A has a faithful simple module.

Definition 0.9. A ring A is semiprimitive if for any nonzero $a \in A$, there is an irreducible representation ρ of A such that $\rho(a) \neq 0$.

In the language of modules: for every $a \neq 0$, there is a simple A-module M such that $aM \neq 0$.
This is equivalent to the existence of a faithful *semisimple* module, see Theorem 5.1.

Definition 0.10. Let L be a left ideal of A. The idealiser of L is defined as

$$(L : A) \coloneqq \{a \in A \colon aA \subseteq L\} = \operatorname{ann}_A(A/L).$$

The idealiser is the unique largest two-sided ideal contained in L.

Definition 0.11. Let A be a ring. The (Jacobson) radical is a two-sided ideal of A, denoted $\operatorname{rad}(A)$, defined as any of the following equivalent objects.

(a) the intersection $\bigcap_\rho \ker(\rho)$, where ρ varies over all irreducible representations of A;

(b) the intersection $\bigcap_M \operatorname{ann}_A(M)$, where M is a simple left A-module;

(c) the intersection $\bigcap_L L$ over all maximal left ideals L of A;

(d) the intersection $\bigcap_R R$ over all maximal right ideals R of A;

(e) the intersection $\bigcap_P P$ over all two-sided ideals P such that A/P is a primitive ring;

(f) the set of elements z such that $1 - az$ has a left inverse for every $a \in A$.

Definition 0.12. An element $a \in A$ is called left quasi-regular if $1 - a$ has a left inverse. A right quasi-regular element is defined analogously. An element is quasi-regular if it is both left and right quasi-regular.

A left ideal is quasi-regular if all its elements are left quasi-regular. Analogously, a right ideal is quasi-regular if all its elements are right quasi-regular.

Definition 0.13. An ideal I is nilpotent if $I^k = 0$ for some k.

Definition 0.14. Let N be a submodule of the A-module M. We say that

(a) M is an essential extension of N if for every <u>nonzero</u> submodule $K \subseteq M$, we have $N \cap K \neq 0$;

(b) N is a superfluous submodule of M if for every <u>proper</u> submodule $K \subsetneq M$, we have $N + K \neq M$.

Definition 0.15. A surjection $f \colon M \twoheadrightarrow N$ is called an essential surjection if there exists no proper submodule $M' \subseteq M$ such that $f(M') = N$.

Equivalently, $\ker(f) \subseteq M$ is a superfluous submodule.

Definition 0.16. Let M be an A-module.

The socle of M is defined as

$$\begin{aligned}\operatorname{soc}(M) &:= \sum_{N \subseteq M \text{ simple}} N \\ &= \bigcap_{N \subseteq M \text{ essential}} N.\end{aligned}$$

The radical of M is defined as

$$\begin{aligned}\operatorname{rad}(M) &:= \bigcap_{N \subseteq M \text{ maximal}} N \\ &= \sum_{N \subseteq M \text{ superfluous}} N.\end{aligned}$$

The convention is that the empty sum is 0 and the empty intersection is M.

Note that $N \subseteq M$ is maximal iff M/N is simple.

Definition 0.17. Let M be an A-module.

An injective hull of M is an essential extension $\iota\colon M \hookrightarrow E$ with E injective.

A projective cover of M is a surjection $\pi\colon P \twoheadrightarrow M$ with P projective and $\ker(\pi) \subseteq P$ a superfluous submodule. Equivalently, an essential surjection $P \twoheadrightarrow M$ with P projective.

If $\pi\colon P \twoheadrightarrow M$ is a projective cover, then $\pi(N) \neq M$ for any proper submodule $N \subsetneq P$.

Definition 0.18. A is called

- (left) perfect if every left module has a projective cover;
- (left) semiperfect if every finitely generated left module has a projective cover.

Definition 0.19. A left principal indecomposable module (PIM) of A is an indecomposable direct summand of A. Equivalently, an indecomposable, projective, cyclic module.

Definition 0.20. A is said to be a subdirect product of $A_1, \ldots, A_k$ if there is an injective ring homomorphism $\iota\colon A \to \prod_i A_i$ such that the each induced map $\pi_i \circ \iota\colon A \to A_i$ is surjective for each i.

Definition 0.21. A (nonzero) ring is called local if its set of nonunits forms a two-sided ideal.

Definition 0.22. A is quasi-Frobenius if R is left noetherian and injective as a left module over itself.

This turns out to be highly symmetric: see Theorem 6.1.

Definition 0.23. A Frobenius algebra over a field k is a finite-dimensional k-algebra A equipped with a nondegenerate bilinear form $\sigma\colon A \times A \to A$ satisfying

$$\sigma(a \cdot b, c) = \sigma(a, b \cdot c)$$

for all $a, b, c \in A$.

Definition 0.24. An A-module M is

- primordial if $\mathrm{End}_A(M)$ is a local ring;
- semi-primordial if it is the direct sum of a family of primordial submodules.

Injectives over a noetherian ring are semi-primordial.

Definition 0.25. An element $e \in A$ is called idempotent if $e^2 = e$. Two idempotents e and f are called orthogonal if $ef = fe = 0$. The idempotents 0 and 1 are the trivial idempotents. The idempotent e is a primitive idempotent if e cannot be written as a sum of two nonzero orthogonal idempotents.

If I is an ideal of A, then an idempotent $e \in A/I$ is said to lift modulo I if there exists an idempotent $f \in B$ with $e = f + I$.

Part II

Theorems

A summary of the main implications is given below.

$$
\begin{tikzcd}
 & \text{simple} \arrow[dl, Rightarrow] \arrow[dr, Rightarrow] & & \\
\text{weakly-simple} \arrow[ur, Rightarrow, bend left, "\text{semisimple}"] \arrow[d, Rightarrow] & & \text{semisimple} \arrow[dl, Rightarrow, bend left] \arrow[dr, Rightarrow] & \\
\text{primitive} \arrow[dr, Rightarrow] & & & \text{artinian} \arrow[ul, Rightarrow, bend right, "\text{semiprimitive}"'] \arrow[d, Rightarrow] \\
 & \text{semiprimitive} \arrow[d, Leftrightarrow] & & \text{perfect} \arrow[d, Rightarrow] \\
 & \text{rad} = 0 & \text{local} \arrow[r, Rightarrow] & \text{semiperfect}
\end{tikzcd}
$$

However, for the class of **left artinian** rings, the following chain of implications hold.

$$
\begin{tikzcd}
\text{simple} \arrow[r, Leftrightarrow] \arrow[d, Rightarrow] & \text{weakly-simple} \arrow[r, Leftrightarrow] & \text{primitive} \\
\text{semisimple} \arrow[r, Leftrightarrow] & \text{rad} = 0 \arrow[r, Leftrightarrow] & \text{semiprimitive}
\end{tikzcd}
$$

§1. Implications between some of the properties

Theorem 1.1. Let A be a ring. The following are equivalent.

(a) A is simple as a left module over A.

(b) A is a division ring.

(c) A is simple as a right module over A.

In such a case, A is a simple ring, a weakly-simple ring, and a semisimple ring.

Theorem 1.2. A semisimple ring is left and right artinian.

Theorem 1.3. There exists a weakly-simple ring that is not artinian and hence not semisimple.

