Chapter 1

Background

This chapter introduces the terminology that will be used throughout the rest of the text. The first section contains a brief discussion about algorithms and complexity, followed by a list of examples of basic algorithmic questions (primality testing, integer factorisation, coprime factorisation). The remaining sections review basic facts of ring and module theory. We will focus on those results that are specific to noncommutative ring theory.

The main references for this chapter are: [66, 73], for the section concerning algorithms, and [56, 57, 58, 60], for the rest.

1.1 Algorithms and complexity

For an entirely formal discussion of algorithms and complexity, one needs to enter the realm of theoretical computer science jargon. Fortunately, however, this can be avoided, since it so happens that the intuitive notions we have of algorithms, "hardness" of a computational problem, "efficiency" etc., are enough for a meaningful discussion, and complexity theory appears to be "robust" enough to allow us to work with them.

Formally, an algorithm is a *Turing machine*. Intuitively, an algorithm is a sequence of steps that takes as *input* a finite sequence of nonnegative integers and produces an *output* in the form of another finite sequence of nonnegative integers. An integer is represented inside an algorithm by a string of *bits*, and a step in the algorithm is then a *bit operation*. It is also useful to have a notion of the "size" of an input. If $n \in \mathbb{Z}_{\geq 0}$, then the *length* of n is taken to be $\text{length}(n) := \log_2(n+2)$, reflecting the number of bits required to write n down in binary. The length of a negative integer m is $1 + \text{length}(|m|)$ and the length of an input is the sum of the lengths of the integers that compose it.

We would like to study the number of steps needed for an algorithm to perform a certain task. The *running time* represents the number of steps required to produce

an output. An algorithm is said to be *polynomial-time* if its running time is bounded above by a polynomial expression in the length of the input. The running time of an algorithm is often referred to as the *complexity of the algorithm*. In our case, this is the *bit-complexity*, as opposed to e.g. the *arithmetic complexity*, where a step is taken to be an arithmetic operation.

Naturally, we are interested in more than just performing arithmetic in $\mathbb{Z}$. However, virtually any mathematical object of interest can be *encoded* as a sequence of nonnegative integers. For the objects we are interested in, we will see exactly how to do this in the following two chapters.

Throughout this text, we will be exclusively interested in *deterministic polynomial-time algorithms*, i.e. algorithms in the running of which no random bit is generated. While allowing for probabilistic algorithms (e.g. *Las Vegas* or *Monte Carlo* algorithms) leads in practice to increased efficiency, these algorithms reveal less about the intrinsic difficulty of the problem at hand and are thus of less theoretical interest. We shall not think about them.

Furthermore, we will be content with being able to declare a certain algorithm as running in polynomial time, without computing exact exponents. The main reason for this is that we have not conceived the algorithms presented in this thesis with the intention of also implementing them. Therefore, there are countless improvements and randomised variations possible, which we have chosen not to explore in detail. Computing running times of an algorithm that is deliberately non-optimal seems futile.

Algorithms are often thought of as auxiliary objects, whose main reason for existence is to facilitate experimentation within computer algebra systems, with the purpose of confirming or invalidating hypotheses formulated in a more theoretical setting, providing examples or guiding the mathematician's intuition. In these cases, one is rarely interested in the "intrinsic" difficulty of a problem. Instead, one usually focuses one's attention to a very particular instance of a problem and only desires that the algorithm used to solve it output a result in a "reasonable" amount of time.

Under this paradigm, our preference for deterministic polynomial-time algorithms seems at least odd and perhaps even outdated. However, the viewpoint that we adopt in this thesis is that algorithms are mathematical objects *per se*, worthy of independent study. The fact that a problem can be solved deterministically in polynomial time says that the problem is not intrinsically difficult or mysterious.

1.1.1 Complexity classes

After fixing the model of computation, we may wish to classify problems based on the rate at which they use up a certain resource, e.g. time. This gives rise to *complexity classes*.

Within complexity classes, we can order the problems according to their difficulty by using *reductions*. A reduction from a problem Q to a problem P is an intermediate algorithm that, given a solution to a problem P, produces a solution to another

problem Q. We say Q reduces to P. This formulation suggests that problem P is "at least as hard" as Q. Intuitively, a reduction has to be an "easy" computation. We will mainly be interested in reductions that are deterministic polynomial-time algorithms.

The problems that are maximal elements with respect to the partial ordering induced by reductions are said to be *complete* for that complexity class. These problems capture the difficulty of the entire class. Moreover, the existence of a "natural" complete problem in a complexity class guarantees that the class is not "artificial".

