Chapter 1. Foundations of Representation Theory

In this chapter we review four important module-theoretic theorems, which lie at the foundations of *representation theory of finite groups*:

1. **Schur's Lemma**: about homomorphisms between simple modules.
2. **The Jordan-Hölder Theorem**: about "uniqueness" properties of composition series.
3. **Nakayama's Lemma**: about an essential property of the Jacobson radical.
4. **The Krull-Schmidt Theorem**: about direct sum decompositions into indecomposable submodules.

Notation: throughout this chapter, unless otherwise specified, we let R denote an arbitrary unital and associative ring.

Again results which intersect the *Commutative Algebra* lecture are stated without proof.

References:

[CR90] C. W. Curtis and I. Reiner, *Methods of representation theory. Vol. I*, Wiley Classics Library, John Wiley & Sons, Inc., New York, 1990.

[Dor72] L. Dornhoff, *Group representation theory. Part B: Modular representation theory*, Marcel Dekker, Inc., New York, 1972.

[NT89] H. Nagao and Y. Tsushima, *Representations of finite groups*, Translated from the Japenese. Academic Press, Inc., Boston, MA, 1989.

[Rot10] J. J. Rotman, *Advanced modern algebra. 2nd ed.*, Providence, RI: American Mathematical Society (AMS), 2010.

6 (Ir)Reducibility and (in)decomposability

Submodules and direct sums of modules allow us to introduce the two main notions that will enable us to break modules in *elementary* pieces in order to simplify their study.

Definition 6.1 (*simple/irreducible module / indecomposable module*)

(a) An R-module M is called **reducible** if it admits an R-submodule U such that $0 \lneq U \lneq M$. An R-module M is called **simple** (or **irreducible**) if it is non-zero and not reducible.

(b) An R-module M is called **decomposable** if M possesses two non-zero proper submodules M_1, M_2 such that $M = M_1 \oplus M_2$. An R-module M is called **indecomposable** if it is non-zero and not decomposable.

Remark 6.2

Clearly any simple module is also indecomposable. However, the converse does not hold in general. Exercise: find a counter-example!

Exercise 6.3

Prove that if $(R, +, \cdot)$ is a ring, then $R^\circ := R$ itself maybe seen as an R-module via left multiplication in R, i.e. where the external composition law is given by

$$R \times R^\circ \longrightarrow R^\circ, (r, m) \mapsto r \cdot m\,.$$

We call R° the **regular** R-module.

Prove that the R-submodules of R° are precisely the left ideals of R. Moreover, $I \lhd R$ is a maximal left ideal of $R \Leftrightarrow R^\circ/I$ is a simple R-module, and $I \lhd R$ is a minimal left ideal of $R \Leftrightarrow I$ is simple when regarded as an R-submodule of R°.

7 Schur's Lemma

Schur's Lemma is a basic result, which lets us understand homomorphisms between *simple* modules, and, more importantly, endomorphisms of such modules.

Theorem 7.1 (*Schur's Lemma*)

(a) Let V, W be simple R-modules. Then:

 (i) $\mathrm{End}_R(V)$ is a skew-field, and

 (ii) if $V \ncong W$, then $\mathrm{Hom}_R(V, W) = 0$.

(b) If K is an algebraically closed field, A is a K-algebra, and V is a simple A-module such that $\dim_K V < \infty$, then

$$\mathrm{End}_A(V) = \{\lambda\, \mathrm{Id}_V \mid \lambda \in K\} \cong K\,.$$

Proof :

(a) First, we claim that every $f \in \mathrm{Hom}_R(V, W) \setminus \{0\}$ admits an inverse in $\mathrm{Hom}_R(V, W)$. Indeed, $f \neq 0 \implies \ker f \subsetneq V$ is a proper R-submodule of V and $\{0\} \neq \mathrm{Im}\, f$ is a non-zero R-submodule of W. But then, on the one hand, $\ker f = \{0\}$, because V is simple, hence f is injective, and on the other hand, $\mathrm{Im}\, f = W$ because W is simple. It follows that f is also surjective, hence bijective. Therefore, by Example 1(d), f is invertible with inverse $f^{-1} \in \mathrm{Hom}_R(V, W)$.