Theorem 1.4. Let A be a ring. The following are equivalent:

(a) A is simple.

(b) A is weakly-simple and left artinian.

(c) A is weakly-simple and semisimple.

(d) A is weakly-simple and has exactly one isomorphism class of minimal left ideals.

All "left"s can be replaced with "right"s as well.

Theorem 1.5. A weakly-simple ring is primitive.

Theorem 1.6. A left artinian primitive ring is simple.

§2. Simple rings

We recall again that our definition of simple (Definition 0.6) is possibly stricter than the one the reader may have seen before (Definition 0.7). See Theorem 1.4.

We begin by stating the main theorems.

Theorem 2.1. Every simple ring A is of the form $\mathrm{End}_D(V)$, where D is a division ring and V is a finite-dimensional vector space over D.

In other words, A is a matrix ring $M_n(D)$ over a division ring. This D and n is uniquely determined.

See Theorem 2.6 for some description of D and V.

Theorem 2.2. Let D be a division ring, and V a finite-dimensional vector space over D. Set $A := \mathrm{End}_D(V)$. Then, A is a simple ring, M a simple A-module, and $D = \mathrm{End}_A(V)$.

Theorem 2.3. A simple ring has exactly one simple module up to isomorphism.

Specifically, the unique simple module over $M_n(D)$ is D^n.

Theorem 2.4. Let A be a simple ring. Then, A is a finite direct sum of simple left ideals.

If I and J are simple left ideals of A, then there exists $a \in A$ such that $Ia = J$.

Theorem 2.5. Let A be a simple ring, M a simple A-module and L a simple left ideal of A. Then, $LM = M$ and M is faithful.

Theorem 2.6. Let A be a simple ring. Then, there exists a faithful simple A-module M such that $D \coloneqq \mathrm{End}_A(M)$ is a division ring and $A \cong \mathrm{End}_D(M)$ via $\lambda_M \colon a \mapsto a_M$.

The module M can be chosen to be any simple left ideal of A.

Note that λ_M appears in Definition 0.1. See also Jacobson Density Theorem 11.1 and Corollary 11.2 which tells us that M is a finite D-module.

§3. Semisimple rings

Theorem 3.1. Let A be a ring. The following conditions are equivalent. Parts of the equivalence constitute the Wedderburn–Artin theorem.

(a) A is semisimple.

(b) A is a finite direct product of rings of the form $\mathrm{End}_D(V)$ where D is a division ring, and V is a finite-dimensional D-vector space.

(c) $A \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$, where D_i are division rings, and n_i are positive integers.
This decomposition is unique.

(d) A is left artinian and semiprimitive.

(e) A is left artinian and $\mathrm{rad}\, A = 0$

(f) A is left artinian and contains no nonzero nilpotent ideals.

(g) A is left artinian and the subdirect product of weakly-simple rings.

(h) Every A-module is projective.

(i) Every A-module is injective.

(j) Every short exact sequence of A-modules is a split exact sequence.

(k) Every A-module is semisimple.

(l) Every left (or right) ideal generated by an idempotent.

See Definition 0.20 for the definition of subdirect product.

Remark 3.2. We describe the recovery of the k, D_i, and n_i:

- The number k is the number of isomorphism classes of simple right A-modules.
- Let $S_1, \ldots, S_k$ be a list of the non-isomorphic simple right modules.
- We recover D_i as the endomorphism ring of S_i.
- The corresponding n_i is the number of right ideals in A that are isomorphic to S_i.

The reason for choosing right ideals and right modules is that we have $A \cong \mathrm{End}_A(A_A)$, where A_A denotes A viewed as a right module over itself.
If we had worked with left ideals, we would have to consider D_i^{op}.

Theorem 3.3 (Artin–Wedderburn for k-algebras)**.** If A is a finite-dimensional semisimple k-algebra, then in the decomposition $A \cong \prod_i M_{n_i}(D_i)$, each D_i is a finite-dimensional division algebra over k.

If k is algebraically closed, then $D_i = k$ for all i.

Note that without the algebraic closure hypothesis, we only have that the center of D_i is a finite extension of k. It could be larger than k. For example, $\mathbb{C}$ as an algebra over $\mathbb{R}$.

Remark 3.4. A semisimple ring may very well contain nonzero nilpotent *elements*! Indeed, the matrix rings contain many such elements.

Theorem 3.5. A semisimple ring A has finitely many isomorphism classes of simple modules. Moreover, every simple left A-module is isomorphic to a (simple) left ideal.

Theorem 3.6. Let A be a semisimple ring, L a simple left ideal, and M a simple left module. If $L \not\cong M$ as left modules, then $LM = 0$.

Theorem 3.7. A semisimple ring A can be written as a finite product of "simple subrings" (which are, in fact, two-sided ideals):

$$A = \prod_{i=1}^{k} A_i.$$

Moreover, if e_i is the unit of $A_i \subseteq A$, then $1_A = \sum_{i=1}^{k} e_i$ and $A_i = Ae_i$.

Some clarification is needed here: A_i is not really a subring of A since $1 \notin A_i$.
What is true is that A is a product of simple rings A_i, in which case each A_i is naturally a subset of A. Each A_i is further then a two-sided ideal generated by an idempotent e_i that acts as identity of A_i.

§4. Weakly-simple rings

Theorem 4.1. If A is weakly-simple, then every nonzero A-module is faithful.

Theorem 4.2 (Rieffel)**.** Let A be a weakly-simple ring, and L a nonzero left ideal. Let $A' \coloneqq \mathrm{End}_A(L)$, $A'' \coloneqq \mathrm{End}_{A'}(L)$, and $\lambda\colon A \to A''$ be as in Definition 0.1.

Then, λ is an isomorphism. In particular, L is a faithful A-module.

Theorem 4.3 (Wedderburn)**.** Let A be a ring and M a faithful simple module over A. So, $A' \coloneqq \mathrm{End}_A(M)$ is a division ring, and $\lambda\colon A \hookrightarrow A''$ makes A a subring of A''.

If M is finite-dimensional over A', then λ is an isomorphism, i.e., $A = A''$.

§5. (Semi)primitive rings

Theorem 5.1. Let A be a ring. The following statements are equivalent.

(a) A is left semiprimitive.

(b) A is right semiprimitive.

(c) A admits a faithful semisimple module.

(d) A is a finite subdirect product of primitive rings.

(e) $\mathrm{rad}(A) = 0$.

See Definition 0.20 for the definition of subdirect product. See also Theorem 7.5 for a generalisation of the last result.

Theorem 5.2. Let A be a ring.

A is left primitive iff A has a maximal left ideal L that contains no non-zero two-sided ideal of A.

A is (left) semiprimitive iff $\bigcap_L (L : A) = 0$, where the intersection is taken over all maximal left ideals of A.

Corollary 5.3. Let R be a commutative ring.

R is primitive iff R is a field.

R is semiprimitive iff R is a subdirect product of fields.

§6. Quasi-Frobenius rings

Theorem 6.1. Let A be a ring. The following are equivalent.

(a) A is quasi-Frobenius.

(b) A is noetherian on one side and self-injective on one side.

(c) A is artinian on one side and self-injective on one side.