The most important complexity classes are listed below, together with informal descriptions:

1. P: consists of problems that can be solved by a deterministic polynomial-time algorithm;

2. NP: consists of problems whose solutions can be verified deterministically in polynomial time;

3. NP-hard: a problem A is NP-hard if every problem B in NP can be reduced to A;

4. NP-complete: consists of problems that are both in NP and NP-hard.

Clearly P $\subseteq$ NP. The question whether the reverse inclusion holds is at this time one of the most important open problems in theoretical computer science.

If P $\neq$ NP, then there exist problems that are in NP, but are neither NP-complete, nor in P (see [73], Theorem 14.1). These are called NP-*intermediate* problems. However, no "natural" NP-intermediate problems are known.

1.1.2 Integer factorisation, coprime factorisation and primality testing

Perhaps the simplest question one might ask oneself is, if given a positive integer, whether one can find a factorisation into primes. Despite its fundamental nature, the problem of integer factorisation is notoriously difficult, which has made it the heart of many algorithms used in cryptography. It is easy to see that integer factorisation lies in the complexity class NP. However, no deterministic polynomial-time algorithm for it is known. It is also not thought to be NP-complete, and is hence considered to be a candidate for the NP-intermediate class. There is an extensive literature devoted to a large variety of algorithms for integer factorisation (see e.g. [13, 62]).

A similar and related problem is that of finding square divisors of a given integer, for which there is also no known deterministic polynomial-time algorithm (see [59] or [12], Section 7.1).

Factoring into primes is out of our reach. However, given a set of integers, we can simultaneously factor them into "coprime" factors.

Definition 1.1.1 ([8], Section 4,7)**.** *Let S be a finite set of positive integers. A* coprime base *for S is a set of positive integers B such that:*

(i) $1 \notin B$,
(ii) *elements of* B *are pairwise coprime,*
(iii) *each element of* S *can be written as a product of powers of elements of* B.

Theorem 1.1.2 ([8], Algorithm 18.1)**.** (Coprime Base Algorithm) *There exists a deterministic polynomial-time algorithm that takes as input a finite set of positive integers* S *and outputs a coprime base* B *for* S*, and a factorisation of each element of* S *into products of powers of elements of* B.

Furthermore, primality testing has been shown to be in P.

Theorem 1.1.3 ([1])**.** *There exists a deterministic polynomial-time algorithm that, given* $n \in \mathbb{Z}_{>1}$*, determines if* n *is prime.*

1.2 Basic ring theory

Definition 1.2.1. *A* ring *is a triple* $(R, +, \cdot)$*, where* R *is a set and* $+, \cdot : R \times R \to R$ *are binary operations such that:*

(R1) $(R, +)$ *is an abelian group,*
(R2) $(R, \cdot)$ *is a monoid, i.e. the operation* $\cdot$ *is associative and has an identity element,*
(R3) *for all* $x, y, z \in R$*, we have* $x \cdot (y + z) = x \cdot y + x \cdot z$ *and* $(x + y) \cdot z = x \cdot z + y \cdot z$.

We say $(R, +, \cdot)$ *is a commutative ring if, in addition* $(R, +, \cdot)$ *satisfies*

(R4) *for all* $x, y \in R$*, we have* $x \cdot y = y \cdot x$.

We denote the identity element of $(R, +)$ *by* 0_R*, and the identity element of* $(R, \cdot)$ *by* 1_R*. A subring of* $(R, +, \cdot)$ *is a subset* $S \subset R$ *such that* $(S, +, \cdot)$ *is itself a ring and* $1_R \in S$.

Definition 1.2.2. *Let* R *be a ring.*

(i) *We define the* centre *of* R *to be*

$$\mathrm{Z}(R) := \{r \in R \mid \forall s \in R : rs = sr\}.$$

(ii) *We define the* characteristic *of* R *to be the integer* $n \in \mathbb{Z}_{\geq 0}$ *such that* $\ker(\mathbb{Z} \to R^+,\ 1 \mapsto 1_R) = n\mathbb{Z}$.

Note 1.2.3. Let R be a finite ring and let R^+ denote the underlying abelian group of R. Then

$$\mathrm{char}(R) = \exp(R^+),$$

where $\exp(R^+)$ is the exponent of the abelian group R^+, i.e. the smallest positive integer m such that for all $r \in R^+$, the composition of r with itself m times equals the identity element.