Now, (ii) is straightforward from the above. For (i), by Exercise 2.2, $\mathrm{End}_R(V)$ is a ring, which is obviously non-zero as $\mathrm{End}_R(V) \ni \mathrm{Id}_V$ and $\mathrm{Id}_V \neq 0$ because $V \neq 0$ since it is simple. Thus, as any $f \in \mathrm{End}_R(V)\backslash\{0\}$ is invertible, $\mathrm{End}_R(V)$ is a skew-field.

(b) Let $f \in \mathrm{End}_A(V)$. By the assumptions on K, f has an eigenvalue $\lambda \in K$. Let $v \in V\backslash\{0\}$ be an eigenvector of f for λ. Then $(f - \lambda \mathrm{Id}_V)(v) = 0$. Therefore, $f - \lambda \mathrm{Id}_V$ is not invertible and

$$f - \lambda \mathrm{Id}_V \in \mathrm{End}_A(V) \overset{(a)}{\Longrightarrow} f - \lambda \mathrm{Id}_V = 0 \Longrightarrow f = \lambda \mathrm{Id}_V .$$

Hence $\mathrm{End}_A(V) \subseteq \{\lambda \mathrm{Id}_V \mid \lambda \in K\}$, but the reverse inclusion also obviously holds, so that

$$\mathrm{End}_A(V) = \{\lambda \mathrm{Id}_V\} \cong K .$$

■

8 Composition series and the Jordan-Hölder Theorem*

From Chapter 2 on, we will assume that all modules we work with can be broken into *simple* modules in the sense of the following definition.

Definition 8.1 (*Composition series / composition factors / composition length*)

Let M be an R-module.

(a) A **series** (or **filtration**) of M is a finite chain of submodules

$$0 = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_n = M \qquad (n \in \mathbb{Z}_{\geqslant 0}) .$$

(b) A **composition series** of M is a series

$$0 = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_n = M \qquad (n \in \mathbb{Z}_{\geqslant 0})$$

where M_i/M_{i-1} is simple for each $1 \leqslant i \leqslant n$. The quotient modules M_i/M_{i-1} are called the **composition factors** (or the **constituents**) of M and the integer n is called the **composition length** of M.

Notice that, clearly, in a composition series all inclusions are in fact strict because the quotient modules are required to be simple, hence non-zero.

Next we see that the existence of a *composition series* implies that the module is *finitely generated*. However, the converse does not hold in general. This is explained through the fact that the existence of a composition series is equivalent to the fact that the module is both *Noetherian* and *Artinian*.

Definition 8.2 (*Chain conditions / Artinian and Noetherian rings and modules*)

(a) An R-module M is said to satisfy the **descending chain condition** (D.C.C.) on submodules (or to be **Artinian**) if every descending chain $M = M_0 \supseteq M_1 \supseteq \ldots \supseteq M_r \supseteq \ldots \supseteq \{0\}$ of submodules eventually becomes stationary, i.e. $\exists\, m_0$ such that $M_m = M_{m_0}$ for every $m \geqslant m_0$.

(b) An R-module M is said to satisfy the **ascending chain condition** (A.C.C.) on submodules (or to be **Noetherian**) if every ascending chain $0 = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_r \subseteq \ldots \subseteq M$ of submodules eventually becomes stationary, i.e. $\exists\, m_0$ such that $M_m = M_{m_0}$ for every $m \geqslant m_0$.

(c) The ring R is called **left Artinian** (resp. **left Noetherian**) if the regular module R° is Artinian (resp. Noetherian).