(d) Any left (or right) injective A-module is projective.

(e) Any left (or right) projective A-module is injective.

Theorem 6.2. For a commutative ring R, the following are equivalent:

(a) R is quasi-Frobenius.

(b) R is a product of local artinian rings which have unique minimal (nonzero) ideals.

Theorem 6.3. If A is quasi-Frobenius, then either A is semisimple or has infinite right global dimension (that is, there exist modules with no finite projective resolution).

Theorem 6.4. Any Frobenius algebra over a field is quasi-Frobenius.

§7. The Jacobson radical

Since the definition is really a theorem in itself, we state it again.

Definition 7.1. Let A be a ring. The (Jacobson) radical is a two-sided ideal of A, denoted $\operatorname{rad}(A)$, defined as any of the following equivalent objects.

(a) the intersection $\bigcap_\rho \ker(\rho)$, where ρ varies over all irreducible representations of A;

(b) the intersection $\bigcap_M \operatorname{ann}_A(M)$, where M is a simple left A-module;

(c) the intersection $\bigcap_L L$ over all maximal left ideals L of A;

(d) the intersection $\bigcap_R R$ over all maximal right ideals R of A;

(e) the intersection $\bigcap_P P$ over all two-sided ideals P such that A/P is a primitive ring;

(f) the set of elements z such that $1 - az$ has a left inverse for every $a \in A$.

Theorem 7.2. Let A be a ring. The two notions of $\operatorname{rad}(A)$ coincide: namely the Jacobson radical of A as a ring, and the radical of A as a left-module over A.

Theorem 7.3. The Jacobson ideal $\operatorname{rad} A$ is quasi-regular as a left ideal.
Moreover, $\operatorname{rad} A$ contains every quasi-regular left ideal.

Theorem 7.4. Any nilpotent element is left quasi-regular.
Thus, any nilpotent left ideal is quasi-regular.

Theorem 7.5. Let A be a ring, and I a two-sided ideal.

- A is semiprimitive iff $\operatorname{rad}(A) = 0$.
- If A/I is semiprimitive, then $\operatorname{rad}(A) \subseteq I$.
- $A/\operatorname{rad}(A)$ is a semiprimitive ring. Hence, $\operatorname{rad}(A/\operatorname{rad} A) = 0$.

Theorem 7.6. The radical of a ring annihilates the socle of the ring.

§8. Socle and radical

We recall that for any module M, we have

$$\operatorname{soc}(M) := \sum_{N \subseteq M \text{ simple}} N = \bigcap_{N \subseteq M \text{ essential}} N,$$

$$\operatorname{rad}(M) := \bigcap_{N \subseteq M \text{ maximal}} N = \sum_{N \subseteq M \text{ superfluous}} N.$$

Theorem 8.1. The socle of M is the largest semisimple submodule of M.
Thus, M is semisimple iff $\operatorname{soc}(M) = M$.

If M is artinian, then the socle is an essential submodule.

If M is finitely generated, then $\operatorname{rad}(M)$ is a superfluous submodule of M. Moreover, $N \subseteq M$ is superfluous iff $N \subseteq \operatorname{rad}(M)$. Thus, the radical is the largest superfluous submodule of M.

Theorem 8.2. If $\operatorname{rad}(M)$ is a superfluous submodule and the *cosocle* $M/\operatorname{rad} M$ is finitely generated, then M is finitely generated.

Theorem 8.3. Let M be an A-module, and N a submodule.

- $\operatorname{rad}(M/\operatorname{rad} M) = 0$.
- $\operatorname{rad}(M/N) = 0$ implies $N \supseteq \operatorname{rad} M$.

Theorem 8.4. For any A-linear map $f\colon M \to N$, one has $f(\operatorname{rad} M) \subseteq \operatorname{rad} N$.

Theorem 8.5 (Radical and semisimplicity)**.** Let M be an A-module.

- If M is semisimple, then $\operatorname{rad}(M) = 0$ and $\operatorname{rad}(\operatorname{End}_A(M)) = 0$.
- If M is artinian and $\operatorname{rad}(M) = 0$, then M is semisimple.

Theorem 8.6. Let A be a left artinian ring, and M a left A-module. Then,

$$\operatorname{rad}(M) = \operatorname{rad}(A) \cdot M.$$

§9. Local rings

Theorem 9.1. Let A be a ring. Let A^* denote its set of units. The following are equivalent.

(a) A is local, i.e., $A \setminus A^*$ is an ideal.

(b) $A \setminus A^*$ is closed addition.

(c) $A \setminus A^* \subseteq \operatorname{rad}(A)$.

(d) $A \setminus A^* = \operatorname{rad}(A)$.

(e) $A \setminus \operatorname{rad}(A) = A^*$.

(f) A has a unique maximal right ideal.

(g) A has a unique maximal left ideal.

Theorem 9.2. If A is local, then A is semiperfect.

Theorem 9.3 (Kaplansky)**.** Any projective module over a local ring is free.

Theorem 9.4. Let A be a ring in which every element is either invertible or nilpotent. Then, A is local.

§10. Indecomposable-esque modules and locality

Recall that a module is primordial if its endomorphism ring is local.

Theorem 10.1. A simple module is primordial.
A primordial module is indecomposable.
An indecomposable module of finite length is primordial.

$$\begin{tikzcd}
\text{simple} \arrow[r, Rightarrow] & \text{primordial} \arrow[rr, Rightarrow, bend left] & & \text{indecomposable} \arrow[ll, Rightarrow, bend left, "\text{finite length}"]
\end{tikzcd}$$

Lemma 10.2 (Fitting)**.** Let M be an A-module of finite length. Given $u \in \mathrm{End}_A(M)$, we have
$$M = \ker(u^\infty) \oplus \mathrm{im}(u^\infty).$$
Further, u restricted to $\ker(u^\infty)$ is nilpotent and u restricted to $\mathrm{im}(u^\infty)$ is an isomorphism.

To clarify notation: the sequences of submodules $(\ker(u^N))_N$ and $(\mathrm{im}(u^N))_N$ both stabilise. The stable value is denoted by $\ker(u^\infty)$ and $\mathrm{im}(u^\infty)$ respectively.

Corollary 10.3. If E is an indecomposable A-module of finite length, then any map in $\mathrm{End}_A(E)$ is either nilpotent or invertible. Thus, $\mathrm{End}_A(E)$ is local.

Theorem 10.4 (Schur)**.** Any nonzero map between simple modules is an isomorphism.

If E is a simple A-module, then $\mathrm{End}_A(E)$ is a division ring.

Theorem 10.5 (Krull–Remak–Schmidt)**.** Let M be an A-module of finite length. Then, M can be *uniquely* decomposed as a (necessarily finite) direct sum of indecomposable modules.

Uniqueness means the following: if we have
$$M \cong E_1 \oplus \cdots \oplus E_r \cong F_1 \oplus \cdots \oplus F_s$$
for indecomposable modules E_i and F_j, then $r = s$, and there exists a permutation σ of $[r]$ such that $E_i \cong F_{\sigma(i)}$.

Corollary 10.6. Let A be a left artinian ring, and M a finitely generated left A-module. Then, M is the finite direct sum of indecomposable modules (in a unique way).