Definition 1.2.4. *Let* $(R, +, \cdot)$ *be a ring. A* left ideal *of* R *is subset* $I \subset R$ *such that*

(I1) $(I,+)$ *is an abelian subgroup of* $(R,+)$,
(I2) *for all* $r \in R$ *and* $i \in I$, *we have* $ri \in I$.

Analogously, we can define right ideals. *An ideal is said to be* two-sided, *if it is both right and left.*

Definition 1.2.5. *Let* R *be a ring and* $I \subseteq R$ *a one-sided (or two-sided) ideal of* R. *Then*

(i) I *is said to be* nil *if every element of* I *is nilpotent.*
(ii) I *is said to be* nilpotent *if there exists* $n \in \mathbb{Z}_{>0}$ *such that* $I^n = 0$.

Definition 1.2.6. *A ring* R *is said to be* simple *if* R *is nonzero and the only two-sided ideals of* R *are* 0 *and* R.

Definition 1.2.7. *Let* $(R, +_R, \cdot_R)$, $(S, +_S, \cdot_S)$ *be two rings. A* ring homomorphism $F : R \to S$ *is a homomorphism of the underlying abelian groups, such that* $F(1_R) = 1_S$ *and for all* $r_1, r_2 \in R$, *we have* $F(r_1 \cdot_R r_2) = F(r_1) \cdot_S F(r_2)$. *A bijective ring homomorphism is called a* ring isomorphism.

Definition 1.2.8. *Let* R *be a ring. We define the* prime subring *of* R *to be the image of the ring homomorphism* $\mathbb{Z} \to R$, *given by* $1 \mapsto 1_R$.

Definition 1.2.9. *An* algebra *is a pair of rings,* k *and* R, *with* k *commutative, together with a ring homomorphism* $\varphi : k \to R$ *such that* $\mathrm{im}(\varphi) \subseteq \mathrm{Z}(R)$. *We then say that* R *is an* algebra over k.

Theorem 1.2.10 ([27], Theorem 1.1)**.** *Let* R *be a finite-dimensional algebra over a field* $\mathbb{F}$ *and let* $n := \dim_{\mathbb{F}}(R)$. *Then* R *is isomorphic to a subalgebra of* $\mathcal{M}_n(\mathbb{F})$.

Theorem 1.2.11 ([57], Theorem 3.1)**.** *Let* R *be a ring,* $n \in \mathbb{Z}_{>0}$ *and* $S = \mathcal{M}_n(R)$. *Then*

(i) *If* I *is a two-sided ideal of* R, *then* $\mathcal{M}_n(I)$ *is a two-sided ideal of* S.
(ii) *Every two-sided ideal of* S *is of the form* $\mathcal{M}_n(I)$, *for some two-sided ideal* I *of* R.

1.3 Basic module theory

Definition 1.3.1. *Let* R *be a ring. A* left R-module *is an abelian group* $(M,+)$, *together with an action* $R \times M \to M$ *such that:*

(M1) *for all* $r, s \in R$ *and* $x \in M$, *we have* $r(sx) = (rs)x$,
(M2) *for all* $r, s \in R$ *and* $x \in M$, *we have* $(r+s)x = rx + sx$,
(M3) *for all* $r \in R$ *and* $x, y \in M$, *we have* $r(x+y) = rx + ry$,
(M4) *for all* $x \in M$, *we have* $1_R x = x$.

Analogously, we can define right R-modules. *A* submodule *of a left* R*-module* M *is an abelian subgroup* $N \subset M$ *such that* $RN \subseteq N$.

Note 1.3.2. By a *module*, we will always mean a left module.

Definition 1.3.3. *Let R, S be two rings. An R-S-bimodule is an abelian group $(M, +)$ such that*

(B1) *M is a left R-module,*
(B2) *M is a right S-module,*
(B3) *for all $x \in M$, $r \in R$ and $s \in S$, we have $(rm)s = r(ms)$.*

We often write ${}_RM_S$ for an R-S-bimodule M.

Definition 1.3.4. *Let R be a ring. Then the* left-regular *R-module, ${}_RR$, is the abelian group $(R, +)$, together with an action $R \times R \to R$ given by left-multiplication. We can similarly define the* right-regular *R-module, R_R.*

Definition 1.3.5. *Let R be a ring. We say an R-module M is* free *if $M \cong \bigoplus_{i \in I} R_i =: R^{(I)}$ as R-modules, where I is an arbitrary indexing set and $R_i \cong R$ for all $i \in I$.*

Definition 1.3.6. *Let R be a ring. We say that R has left IBN (Invariant Basis Number) if for all $n, m \in \mathbb{Z}_{>0}$, whenever ${}_RR^n \cong {}_RR^m$, we have that $n = m$.*

Note 1.3.7 ([56], Corollary 1.2)**.** Let R be a ring. If ${}_RR^{(I)} \cong {}_RR^{(J)}$, where R is nonzero and I is infinite, then $|I| = |J|$.