Theorem 8.3 (*Jordan-Hölder*)

Any series of R-submodules $0 = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_r = M$ ($r \in \mathbb{Z}_{\geqslant 0}$) of an R-module M may be refined to a composition series of M. In addition, if

$$0 = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_n = M \quad (n \in \mathbb{Z}_{\geqslant 0})$$

and

$$0 = M'_0 \subsetneq M'_1 \subsetneq \ldots \subsetneq M'_m = M \quad (m \in \mathbb{Z}_{\geqslant 0})$$

are two composition series of M, then $m = n$ and there exists a permutation $\pi \in \mathfrak{S}_n$ such that $M'_i/M'_{i-1} \cong M_{\pi(i)}/M_{\pi(i)-1}$ for every $1 \leqslant i \leqslant n$. In particular, the composition length is well-defined.

Proof: See *Commutative Algebra*. ■

Corollary 8.4

If M is an R-module, then TFAE:

(a) M has a composition series;

(b) M satisfies D.C.C. and A.C.C. on submodules;

(c) M satisfies D.C.C. on submodules and every submodule of M is finitely generated.

Proof: See *Commutative Algebra*. ■

Theorem 8.5 (*Hopkins' Theorem*)

If M is a module over a left Artinian ring, then TFAE:

(a) M has a composition series;

(b) M satisfies D.C.C. on submodules;

(c) M satisfies A.C.C. on submodules;

(d) M is finitely generated.

Proof: See *Commutative Algebra*. (Or Exercise: deduce it from the properties of the Jacobson radical and semisimplicity, which we are going to develop in the next sections.) ■

9 The Jacobson radical and Nakayama's Lemma*

The Jacobson radical is one of the most important two-sided ideals of a ring. As we will see in the next sections and Chapter 2, this ideal carries a lot of information about the structure of a ring and that of its modules.

Proposition-Definition 9.1 (*Annihilator / Jacobson radical*)

(a) Let M be an R-module. Then $\operatorname{ann}_R(M) := \{r \in R \mid rm = 0 \;\; \forall\, m \in M\}$ is a two-sided ideal of R, called **annihilator** of M.

(b) The **Jacobson radical** of R is the two-sided ideal

$$J(R) := \bigcap_{\substack{V \text{ simple} \\ R\text{-module}}} \operatorname{ann}_R(V) = \{x \in R \mid 1 - axb \in R^\times \;\; \forall\, a, b \in R\}\,.$$

(c) If V is a simple R-module, then there exists a maximal left ideal $I \lhd R$ such that $V \cong R^\circ/I$ (as R-modules) and

$$J(R) = \bigcap_{\substack{I \lhd R, \\ I \text{ maximal} \\ \text{left ideal}}} I\,.$$

Proof: See *Commutative Algebra*. ■

Exercise 9.2

(a) Prove that any simple R-module may be seen as a simple $R/J(R)$-module.

(b) Conversely, prove that any simple $R/J(R)$-module may be seen as a simple R-module. [Hint: use a change of the base ring via the canonical morphism $R \longrightarrow R/J(R)$.]

(c) Deduce that R and $R/J(R)$ have the same simple modules.

Theorem 9.3 (*Nakayama's Lemma*)

If M is a finitely generated R-module and $J(R)M = M$, then $M = 0$.

Proof: See *Commutative Algebra*. ■

Remark 9.4

One often needs to apply Nakayama's Lemma to a finitely generated quotient module M/U, where U is an R-submodule of M. In that case the result may be restated as follows:

$$M = U + J(R)M \quad \Longrightarrow \quad U = M$$

10 Indecomposability and the Krull-Schmidt Theorem

We now consider the notion of *indecomposability* in more details. Our first aim is to prove that indecomposability can be recognised at the endomorphism algebra of a module.

Definition 10.1

A ring R is said to be **local** $:\Longleftrightarrow R\backslash R^\times$ is a two-sided ideal of R.

Example 5

(a) Any field K is local because $K\backslash K^\times = \{0\}$ by definition.

(b) Exercise: Let p is a prime number and $R := \{\frac{a}{b} \in \mathbb{Q} \mid p \not| b\}$. Prove that $R\backslash R^\times = \{\frac{a}{b} \in R \mid p|a\}$ and deduce that R is local.