In particular, A is the direct sum of principal indecomposable modules.

Since we cannot have infinite direct sums in a noetherian or artinian module, we still have an existence theorem:

Theorem 10.7. Let M be an A-module that is either artinian or noetherian. Then, M is a finite direct sum of indecomposables, not necessarily in a unique way.

We also have a uniqueness theorem for semi-primordial modules.

Theorem 10.8. Let A be a ring. Suppose we have an isomorphism

$$E_1 \oplus \cdots \oplus E_r \cong F_1 \oplus \cdots \oplus F_s$$

for primordial A-modules E_i and F_j. Then, $r = s$, and there exists a permutation σ of $[r]$ such that $E_i \cong F_{\sigma(i)}$.

§11. Jacobson Density Theorem

Theorem 11.1 (Jacobson Density Theorem)**.** Let M be a semisimple A-module. Let A' denote the commutant of M, and A'' the bicommutant. Let $\lambda \colon A \to A''$ be the ring homomorphism $a \mapsto a_M$.

For any $\psi \in A''$ and any finite subset $S \subseteq M$, there exists $a \in A$ such that ψ and a_M agree on S.

If M is finitely generated over A', then λ is surjective.

Corollary 11.2. Let A be a left artinian ring, and M a semisimple A-module. If $A' := \mathrm{End}_A(M)$ is a division ring (e.g., M is simple), then M is a finite-dimensional vector space over A'. Hence, $\lambda(A) = A''$.

Corollary 11.3. Let V be a finite-dimensional vector space over an algebraically closed field k, and A a subalgebra of $\mathrm{End}_k(V)$.

If V is a simple A-module, then $A = \mathrm{End}_k(V)$.

Corollary 11.4. Let V be a finite-dimensional vector space over an algebraically closed field k, and G a submonoid of $\mathrm{GL}(V)$.

If V is a simple G-module, then $k[G] = \mathrm{End}_k(V)$.

Note that here $k[G]$ is the subalgebra of $\mathrm{End}_k(V)$ generated by $G \subseteq \mathrm{GL}(V) \subseteq \mathrm{End}_k(V)$.

§12. Projective modules

Throughout this section, A will denote a ring, $J := \mathrm{rad}(A)$ the Jacobson radical, set $\overline{A} := A/J$, and $\overline{M} := M/JM$ for a left A-module M. This makes $\overline{(-)}$ an additive functor in the obvious way. All modules are considered to be left modules.

In particular, given A-modules M and N, we have a map of abelian groups

$$\mathrm{Hom}_A(M, N) \to \mathrm{Hom}_{\overline{A}}(\overline{M}, \overline{N})$$

and a map of rings

$$\mathrm{End}_A(M) \to \mathrm{End}_{\overline{A}}(\overline{M}).$$

We study when these maps are injective or surjective.

Theorem 12.1. Let P be a projective A-module, and N an arbitrary A-module.

Then, $\overline{P}$ is a projective $\overline{A}$-module, and $\mathrm{Hom}_A(P, N) \twoheadrightarrow \mathrm{Hom}_{\overline{A}}(\overline{P}, \overline{N})$ is onto.

Theorem 12.2. Suppose A is (left) artinian, and P is a projective A-module. Then, the map $\mathrm{End}_A(P) \twoheadrightarrow \mathrm{End}_{\overline{A}}(\overline{P})$ induces an isomorphism

$$\frac{\mathrm{End}_A(P)}{\mathrm{rad}(\mathrm{End}_A(P))} \cong \mathrm{End}_{\overline{A}}(\overline{P}).$$

Corollary 12.3. Suppose A is artinian, and P, Q are projective A-modules. Then,

$$P \cong Q \Leftrightarrow \overline{P} \cong \overline{Q}.$$

Theorem 12.4. If P and Q are projective modules over any ring, then $P \cong Q$ if and only if $P/\mathrm{rad}\, P \cong /\mathrm{rad}\, Q$.

Theorem 12.5. Suppose A is artinian, and P is a direct summand of A as a left module. Then,

$$P \text{ is a PIM} \Leftrightarrow P \text{ is indecomposable} \Leftrightarrow \overline{P} \text{ is indecomposable} \Leftrightarrow \overline{P} \text{ is simple}.$$

Note that $\overline{A}$ is semisimple in the above situation, giving the last $\Leftrightarrow$.

§13. Superfluous extensions and (semi)perfect rings

Theorem 13.1. The zero submodule is always superfluous, and a nonzero module is never a superfluous submodule of itself.

Theorem 13.2 (Nakayama's lemma)**.** Let M be a finitely generated left A-module. Then, $\mathrm{rad}(A)M$ is a superfluous submodule of M.

If M is noetherian, then $\mathrm{rad}(M)$ is a superfluous submodule.

Theorem 13.3. Injective hulls and projective covers are unique up to isomorphism.

Injective hulls always exist, but projective covers may not exist.

Example 13.4. The $\mathbb{Z}$-module $\mathbb{Z}/2$ has no projective cover.

Theorem 13.5. If M is a projective module, then its projective cover is M.

Theorem 13.6. Let A be a semiprimitive ring (i.e., $\mathrm{rad}(A) = 0$), and M an A-module.

M has a projective cover iff M is projective.

Theorem 13.7. Any left artinian ring is right-and-left perfect.

Any local ring is right-and-left semiperfect.

Theorem 13.8 (Characterisation of perfect rings)**.** Let A be a ring. The following are equivalent.

(a) A is <u>left</u> perfect.

(b) Every left A-module has a projective cover.

(c) A satisfies the descending chain condition on principal <u>right</u> ideals.

Theorem 13.9 (Characterisation of semiperfect rings)**.** Let A be a ring. The following are equivalent.

(a) A is left semiperfect.

(b) A is right semiperfect.

(c) Every finitely generated left A-module has a projective cover.

(d) Every simple left A-module has a projective cover.

(e) $A/\operatorname{rad} A$ is semisimple and idempotents lift modulo $\operatorname{rad} A$.

Theorem 13.10. Over a semiperfect ring, every indecomposable projective module is a PIM, and every finitely generated projective module is a direct sum of PIMs.

§14. Artinian rings

We restate the theorem from earlier.

Theorem 14.1. For a left artinian ring, one has:

$$
\begin{array}{ccccc}
\text{simple} & \Longleftrightarrow & \text{weakly-simple} & \Longleftrightarrow & \text{primitive} \\
\Downarrow & & & & \\
\text{semisimple} & \Longleftrightarrow & \operatorname{rad} = 0 & \Longleftrightarrow & \text{semiprimitive}
\end{array}
$$

Theorem 14.2. Let A be left artinian. Then, $\operatorname{rad} A$ is nilpotent.

Theorem 14.3. Let A be left artinian. Then, $A/\operatorname{rad} A$ is semisimple.

Sketch. Use Theorems 3.1 and 7.5. □

Theorem 14.4. Let A be a left artinian ring, and M a left A-module. Then,

$$\operatorname{rad}(M) = \operatorname{rad}(A) \cdot M.$$

Theorem 14.5. If A is left artinian, then A is right-and-left perfect.

Sketch. We show that A is left semiperfect. If M is finitely generated, we can write $f\colon P \twoheadrightarrow M$ for some projective P. Choose P of minimal length. Then, f is the projective cover, i.e., f is essential.