Definition 1.3.8. *Let R be a ring with left IBN and let $M \cong R^{(I)}$ be a free R-module, for some indexing set I. The* rank *of M over R, which we denote by $\mathrm{rk}_R(M)$ is the cardinality of I.*

Example 1.3.9 ([56], Example 1.6)**.** The following rings have left IBN: division rings, local rings, nonzero commutative rings, nonzero left-artinian rings.

Definition 1.3.10. *Let R be a ring and M, N two R-modules. A* module homomorphism *$f : M \to N$ is a homomorphism of the underlying abelian groups, such that for all $r \in R$, we have $f(rm) = rf(m)$.*

Definition 1.3.11. *Let R be a ring and M an R-module. Then*

(i) *M is* simple *if $M \neq 0$ and its only submodules are 0 and M.*
(ii) *M is* indecomposable *if $M \neq 0$ and M cannot be written as the direct sum of two nontrivial, proper submodules.*
(iii) *M is* semisimple *if for any submodule $N \leq M$, there exists $C \leq M$ such that $M = N \oplus C$.*
(iv) *M is* artinian *if every descending chain of submodules of M stabilizes.*
(v) *M is* noetherian *if every ascending chain of submodules of M stabilizes.*
(vi) *M is* finitely generated *over R if there exists a finite set $X \subset M$ such that $M = \sum_{x \in X} Rx$.*
(vii) *M has* finite length *if M has a finite composition series, i.e. there exists $t \in \mathbb{Z}_{\geq 0}$ and a sequence $(N_i)_{i=0}^t$ of submodules of M such that $M = N_t > N_{t-1} > \ldots > N_1 > N_0 = 0$ and for all $0 \leq i \leq t-1$, we have that N_{i+1}/N_i is simple.*

Proposition 1.3.12 ([57], Theorem 19.16)**.** (Fitting's Lemma) *Let R be a ring, M a finite-length R-module and $f \in \mathrm{End}_R(M)$. Then there exists $n \in \mathbb{Z}_{>0}$ such that*

$$M = \ker(f^n) \oplus \mathrm{im}(f^n).$$

Theorem 1.3.13 ([57], Corollary 19.22)**.** (Krull-Remak-Schmidt Theorem) *Let R be a ring and M an R-module of finite length. Then there exist $n \in \mathbb{Z}_{>0}$ and indecomposable submodules $M_i \leq M$ such that*

$$M = \bigoplus_{i=1}^{n} M_i.$$

Moreover, n is uniquely determined, and the sequence $(M_i)_{i=1}^n$ is uniquely determined up to isomorphism, and up to a permutation.

Proposition 1.3.14. *Let R be a ring and $I \subset R$ a two-sided ideal. Let M be an abelian group. Then M is an R/I-module if and only if M is an R-module that is annihilated by I.*

Proof. Suppose M is an R-module that is annihilated by I. Then we can define an R/I-module structure on M, given by $R/I \times M \to M$, $(r+I)m \mapsto rm$. Conversely, if M is an R/I-module, then M is an R-module via $R \times M \to M$, $rm \mapsto \overline{r}m$, where $^- : R \to R/I$. Clearly M is then annihilated by I. □

1.4 More ring theory

1.4.1 Menagerie of rings I

Definition 1.4.1. *Let R be a ring. Then*

(i) *R is a* division ring *if $R \neq 0$ and for all $0 \neq r \in R$, there exists $s \in R$ such that $rs = sr = 1_R$.*
(ii) *R is* Dedekind-finite *if every element of R that is left-invertible is also right-invertible.*
(iii) *R is* left-artinian (resp. right-artinian) *if ${}_RR$ (resp. R_R) is artinian.*
(iv) *R is* left-noetherian (resp. right-noetherian) *if ${}_RR$ (resp. R_R) is noetherian.*

Proposition 1.4.2 ([57], Theorem 3.3)**.** *Let D be a division ring and let $R = \mathcal{M}_n(D)$, for some $n \in \mathbb{Z}_{>0}$. Then, up to isomorphism, R has a unique simple left module V, and $V \cong D^n$ as R-modules.*

1.4.2 Semisimple rings

One of the most important class of rings is that of *semisimple rings*.