(c) Exercise: Let K be a field and let $R := \left\{A = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ 0 & a_1 & \dots & a_{n-1} \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & a_1 \end{pmatrix} \in M_n(K)\right\}$. Prove that $R\backslash R^\times = \{A \in R \mid a_1 = 0\}$ and deduce that R is local.

Proposition 10.2

Let R be a ring. Then TFAE:

(a) R is local;

(b) $R\backslash R^\times = J(R)$, i.e. $J(R)$ is the unique maximal left ideal of R;

(c) $R/J(R)$ is a skew-field.

Proof: Set $N := R\backslash R^\times$.

(a)⇒(b): Clear: $I \lhd R$ proper left ideal $\Rightarrow I \subseteq N$. Hence, by Proposition-Definition 9.1(c),

$$J(R) = \bigcap_{\substack{I \lhd R, \\ I \text{ maximal} \\ \text{left ideal}}} I \subseteq N\,.$$

Now, by (a) N is an ideal of R, hence N must be a maximal left ideal, even the unique one. It follows that $N = J(R)$.

(b)⇒(c): If $J(R)$ is the unique maximal left ideal of R, then in particular $R \neq 0$ and $R/J(R) \neq 0$. So let $r \in R\backslash J(R) \overset{(b)}{=} R^\times$. Then obviously $r + J(R) \in (R/J(R))^\times$. It follows that $R/J(R)$ is a skew-field.

(c)⇒(a): Since $R/J(R)$ is a skew-field by (c), $R/J(R) \neq 0$, so that $R \neq 0$ and there exists $a \in R\backslash J(R)$. Moreover, again by (c), $a + J(R) \in (R/J(R))^\times$, so that $\exists\, b \in R\backslash J(R)$ such that

$$ab + J(R) = 1 + J(R) \in R/J(R)$$

Therefore, $\exists\, c \in J(R)$ such that $ab = 1 - c$, which is invertible in R by Proposition-Definition 9.1(b). Hence $\exists\, d \in R$ such that $abd = (1-c)d = 1 \Rightarrow a \in R^\times$. Therefore $R\backslash J(R) = R^\times$, and it follows that $R\backslash R^\times = J(R)$ which is a two-sided ideal of R. ∎

Proposition 10.3 (*Fitting's Lemma*)

Let M be an R-module which has a composition series and let $\varphi \in \mathrm{End}_R(M)$ be an endomorphism of M. Then there exists $n \in \mathbb{Z}_{>0}$ such that

(i) $\varphi^n(M) = \varphi^{n+i}(M)$ for every $i \geqslant 1$;

(ii) $\ker(\varphi^n) = \ker(\varphi^{n+i})$ or every $i \geqslant 1$; and

(iii) $M = \varphi^n(M) \oplus \ker(\varphi^n)$.

Proof: By Corollary 8.4 the module M satisfies both A.C.C. and D.C.C. on submodules. Hence the two chains of submodules

$$\varphi(M) \supseteq \varphi^2(M) \supseteq \dots,$$

$$\ker(\varphi) \subseteq \ker(\varphi^2) \subseteq \dots$$

eventually become stationary. Therefore we can find an index n satisfying both (i) and (ii).

Exercise: Prove that $M = \varphi^n(M) \oplus \ker(\varphi^n)$. ■

Proposition 10.4

Let M be an R-module which has a composition series. Then:

$$M \text{ is indecomposable } \iff \mathrm{End}_R(M) \text{ is a local ring.}$$

Proof: "$\Rightarrow$": Assume that M is indecomposable. Let $\varphi \in \mathrm{End}_R(M)$. Then by Fitting's Lemma there exists $n \in \mathbb{Z}_{>0}$ such that $M = \varphi^n(M) \oplus \ker(\varphi^n)$. As M is indecomposable either $\varphi^n(M) = M$ and $\ker(\varphi^n) = 0$ or $\varphi^n(M) = 0$ and $\ker(\varphi^n) = M$.

- In the first case φ is bijective, hence invertible.
- In the second case φ is nilpotent.

Therefore, $N := \mathrm{End}_R(M) \backslash \mathrm{End}_R(M)^\times = \{\text{nilpotent elements of } \mathrm{End}_R(M)\}$.