Suppose not. Then, pick $N \subsetneq P$ of minimal length with $f(N) = M$. We will show that N is projective, proving the result. It suffices to show that the inclusion $\iota\colon N \hookrightarrow P$ splits.

By projectivity of P, we get $g\colon P \to N$ such that $f = f|_N \circ g$. Minimality of N gives us $g(N) = N$. Thus, $g|_N$ is surjective and hence an isomorphism. Thus, the composition $g|_N^{-1} \circ g \circ \iota$ is the identity on N, giving us the splitting. □

Theorem 14.6. If A is left artinian, then any finitely generated left A-module is the direct sum of finitely many indecomposables.

In particular, A is a finite direct sum of PIMs.

Sketch. Follows from Krull–Remak–Schmidt 10.5. □

Theorem 14.7. Over an artinian ring, every indecomposable projective module is a PIM, and every finitely generated projective module is a direct sum of PIMs.

Sketch. Let P be a projective indecomposable. Write $P \oplus Q = F$ for some free module F. Since the ring is artinian, we have that $F \cong \bigoplus_i P_i$ for PIMs P_i. Thus, $P \oplus Q = \bigoplus_i P_i$. By uniqueness of decomposition, we see that $P \cong P_i$ for some i, i.e., P is a PIM. □

Theorem 14.8. Let A be left artinian. Every nonzero homomorphic image of an indecomposable left projective module is again indecomposable.

That is, if $P \twoheadrightarrow N$ with P an indecomposable project (not necessarily a PIM), then N is indecomposable (or zero).

Theorem 14.9. Let A be left artinian and local. Then, (the left module) A is the only PIM.

Theorem 14.10. If A is a left artinian ring, then A has finitely many simple left A-modules (up to isomorphism). More precisely, setting $J := \mathrm{rad}(A)$, one has a bijection

$$\left\{ \begin{array}{c} \text{isomorphism classes of} \\ \text{simple } A\text{-modules} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{isomorphism classes of} \\ \text{simple } A/J\text{-modules} \end{array} \right\}.$$

Sketch. If M is a simple A-module, then $\mathrm{rad}(A) \subseteq \mathrm{ann}_A(M)$, i.e., $\mathrm{rad}(A) \cdot M = 0$.

This gives us the isomorphism-preserving bijection. But $A/\mathrm{rad}\, A$ is a semisimple ring, so Theorem 3.5 gives us the finiteness. □

Theorem 14.11. If A is a left artinian ring, and $J \coloneqq \operatorname{rad}(A)$ its Jacobson radical, then the map $P \mapsto P/JP$ induces a bijection

$$\left\{\begin{array}{c}\text{isomorphism classes of}\\ \text{principal indecomposable } A\text{-modules}\end{array}\right\} \leftrightarrow \left\{\begin{array}{c}\text{isomorphism classes of}\\ \text{simple modules (over } A \text{ or } A/J)\end{array}\right\}.$$

In particular, the left set is finite. The module P/JP is called the head of P. The other direction is given by mapping a simple A/J-module to its projective cover (viewed as an A-module).

Sketch. Theorem 12.5 tells us that P/JP is indeed simple when P is a PIM. Corollary 12.3 shows that the map $P \mapsto P/JP$ is injective.

In the other direction, let S be a simple A-module, and $\pi \colon P \twoheadrightarrow S$ its projective cover. Write $P = \bigoplus_i P_i$ as a sum of PIMs. The induced maps $P_i \hookrightarrow P \twoheadrightarrow S$ cannot all be zero. If $P_1 \to S$ is nonzero, then it is surjective since S is simple. But π being essential then forces $P = P_1 \in \{\text{PIMs}\}$.

This shows that we do have a well-defined map in the backwards direction.

Moreover, $P \twoheadrightarrow S$ induces $\overline{P} \twoheadrightarrow \overline{S} = S$. Since $\overline{P}$ is simple, this map is an isomorphism.

This shows that (going mod J) is a left inverse for (taking projective cover). Since the former is known to be injective, this finishes the proof. $\square$

Corollary 14.12. For A left artinian, and J its radical, we have: if S is a simple left A-module, we have an exact sequence

$$0 \to \operatorname{rad}(P) \to P \to S \to 0,$$

where the second map is the projective cover.

Said differently, if $P \twoheadrightarrow S$ is the projective cover, then $P/\operatorname{rad} P = P/JP \cong S$.

§15. Symmetric and asymmetric properties

We list the properties we have considered in this document and note whether they are symmetric. A property P of a ring is symmetric if the following is true: A has P iff A^{op} has P.
Equivalently, since our properties are often listed stated as "A is left P", being symmetric is saying: A is left P iff A is right P.

(a) Artinian: not symmetric.

(b) Noetherian: not symmetric.

(c) Finite length: not symmetric.
Moreover, even if A has finite length as a left and right module, these lengths could be different.

(d) Local: symmetric by definition.

(e) Semisimple: symmetric by classification theorem.

(f) Simple: symmetric by classification theorem.

(g) Weakly-simple: symmetric by definition.

(h) Semiprimitive: symmetric since characterised by $\mathrm{rad} = 0$.

(i) Primitive: **not** symmetric!

(j) Semiperfect: symmetric.

(k) Perfect: **not** symmetric!

(l) Quasi-Frobenius: symmetric.

Part III

Representation theory?

We now focus our attention to the artinian ring $k[G]$.

§16. Definitions

In what follows, k will denote an arbitrary field and G a finite group.

Definition 16.1. The group ring (or the group algebra) $k[G]$ is the k-algebra defined as follows:

- as a vector space, we have $k[G] = \bigoplus_{g \in G} kg$;
- the multiplication on the basis $\{g : g \in G\}$ is given by $g \cdot h = gh$;
- the ring homomorphism $\eta\colon k \to k[G]$ with $1 \mapsto 1$ makes this a k-algebra.

The modular case refers to the situation when $\mathrm{char}(k) \mid |G|$.

Note that the k-dimension of $k[G]$ is $|G|$. The ring $k[G]$ is commutative iff G is abelian.

Recall that a representation of G on a k-vector space V is a group homomorphism $\rho\colon G \to GL(V)$. This is precisely the same data as a $k[G]$-module V.

Note that $k[G]$ is (left and right) artinian, being finite-dimensional over a field.

Definition 16.2. The algebra $k[G]$ is further an augmented algebra.

The augmentation map is defined as

$$\begin{aligned} \varepsilon\colon k[G] &\to k \\ \sum_{g\in G} a_g g &\mapsto \sum_{g\in G} a_g. \end{aligned}$$

This is a map of k-algebras, a k-linear ring homomorphism.

The augmentation ideal of G is defined as

$$I(G) \coloneqq \ker(\varepsilon) = \left\{ \sum_g a_g g : \sum_g a_g = 0 \right\}.$$

Definition 16.3. The map ε gives k the structure of a $k[G]$-bimodule.

Remark 16.4. Under the identification {left $k[G]$-modules} = {representations of G}, the left module k (viewed as a module via the augmentation) corresponds to the trivial representation $G \to GL_1(k)$.