Theorem 1.4.3 ([57], Theorems 2.5, 2.8, Corollary 3.7)**.** *Let R be a ring. Then the following are equivalent:*

(i) *The left-regular module, ${}_RR$, is semisimple.*
(ii) *All left R-modules are semisimple.*
(iii) *All left R-modules are projective.*
(iv) *All left R-modules are injective.*

Replacing "left" with "right" gives further equivalent conditions.

Definition 1.4.4. *Let R be a ring. If R satisfies any of the conditions of Theorem 1.4.3, then R is said to be a* semisimple ring.

Theorem 1.4.5 ([57], Theorem 3.5)**.** (Wedderburn's Theorem) *Let R be a ring. Then R is semisimple if and only if*

$$R \cong \prod_{i=1}^{t} \mathcal{M}_{n_i}(D_i),$$

where $t \in \mathbb{Z}_{\geq 0}$, $n_i \in \mathbb{Z}_{>0}$ and the D_i are division rings.

Note 1.4.6. Let R be a semisimple ring. Then the isomorphism classes of simple R-modules form a finite set. Moreover, the proof of Theorem 1.4.5 shows that

$$R \cong \prod_{S \text{ simple}} \mathrm{End}_{\mathrm{End}_R(S)}(S),$$

where the product ranges over the isomorphism classes of simple R-modules.

1.4.3 The Jacobson radical

The notion of semisimplicity is inextricably linked to that of the Jacobson radical.

Definition 1.4.7. *Let R be a ring. The* Jacobson radical *is defined as*

$$\mathrm{J}(R) := \bigcap_{\substack{I \subset R \\ I \text{ max left ideal}}} I.$$

Theorem 1.4.8 ([57], Corollary 4.2)**.** *Let R be a ring. Then*

$$\mathrm{J}(R) = \bigcap_{\substack{M \\ M \text{ simple } R\text{-module}}} \mathrm{ann}_R(M)$$

Theorem 1.4.9 ([57], Lemma 4.11, Theorems 4.12,4.14)**.** *Let R be a ring and $\mathrm{J}(R)$ its Jacobson radical. Then*

(i) *$\mathrm{J}(R)$ is a two-sided ideal of R.*
(ii) *If $I \subset R$ is a nil one-sided ideal, then $I \subseteq \mathrm{J}(R)$.*
(iii) *If R is left-artinian, then $\mathrm{J}(R)$ is the largest nilpotent left (resp. right) ideal of R.*
(iv) *R is semisimple if and only if R is left-artinian and $\mathrm{J}(R) = 0$.*

Theorem 1.4.10 ([18], Section 2)**.** *Let R be a finite-dimensional algebra of matrices over a field $\mathbb{F}$, where* $\mathrm{char}(\mathbb{F}) = 0$*. Then*

$$\mathrm{J}(R) = \{r \in R \mid \mathrm{Tr}(rs) = 0 \text{ for all } s \in R\}. \tag{1.1}$$

Proposition 1.4.11 ([57], Exercise 4.12B)**.** *For any collection of rings $\{A_i\}_{i\in I}$ we have $\mathrm{J}(\prod_i A_i) = \prod_i \mathrm{J}(A_i)$.*

Proposition 1.4.12 ([57], Example 21.14)**.** *Let R be a ring and $n \in \mathbb{Z}_{>0}$. Then $\mathrm{J}(\mathcal{M}_n(R)) = \mathcal{M}_n(\mathrm{J}(R))$.*

Proposition 1.4.13. *Let R be a ring, $I \subseteq R$ a two-sided nilpotent ideal and M an R-module. Then M is an R/I-modules, and M is simple over R/I if and only if it is simple over R.*

Proof. This is an easy corollary of Proposition 1.3.14. □

1.4.4 Menagerie of rings II

Definition 1.4.14. *Let R be a ring. Then*

(i) *R is* semilocal *if $R/\mathrm{J}(R)$ is semisimple.*
(ii) *R is* semiprimary *if $\mathrm{J}(R)$ is nilpotent and $R/\mathrm{J}(R)$ is semisimple.*
(iii) *R is* local *if $R/\mathrm{J}(R)$ is a division ring.*

Theorem 1.4.15 ([57], Theorem 19.1)**.** *Let R be a ring. Then R is local if and only if R has a unique maximal left (equiv. right) ideal.*