Claim: N is a two-sided ideal of $\mathrm{End}_R(M)$.

Let $\varphi \in N$ and $m \in \mathbb{Z}_{>0}$ minimal such that $\varphi^m = 0$. Then

$$\varphi^{m-1}(\varphi\rho) = 0 = (\rho\varphi)\varphi^{m-1} \quad \forall\, \rho \in \mathrm{End}_R(M).$$

As $\varphi^{m-1} \neq 0$, $\varphi\rho$ and $\rho\varphi$ cannot be invertible, hence $\varphi\rho, \rho\varphi \in N$.

Next let $\varphi, \rho \in N$. If $\varphi + \rho =: \psi$ were invertible in $\mathrm{End}_R(M)$, then by the previous argument we would have $\psi^{-1}\rho, \psi^{-1}\varphi \in N$, which would be nilpotent. Hence

$$\psi^{-1}\varphi = \mathrm{Id}_M - \psi^{-1}\rho$$

would be invertible.

(Indeed, $\psi^{-1}\rho$ nilpotent $\Rightarrow (\mathrm{Id}_M - \psi^{-1}\rho)(\mathrm{Id}_M + \psi^{-1}\rho + (\psi^{-1}\rho)^2 + \dots + (\psi^{-1}\rho)^{a-1}) = \mathrm{Id}_M$, where a is minimal such that $(\psi^{-1}\rho)^a = 0$.)

This is a contradiction. Therefore $\varphi + \rho \in N$, which proves that N is an ideal.

Finally, it follows from the Claim and the definition that $\mathrm{End}_R(M)$ is local.

"$\Leftarrow$": Assume M is decomposable and let M_1, M_2 be proper submodules such that $M = M_1 \oplus M_2$. Then consider the two projections

$$\pi_1 : M_1 \oplus M_2 \longrightarrow M_1 \oplus M_2, (m_1, m_2) \mapsto (m_1, 0)$$

onto M_1 along M_2 and

$$\pi_2 : M_1 \oplus M_2 \longrightarrow M_1 \oplus M_2, (m_1, m_2) \mapsto (0, m_2)$$

onto M_2 along M_1. Clearly $\pi_1, \pi_2 \in \mathrm{End}_R(M)$ but $\pi_1, \pi_2 \notin \mathrm{End}_R(M)^\times$ since they are not surjective by construction. Now, as $\pi_2 = \mathrm{Id}_M - \pi_1$ is not invertible it follows from the characterisation of the Jacobson radical of Proposition-Definition 9.1(b) that $\pi_1 \notin J(\mathrm{End}_R(M))$. Therefore

$$\mathrm{End}_R(M) \setminus \mathrm{End}_R(M)^\times \neq J(\mathrm{End}_R(M))$$

and it follows from Proposition 10.2 that $\mathrm{End}_R(M)$ is not a local ring. ■

Next, we want to be able to decompose R-modules into direct sums of indecomposable submodules. The Krull-Schmidt Theorem will then provide us with certain uniqueness properties of such decompositions.

Proposition 10.5

Let M be an R-module. If M satisfies either A.C.C. or D.C.C., then M admits a decomposition into a direct sum of finitely many indecomposable R-submodules.

Proof: Let us assume that M is not expressible as a finite direct sum of indecomposable submodules. Then in particular M is decomposable, so that we may write $M = M_1 \oplus W_1$ as a direct sum of two proper submodules. W.l.o.g. we may assume that the statement is also false for W_1. Then we also have a decomposition $W_1 = M_2 \oplus W_2$, where M_2 and W_2 are proper sumbodules of W_1 with the statement being false for W_2. Iterating this argument yields the following infinite chains of submodules:

$$W_1 \supsetneq W_2 \supsetneq W_3 \supsetneq \cdots ,$$

$$M_1 \subsetneq M_1 \oplus M_2 \subsetneq M_1 \oplus M_2 \oplus M_3 \subsetneq \cdots .$$