Indeed, for $g \in G$ and $\alpha \in k$, we have $g \cdot \alpha = \alpha$.

§17. Basic constructions

We list some basis constructions and observations that connected groups with their algebras.

§§17.1. Functoriality

Given a group homomorphism $\varphi\colon G_1 \to G_2$, we get a k-linear map $k[\varphi]$ given on a basis as

$$\begin{aligned} k[\varphi]\colon k[G_1] &\to k[G_2] \\ g &\mapsto \varphi(g). \end{aligned}$$

This is a homomorphism of *augmented* k-algebras.

Lemma 17.1. Its kernel is generated both as a left and right ideal by $\{g - 1 : g \in \ker(\varphi)\}$.

Note that if $H \leqslant G$ is a subgroup, then $k[H]$ is naturally a subalgebra of $k[G]$.

Theorem 17.2. If N is a normal subgroup of G, then the canonical surjection $G \twoheadrightarrow G/N$ induces a surjection $k[G] \twoheadrightarrow k[G/N]$ whose kernel is generated by $\{n - 1 : n \in N\}$. Thus, we get

$$k[G/N] \cong k[G]/\,I(N)k[G].$$

§§17.2. Product of groups

There is a natural isomorphism of augmented k-algebras, given on a basis as

$$\begin{aligned} k[G_1] \otimes_k k[G_2] &\cong k[G_1 \times G_2], \\ g_1 \otimes g_2 &\mapsto (g_1, g_2). \end{aligned}$$

Going forth, we may often implicitly identify the group ring of a product with the tensor algebra.

§§17.3. The diagonal map

The diagonal homomorphism $\Delta\colon G \to G \times G$ induces an algebra homomorphism

$$\begin{aligned} \Delta\colon k[G] &\to k[G] \otimes_k k[G] \\ g &\mapsto g \otimes g. \end{aligned}$$

This is called the diagonal homomorphism (or coproduct) of the group algebra $k[G]$.

§§17.4. The anti-isomorphism

Recall that every group G is isomorphic to its opposite group G^{op} via $g \mapsto g^{-1}$. Equivalently, this map is an *anti-isomorphism* $G \to G$. Consequently, we get the anti-isomorphism

$$\sigma\colon k[G] \to k[G].$$

This map is called the antipode.

The antipode commutes with the diagonal:

$$\begin{tikzcd} k[G] \arrow[r, "\sigma^G"] \arrow[d, "\Delta^G"'] & k[G] \arrow[d, "\Delta^G"] \\ k[G \times G] \arrow[r, "\sigma^{G\times G}"'] & k[G \times G] \end{tikzcd}$$

This data makes $k[G]$ into a Hopf algebra.

§§17.5. Conjugation

If M is a left $k[G]$-module, then the underlying k-vector space M may be viewed as a *right* $k[G]$-module by defining

$$m \cdot g := g^{-1}m$$

for $g \in G$ and $m \in M$.

However, M is above is **NOT** a $k[G]$-bimodule.

We have

$$g \cdot (m \cdot h) = g \cdot (h^{-1}m) = gh^{-1}m$$

and

$$(g \cdot m) \cdot h = (gm) \cdot h = h^{-1}gm.$$

§§17.6. Tensor product

Let R and S be k-algebras, and let M and N be left modules over R and S respectively. Then, $M \otimes_k N$ has a natural left $(R \otimes_k S)$-module structure via

$$(r \otimes_k s) \cdot (m \otimes_k n) = (rm) \otimes_k (sn).$$

If M and N are left $k[G]$-modules, we get a left $(k[G] \otimes_k k[G])$-module $M \otimes_k N$. The diagonal map makes this into a left $k[G]$-module with

$$g \cdot (m \otimes_k n) = (gm) \otimes_k (gn).$$

We have an isomorphism of $k[G]$-modules

$$\begin{aligned} M \otimes_k N &\xrightarrow{\cong} N \otimes_k M, \\ m \otimes_k n &\mapsto n \otimes_k m. \end{aligned}$$

The above is the correct tensor product to consider, since this does give us back a $k[G]$-module.

§§17.7. Homomorphisms

Let M and N be left $k[G]$-module. The k-vector space $\mathrm{Hom}_k(M, N)$ can be endowed with a G-action as

$$(g \cdot \alpha)(m) := g\alpha(g^{-1}m)$$

for $g \in G$ and $m \in M$.

Note that $\mathrm{Hom}_{k[G]}(M, N)$ is a subset of $\mathrm{Hom}_k(M, N)$. The definition gives us

$$\mathrm{Hom}_{k[G]}(M, N) = \mathrm{Hom}_k(M, N)^G.$$

In particular, one has the natural identification

$$\mathrm{Hom}_{k[G]}(k, M) = M^G.$$

Thus, the functor $\mathrm{Hom}_{k[G]}(k, -)$ is the invariants functor $(-)^G$.

Theorem 17.3. Let L, M, N be left modules over $k[G]$. Then,

$$\mathrm{Hom}_{k[G]}(L \otimes_k M, N) \cong \mathrm{Hom}_{k[G]}(L, \mathrm{Hom}_k(M, N)).$$

§§17.8. Dual

Let M be a left $k[G]$-module and set $M^* \coloneqq \mathrm{Hom}_k(M, k)$ as a k-vector space. Specialising §17.7 to this object makes M^* a left $k[G]$-module. On the other hand, conjugation (§17.5) gives M a right module structure, which gives M^* a natural left $k[G]$-module structure by

$$(g \cdot \alpha)(m) \coloneqq \alpha(m \cdot g).$$

A calculation shows that they both coincide.

Moreover, the canonical k-linear maps

$$\begin{aligned} M &\to M^{**} \\ m &\mapsto (f \mapsto f(m)) \end{aligned} \qquad\qquad \begin{aligned} N \otimes_k M^* &\to \mathrm{Hom}_k(M, N) \\ n \otimes_k f &\mapsto (m \mapsto f(m)n) \end{aligned}$$

are $k[G]$-linear. These maps are bijective when $\mathrm{rank}_k M$ is finite.

§18. Basic properties of the group algebra

In this section, we list some properties of $k[G]$ that follows from the general theory of earlier. As before, k will denote a field, and G a finite group.

Theorem 18.1. The group algebra $k[G]$ is a Frobenius algebra over k with the bilinear map

$$\sigma(a, b) = \text{coefficient of } 1 \text{ in } a \cdot b.$$

In particular, $k[G]$ is a quasi-Frobenius ring. Thus, $k[G]$ is self-injective.

Theorem 18.2. The following are equivalent. The implication (a) $\Leftrightarrow$ (b) is known as Maschke's theorem.

(a) (Nonmodular) $\mathrm{char}(k) \nmid |G|$.

(b) The group algebra $k[G]$ is semisimple.

(c) Every left (or right) $k[G]$-module has finite projective dimension.

(d) The module k—viewed as a left (or right) $k[G]$-module via the augmentation—is projective.

(e) The augmentation map $k[G] \twoheadrightarrow k$ has a $k[G]$-linear section.

Sketch. (b) $\Leftrightarrow$ (c): follows from Theorem 6.3 since $k[G]$ is quasi-Frobenius.

(b) $\Rightarrow$ (d): any module over a semisimple ring is projective.