1.5 Idempotents

Definition 1.5.1. *Let R be a ring. An element $e \in R$ is an* idempotent *if $e^2 = e$. Two idempotents e_1 and e_2 are said to be* orthogonal *if $e_1e_2 = e_2e_1 = 0$.*

Definition 1.5.2. *Let R be a ring and $e \in R$ an idempotent. Then*

(i) *e is* central *if $e \in \mathrm{Z}(R)$.*
(ii) *e is* primitive *if $e \neq 0$ and it cannot be written as the sum of two nonzero orthogonal idempotents.*
(iii) *e is* centrally primitive *if $e \in \mathrm{Z}(R)$, $e \neq 0$ and e cannot be written as the sum of two nonzero orthogonal central idempotents.*

Definition 1.5.3. *A ring R is said to be* connected *if $R \neq 0$ and the only central idempotents in R are 0 and 1.*

Theorem 1.5.4. *Let R be a ring, and M an R-module.*

(i) *Let N, P be R-modules. Then $M = N \oplus P$ if and only if there exists an idempotent $e \in \mathrm{End}_R(M)$ such that $N = e(M)$ and $P = (1-e)(M)$.*

(ii) *Let A, B be R-modules. Then $R = A \oplus B$ if and only if there exists an idempotent $e \in R$ such that $A = Re$ and $B = R(1-e)$.*

(iii) ([77], Proposition 1.1.14) *Let R_1, R_2 be two-sided ideals of R. Then $R = R_1 \times R_2$ if and only if there exist central orthogonal idempotents e_1, e_2 such that $e_1 + e_2 = 1$, with $R_i = Re_i$, for $i = 1, 2$.*

Let R be a ring and suppose that $1 \in R$ can be written as a finite sum of orthogonal centrally primitive idempotents. Then such a decomposition $1 = e_1 + \ldots + e_n$ is unique up to permutation of the summands, and R can be written as a finite product of connected rings. Moreover, we have

$$R = Re_1 \oplus \ldots \oplus Re_n.$$

We call this a *block decomposition* of R.

Theorem 1.5.5 ([57], Proposition 22.2)**.** *Let R be a left-noetherian ring. Then R has a block decomposition.*

Proposition 1.5.6. *Let R be a ring. If R has a block decomposition $R = Re_1 + \ldots + Re_n$, where $\{e_i\}_{i=1}^n$ is a set of orthogonal centrally primitive idempotents of sum 1, then $\mathrm{Z}(R)$ has block decomposition $\mathrm{Z}(R) = \mathrm{Z}(R)e_1 + \ldots + \mathrm{Z}(R)e_n$.*

Theorem 1.5.7 ([57], Corollary 19.19)**.** *A nonzero left-artinian ring R is local if and only if R has no nontrivial idempotents.*

Proposition 1.5.8. *Let R be a left-artinian ring with Jacobson radical $\mathrm{J}(R)$. Then the natural projection $p : R \to R/\mathrm{J}(R)$ induces a surjective map on the set of idempotents.*

Proof. Let $E \in R$ be an idempotent. Then certainly $p(E)$ is an idempotent in $R/\mathrm{J}(R)$. Suppose $e \in R/\mathrm{J}(R)$ is an idempotent, i.e. $e^2 - e \in \mathrm{J}(R)$. What we want to find is an element satisfying $x^2 - x = 0$ in R, which is mapped to e. Consider the polynomial $F(x) = 3x^2 - 2x^3$. Let $e_1 := F(e)$. Then

$$e_1^2 - e_1 = (3e^2 - 2e^3)^2 - (3e^2 - 2e^3) = (4e^2 - 4e - 3)(e^2 - e)^2 \in \mathrm{J}(R)^2,$$

so $e_1^2 - e_1 \in \mathrm{J}(R)^2$. Moreover, $e_1 = e - (2e-1)(e^2 - e)$, so $e_1 \equiv e \mod \mathrm{J}(R)$.

We define $e_i := F(e_{i-1})$. By induction, we have $e_i^2 - e_i \in \mathrm{J}(R)^{2^i}$ and $e_i \equiv e \mod \mathrm{J}(R)$. Since R is left-artinian, $\mathrm{J}(R)$ is nilpotent, so there exists $n \in \mathbb{Z}_{\geq 0}$ such that $e_n^2 - e_n \in \mathrm{J}(R)^n = 0$. Then $E = e_n$ is the element we were after. □

Remark 1.5.9. The key to the above proof is that $e^2 - e$ is nilpotent. Hence we can use the same lifting technique against any nil ideal of R.