The first chain contradicts D.C.C. and the second chain contradicts A.C.C.. The claim follows. ■

Theorem 10.6 (*Krull–Schmidt*)

Let M be an R-module which has a composition series. If

$$M = M_1 \oplus \cdots \oplus M_n = M'_1 \oplus \cdots \oplus M'_{n'} \qquad (n, n' \in \mathbb{Z}_{>0})$$

are two decomposition of M into direct sums of finitely many indecomposable R-submodules, then $n = n'$, and there exists a permutation $\pi \in \mathfrak{S}_n$ such that $M_i \cong M'_{\pi(i)}$ for each $1 \leqslant i \leqslant n$ and

$$M = M'_{\pi(1)} \oplus \cdots \oplus M'_{\pi(r)} \oplus \bigoplus_{j=r+1}^{n} M_j \qquad \text{for every } 1 \leqslant r \leqslant n.$$

Proof: For each $1 \leqslant i \leqslant n$ let

$$\pi_i : M = M_1 \oplus \cdots \oplus M_n \to M_i, m_1 + \ldots + m_n \mapsto m_i$$

be the projection on the i-th factor of first decomposition, and for each $1 \leqslant j \leqslant n'$ let

$$\psi_j : M = M'_1 \oplus \cdots \oplus M'_{n'} \to M'_j, m'_1 + \ldots + m'_{n'} \mapsto m'_j$$

be the projection on the j-th factor of second decomposition.

Claim: if $\psi \in \mathrm{End}_R(M)$ is such that $\pi_1 \circ \psi|_{M_1} : M_1 \to M_1$ is an isomorphism, then

$$M = \psi(M_1) \oplus M_2 \oplus \cdots \oplus M_n \text{ and } \psi(M_1) \cong M_1 .$$

Indeed: By the assumption of the claim, both $\psi|_{M_1} : M_1 \to \psi(M_1)$ and $\pi_1|_{\psi(M_1)} : \psi(M_1) \to M_1$ must be isomorphisms. Therefore $\psi(M_1) \cap \ker(\pi_1) = 0$, and for every $m \in M$ there exists $m_1' \in \psi(M_1)$ such that $\pi_1(m) = \pi_1(m_1')$, hence $m - m_1' \in \ker(\pi_1)$. It follows that

$$M = \psi(M_1) + \ker(\pi_1) = \psi(M_1) \oplus \ker(\pi_1) = \psi(M_1) \oplus M_2 \oplus \cdots \oplus M_n .$$

Hence the Claim holds.
Now, we have $\mathrm{Id}_M = \sum_{j=1}^{n'} \psi_j$, and so $\mathrm{Id}_{M_1} = \sum_{j=1}^{n'} \pi_1 \circ \psi_j|_{M_1} \in \mathrm{End}_R(M_1)$. But as M has a composition series, so has M_1, and therefore $\mathrm{End}_R(M_1)$ is local by Proposition 10.4. Thus if all the $\pi_1 \circ \psi_j|_{M_1} \in \mathrm{End}_R(M_1)$ are not invertible, they are all nilpotent and then so is Id_{M_1}, which is in turn not invertible. This is not possible, hence it follows that there exists an index j such that

$$\pi_1 \circ \psi_j|_{M_1} : M_1 \to M_1$$

is an isomorphism and the Claim implies that $M = \psi_j(M_1) \oplus M_2 \oplus \cdots \oplus M_n$ and $\psi_j(M_1) \cong M_1$.
We then set $\pi(1) := j$. By definition $\psi_j(M_1) \subseteq M_j'$ as M_j' is indecomposbale, so that

$$\psi_j(M_1) \cong M_j' = M'_{\pi(1)} .$$

Finally, an induction argument (Exercise!) yields:

$$M = M'_{\pi(1)} \oplus \cdots \oplus M'_{\pi(r)} \oplus \bigoplus_{j=r+1}^{n} M_j ,$$

mit $M'_{\pi(i)} \cong M_i$ $(1 \leqslant i \leqslant r)$. In particular, the case $r = n$ implies the equality $n = n'$. ■