(d) $\Leftrightarrow$ (e): true because $k[G]$ is projective.

(a) $\Rightarrow$ (b): Suppose $\operatorname{char}(k) \nmid |G|$. Any inclusion $W \hookrightarrow V$ of $k[G]$-modules has a k-linear splitting $\pi\colon V \to W$. This gives rise to the $k[G]$-linear splitting given by

$$\frac{1}{|G|} \sum_{g \in G} g_V \circ \pi \circ g_V^{-1}.$$

(e) $\Rightarrow$ (a): Let $\iota\colon k \hookrightarrow k[G]$ be a (left) $k[G]$-linear section to $\varepsilon\colon k[G] \to k$. For any $h \in H$, we have

$$\iota(1) = \iota(\varepsilon(h)1) = \iota(h \cdot 1) = h\iota(1).$$

Thus, if we write $\iota(1) = \sum_g a_g g$, we see that a_g is constant with respect to g. In turn,

$$1 = \varepsilon(\iota(1)) = \sum_g a_1 = |G| a_1,$$

showing that $|G|$ is invertible in k. □

Corollary 18.3. Let k be a field and G a finite group such that $\operatorname{char}(k) \nmid |G|$. Then,

- the indecomposable and irreducible representations of G coincide;
- there are finitely many irreducible representations of G;
- every representation decomposes as a direct sum of irreducible representations of G.

Regardless, since $k[G]$ is artinian even in the modular case, we have the following.

Theorem 18.4. Let k be a field, and G be any finite group. Then,

- the ring $k[G]$ has finitely many simple modules;

- the group G has finitely many irreducible representations over k;
- any finite-dimensional representation is (uniquely) the direct sum of finitely many indecomposable representations;
- every $k[G]$-module has a projective cover;
- every indecomposable projective is a PIM;
- the projective cover of each simple module is indecomposable and cyclic, i.e., a PIM;
- if $J := \mathrm{rad}(k[G])$, then we have a one-to-one correspondence of isomorphism classes

$$\{\text{projective indecomposables}\} = \{\text{PIMs}\} \leftrightarrow \{\text{simple modules}\}$$
$$P \mapsto P/JP,$$

with the inverse being given by taking projective covers.

In the modular case, the issue is that there exist representations that cannot be written as a (direct) sum of irreducible representations.

§19. The augmentation ideal

Theorem 19.1. Let $\{g_\lambda\}_{\lambda\in\Lambda}$ be generating set for G. Then, the left (or right) ideal generated by $\{g_\lambda - 1\}_{\lambda\in\Lambda}$ is the augmentation ideal $I(G)$.

As remarked earlier, if $N \trianglelefteq G$ is a normal subgroup, then the kernel of the natural map

$$k[G] \to k[G/N]$$

is generated by $\{n - 1 : n \in N\}$; this is precisely $I(N)k[G]$.

§20. Representation type of groups

We give a classification of representation type finite groups on the basis of the type of Sylow-p subgroup that they have. Recall that any two Sylow-p subgroups of a finite group are isomorphic. By "representation type", we roughly mean the number of inequivalent indecomposable representations.

Theorem 20.1. Let G be a finite group and k an <u>infinite</u> field of characteristic $p > 0$.

(a) (Finite) $k[G]$ has finitely many indecomposables iff the Sylow-p subgroups of G are cyclic.

(b) (Domestic) $k[G]$ has domestic representation type iff $p = 2$ and the Sylow-2 subgroups are isomorphic to the Klein four group.

(c) (Tame) $k[G]$ has tame representation type iff $p = 2$ and the Sylow-2 subgroups are dihedral, semidihedral, or generalised quaternion.

(d) (Wild) In all other cases, $k[G]$ has wild representation type.

Loosely(!) speaking: Tame type means it is not finite and that in every dimension, modulo finitely many exceptions, there is a one-parameter family that parameterises the indecomposables.
Domestic is something about being able to narrow down to an independent-of-n family.

§§20.1. Klein four group

Consider the Klein four group $V_4 \coloneqq \mathbb{Z}/2 \times \mathbb{Z}/2$, and k a field of characteristic two.

A complete classification is given in Benson's *Representations and cohomology, I: Basic representation theory of finite groups and associative algebras* (Theorem 4.3.3) but we give some examples of indecomposables here.

After a change of variables, we have $k[V_4] = k[x, y]/(x^2, y^2)$.

Example 20.2. Every rank two indecomposable $k[V_4]$ is of the form

$$V_{(\alpha_1,\alpha_2)} = \frac{k[V_4]}{(\alpha_1 x + \alpha_2 y, xy)}.$$

Moreover, $V_{(\alpha_1,\alpha_2)}$ is isomorphic to $V_{(\beta_1,\beta_2)}$ iff (α_1, α_2) is proportional to (β_1, β_2).

The above gives a $\mathbb{P}^1(k)$-parameterised family.

For $n \geqslant 0$, let M_n denote the n-th syzygy of k as a kV_4-module, and set $M_n^* \coloneqq \mathrm{Hom}_k(M, k)$.

Then, we have:

Example 20.3. The family $\{\ldots, M_2, M_1, k, M_1^*, M_2^*, \ldots\}$ consists of inequivalent indecomposable kV_4-modules. We have

$$\mathrm{rank}(M_n) = \mathrm{rank}(M_n^*) = 2n + 1.$$

Every indecomposable of odd rank appears in the above family.

There are other indecomposables in even ranks. These are parameterised by "indecomposable rational canonical forms".

§21. Projective modules

As before, G is a finite group, and k an arbitrary field of characteristic p. Recall that $k[G]$ is quasi-Frobenius: thus, the injectives and projectives coincide. So, all the consequent theorems have their "injective" analogue.

Theorem 21.1. Let G be a group and P a projective $k[G]$-module. For any $k[G]$-module X, the $k[G]$-modules $P \otimes_k X$ and $X \otimes_k P$ are projective.

Note again that the tensor is over k. The two modules are isomorphic as noted before. The above says that—under a suitable interpretation—the subcategory of projective modules is an *ideal*.

Theorem 21.2. Let G be a finite group, and M a finite $k[G]$-module. The projectivity of the following modules are equivalent:

(a) M,

(b) $M \otimes_k M$,

(c) $M^* \otimes_k M$,

(d) $M \otimes_k M^*$,

(e) $\mathrm{Hom}_k(M, M)$, and

(f) M^*.

What we mean is that if one of the above modules is projective, then so are the rest.

Theorem 21.3. Let A be a finite-dimensional k-algebra. For each finite left A-module M, one has

$$\mathrm{pdim}_A(M) = \mathrm{flatdim}_A(M) = \mathrm{injdim}_{A^{\mathrm{op}}}(M^*).$$

We recall again that:

Theorem 21.4. If G is a p-group and $\mathrm{char}(k) = p$, then $k[G]$ is local and the only projective modules are the free modules.

More generally, one has:

Theorem 21.5. Let p^d be the order of a Sylow-p subgroup of G. If P is a finite $k[G]$-module, then p^d divides $\mathrm{rank}_k P$.