1.6 More module theory

1.6.1 Schur's Lemma, Converse Schur Lemma

Proposition 1.6.1 ([57], Lemma 3.6)**.** (Schur's Lemma) *Let R be a ring and M a simple module. Then $\mathrm{End}_R(M)$ is a division ring.*

Note 1.6.2. The converse is not necessarily true. To see this, let F be a field and consider the ring

$$R = \begin{pmatrix} F & F \\ 0 & F \end{pmatrix}$$

and the R-module

$$M = R \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & F \\ 0 & F \end{pmatrix}.$$

Then $\mathrm{End}_R(M) \cong F$, but M is not simple.

Definition 1.6.3. *Let R be a ring. We say ${}_R\mathfrak{M}$, the category of R-modules, satisfies the* converse of Schur's Lemma *if every R-module whose endomorphism ring is a division ring, is in fact simple.*

Theorem 1.6.4 ([71], Theorem 1.6)**.** (Converse Schur) *Let R be a semiprimary ring. Then the category of R-modules, ${}_R\mathfrak{M}$, satisfies the converse of Schur's Lemma if and only if R is a finite direct product of full matrix rings over local rings.*

1.6.2 Nakayama's Lemma

Theorem 1.6.5 ([57], Lemma 4.22)**.** (Nakayama's Lemma) *Let R be a ring and $J \subseteq R$ a left ideal of R. Then the following are equivalent:*

(i) $J \subseteq \mathrm{J}(R)$.
(ii) *For any finitely generated left R-module M,*

$$J \cdot M = M \Rightarrow M = 0.$$

(iii) *For any left R-modules $N \leq M$ such that M/N is finitely generated,*

$$N + J \cdot M = M \Rightarrow N = M.$$

1.6.3 Projective and injective modules

Definition 1.6.6. *Let R be a ring and P an R-module. Then P is said to be* projective *if for any surjective R-module homomorphism $g : B \twoheadrightarrow C$ and any R-module homomorphism $f : P \to C$, there exists an R-module homomorphism $h : P \to B$ such that $f = gh$:*

$$\begin{array}{ccccc} & & & & P \\ & & & \swarrow^{h} & \downarrow f \\ B & & \xrightarrow{g} & & C \longrightarrow 0. \end{array}$$

Theorem 1.6.7 ([56], §2A)**.** *Let R be a ring and P an R-module. Then the following are equivalent:*

(i) *P is projective.*
(ii) *P is a direct summand of a free R-module.*

(iii) *Every surjective R-module homomorphism $M \twoheadrightarrow P$ splits.*
(iv) *The functor $\mathrm{Hom}_R(P, -)$ is exact on ${}_R\mathfrak{M}$.*

Finitely generated projective modules over $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$, for $n \in \mathbb{Z}_{>0}$, are easy to describe.

Proposition 1.6.8. (i) *A $\mathbb{Z}$-module is finitely generated projective if and only if it is free of finite rank.*
(ii) *Let p be a prime and let $e \in \mathbb{Z}_{>0}$. A $\mathbb{Z}/p^e\mathbb{Z}$-module is finitely generated projective if and only if it is free of finite rank.*
(iii) *Let $n \in \mathbb{Z}_{>0}$. A $\mathbb{Z}/n\mathbb{Z}$-module is finitely generated projective if and only if it is a direct sum of copies of modules of the form $\mathbb{Z}/m\mathbb{Z}$, with $m \mid n$ such that $\gcd(\frac{n}{m}, m) = 1$.*

Proof. Part (i) is a consequence of $\mathbb{Z}$ being a principal ideal domain. Part (ii) holds since $\mathbb{Z}/p^e\mathbb{Z}$ is a local ring.

For part (iii), note that $\mathbb{Z}/m\mathbb{Z}$ is a $\mathbb{Z}/n\mathbb{Z}$-module if and only if $m \mid n$. It is now enough to show that if $m \mid n$, then $\mathbb{Z}/m\mathbb{Z}$ is $\mathbb{Z}/n\mathbb{Z}$-projective if and only if $\gcd(\frac{n}{m}, m) = 1$. Suppose $n = \prod_{i \in I} p_i^{a_i}$, where I is a finite indexing set and all p_i are distinct primes. Then $\gcd(\frac{n}{m}, m) = 1$ if and only if $m = \prod_{j \in J} p_j^{a_j}$, for some subset $J \subseteq I$. But this happens if and only if $\mathbb{Z}/m\mathbb{Z} = \bigoplus_{j \in J} \mathbb{Z}/p_j^{a_j}\mathbb{Z}$, which is a direct summand of $\mathbb{Z}/n\mathbb{Z}$. □