Sketch. Let $H \leqslant G$ be a Sylow-p subgroup. Then, P is a projective kH-module and hence free over kH. $\square$

§§21.1. Symmetric group on three letters

Consider
$$\Sigma_3 = \langle a, b \mid a^2 = b^3 = 1,\ ba = ab^2 \rangle.$$

Let k be a field of characteristic p.

If $p \neq 2, 3$, then $k\Sigma_3$ is semisimple and every module is projective.

Suppose $p = 3$: By Theorem 18.4, we know that $k\Sigma_3$ is a sum of projective indecomposables and that every projective indecomposable appears in the (unique) representation of $k\Sigma_3$ as a sum of indecomposables. Each such projective has rank divisible by three. Since $\operatorname{rank}_k k\Sigma_3 = 6$, we see that there are at most two distinct indecomposable projectives.

We construct two such projectives: Let $H = \langle a \rangle$ be a Sylow-2 subgroup. We can turn k into a left $k[H]$-module in two different ways: the trivial one, via the augmentation map, and the one defined by the character $a \mapsto -1$; denote the latter by ${}^{\sigma}k$.
Since $k[H]$ is semisimple, both of these are projective $k[H]$-modules. Base change preserves projectives (direct summands of free modules), so we get two projective $k[\Sigma_3]$-modules
$$P_1 := k[\Sigma_3] \otimes_{k[H]} k \quad \text{and} \quad P_2 := k[\Sigma_3] \otimes^{\sigma}_{k[H]} k.$$

These are indecomposable since these are rank 3 (and 3 divides the rank of any projective). Also, $\operatorname{rank}_k(P_1^G) = 1$ and $\operatorname{rank}_k(P_2^G) = 0$ shows that these are not isomorphic.

Suppose $p = 2$: Let $H = \langle b \rangle = \{1, b, b^2\}$. Note that
$$k[H] = k[x]/(x^3 - 1) \cong \frac{k[x]}{(x-1)} \times \frac{k[x]}{(x^2+x+1)}.$$

If $x^2 + x + 1$ is irreducible, then $k[H]$ has two simple (projective) modules, of ranks 1 and 2 over k. Base-changing them to $k[\Sigma_3]$ will give projectives of ranks 2 and 4.
If $x^2 + x + 1$ is irreducible, then this will give us three projectives over $k[\Sigma_3]$, of rank 2 each.

One checks that in each case, this does give us the complete family of projective indecomposables.

§22. Cohomology of supplemented algebras

Recall that a group algebra is a supplemented algebra, i.e., we have ring homomorphisms $\eta\colon k \to A$ and $\varepsilon\colon R \to k$ such that $\varepsilon \circ \eta = \mathrm{id}_k$.

Let R be a supplemented k-algebra, and view k as an R-module via the augmentation. Let M be a left R-module. The cohomology of R with coefficients in M is the graded k-vector

space $\operatorname{Ext}^*_R(k, M)$.
When $M = k$, we get $\operatorname{Ext}^*_R(k, k)$, which is usually called the cohomology of R.

Just to recall: the above graded k-vector space is computed as following: start with a (left) R-projective resolution of k as

$$\cdots \to P_1 \to P_0 \to 0.$$

Applying $\operatorname{Hom}_R(-, M)$ to the above gives us a cocomplex of k-vector spaces (note that we lose the R-module structure in the noncommutative case):

$$0 \to \operatorname{Hom}_R(P_0, M) \to \operatorname{Hom}_R(P_1, M) \to \cdots.$$

The homology at the n-th stage is $\operatorname{Ext}^n_R(k, M)$.

We now describe how to give $\operatorname{Ext}^*_R(k, k)$ the structure of a supplemented k-algebra, over which $\operatorname{Ext}^*_R(k, M)$ can be made into a *right* module.

§§22.1. Composition product

Let $P = (P_\bullet, \partial^P_\bullet)$ be a projective resolution of k. Recall that $\operatorname{Hom}_R(P, P)$ is a complex of k-vector spaces defined as:

- $\operatorname{Hom}_R(P, P)_n = \prod_{i \in \mathbb{Z}} \operatorname{Hom}_R(P_i, P_{i+n})$, the degree n morphisms with no compatibility condition;
- the differential

$$\begin{aligned} \operatorname{Hom}_R(P, P)_{n+1} &\to \operatorname{Hom}_R(P, P)_n \\ f &\mapsto \partial^P \circ f - (-1)^{n+1} f \circ \partial^P. \end{aligned}$$

  (If we imagine f as a tuple of module maps, the compositions on the right are being performed component-wise in the appropriate sense.)

We may also think of $\operatorname{Hom}_R(P, P)$ as a graded k-vector space in the natural way. For homogeneous $f, g \in \operatorname{Hom}_R(P, P)$, we have

$$\partial(f \circ g) = \partial(f) \circ g + (-1)^{|f|} f \circ \partial(g).$$

This makes $\operatorname{Hom}_R(P, P)$ into a differential graded algebra (DGA), called the endomorphism DGA of P.

We also recall that Ext can be computed using the endomorphism complex. In particular,

$$\operatorname{Ext}^n_R(k, k) = H_n(\operatorname{Hom}_R(P, P)).$$

§23. Examples

We work out some of the earlier theory in explicit examples.

§§23.1. Abelian groups

We have $k[\mathbb{Z}] = k[x, x^{-1}]$ with $I(\mathbb{Z}) = (x-1)$.
If $d > 0$ is a positive integer, then $k[\mathbb{Z}/d] = k[x]/(x^d - 1)$ with $I(\mathbb{Z}/d) = (x-1)$.

If G is a finitely generated abelian group, then we can write $G \cong \mathbb{Z}^n \oplus \mathbb{Z}/d_1 \oplus \cdots \oplus \mathbb{Z}/d_k$. Then,

$$k[G] = \frac{k[x_1, \ldots, x_n, y_1, \ldots, y_k]}{(y_1^{d_1} - 1, \ldots, y_k^{d_k} - 1)}.$$

Note that this is a complete intersection.

§§23.2. p-groups

Theorem 23.1. Let k be a field of characteristic $p > 0$, and G a finite group.

The ring $k[G]$ is local iff G is a p-group.

Suppose now that $\operatorname{char}(k) = p > 0$ and that G is a p-group.

Then, the ideal of nonunits, which is equal to the Jacobson radical, coincides with the augmentation ideal:

$$\operatorname{rad}(k[G]) = \left\{ \sum_g a_g g : \sum_g a_g = 0 \right\} = I(G).$$

Thus, $k[G]/\operatorname{rad} \cong k$ and we get:

Theorem 23.2. Suppose $\operatorname{char}(k) = p > 0$ and G is a p-group.

There is exactly one simple $k[G]$-module, namely k.

There is exactly one projective indecomposable over $k[G]$, namely $k[G]$. (In particular, the unique PIM as well.)

For cyclic groups, the representation theory is even better.

Theorem 23.3. Let k be a field of characteristic $p > 0$, and $G := C_{p^r}$ the cyclic group of order p^r. There are exactly p^r inequivalent indecomposable $k[G]$-modules, one of dimension n for each $1 \leqslant n \leqslant p^r$. Moreover, there is a chain of inclusions

$$V_1 \subseteq V_2 \subseteq \cdots \subseteq V_{p^r}.$$

The representation V_n is given by G acting on k^n via the size-n Jordan block.