Proposition 1.6.9 ([20], Proposition 1.4)**.** *Let k be a commutative ring and let R be a k-algebra such that R is projective as a k-module. Let M be a projective R-module. Then M is projective over k.*

Definition 1.6.10. *Let R be a ring and I an R-module. Then I is said to be* injective *if for any injective R-module homomorphism $g : A \hookrightarrow B$ and any R-module homomorphism $f : A \to I$, there exists an R-module homomorphism $h : B \to I$ such that $f = hg$:*

$$\begin{array}{ccccc} & & I & & \\ & & {\scriptstyle f}\uparrow & \nwarrow^{h} & \\ 0 & \longrightarrow & A & \xrightarrow[g]{} & B. \end{array}$$

Definition 1.6.11. *Let R be a ring. If R is injective as a left-regular (resp. right-regular) module, we say that R is* left (resp. right) self-injective.

Theorem 1.6.12 ([56], §3A; [76], Proposition 3.42)**.** *Let R be a ring and I an R-module. Then the following are equivalent:*

(i) *I is injective.*
(ii) *Every injective R-module homomorphism $I \hookrightarrow M$ splits.*
(iii) (Baer's Test) *For all left ideals $K \subset R$, any R-homomorphism $K \to I$ can be extended to a map $R \to I$.*
(iv) *Every short exact sequence $0 \to I \to M \to N \to 0$, where M is an R-module and N is a cyclic R-module, splits.*
(v) *The functor $\mathrm{Hom}_R(-, I)$ is exact on ${}_R\mathfrak{M}$.*

1.6.4 Flat and finitely presented modules

Definition 1.6.13. *Let R be a ring and M an R-module. We say M is* flat *over R if the functor $- \otimes_R M$ is exact.*

Proposition 1.6.14 ([56], Proposition 4.3; [57], Theorem 23.20)**.** *Over a left-artinian ring, the notions of projective modules and flat modules coincide.*

Definition 1.6.15. *Let R be a ring and M an R-module. We say M is* finitely presented *over R if there is an exact sequence $R^m \to R^n \to M \to 0$, for some $m, n \in \mathbb{Z}_{\geq 0}$.*

Proposition 1.6.16 ([56], Proposition 4.29)**.** *A ring R is left-noetherian if and only if every finitely generated R-module is finitely presented.*

1.6.5 Rank of a projective module

In this section, suppose R is a commutative ring. Denote by $\mathrm{Spec}(R)$ the set of prime ideals of R and by $\mathrm{Max}(R)$ the set of maximal ideals of R. Let M be an R-module and $\mathfrak{p} \in \mathrm{Spec}(R)$. Then we denote by $M_{\mathfrak{p}}$ the localisation of M at $R \backslash \mathfrak{p}$.

Proposition 1.6.17 ([58], Corollary 3.4)**.** *Let M be a finitely presented R-module. Then the following are equivalent:*

(i) *M is projective over R,*
(ii) *for all $\mathfrak{m} \in \mathrm{Max}(R)$, we have that $M_{\mathfrak{m}}$ is projective over $R_{\mathfrak{m}}$,*
(iii) *for all $\mathfrak{p} \in \mathrm{Spec}(R)$, we have that $M_{\mathfrak{p}}$ is free over $R_{\mathfrak{p}}$.*

Let P be a projective R-module. Consider the function

$$\mathrm{rk}_R(P) : \mathrm{Spec}(R) \to \mathbb{Z}, \quad \mathfrak{p} \mapsto \mathrm{rk}_{R_{\mathfrak{p}}}(P_{\mathfrak{p}}).$$

Definition 1.6.18. *Let P be a projective R-module. If $\mathrm{rk}_R(P)$ is a constant function, then we say P has* constant rank*.*

Proposition 1.6.19 ([58], Corollary 3.6)**.** *If R is connected, then every projective R-module has constant rank.*

1.6.6 Hom & $\otimes$

Let R, S, T be rings, let M be an R-S-bimodule, N an R-T-bimodule and P an S-T-bimodule. Then

(i) $\mathrm{Hom}_R({}_RM_S, {}_RN_T)$ is an S-T-bimodule, where for all $s \in S$, $t \in T$, $m \in M$ and $f \in \mathrm{Hom}_R(M, N)$, we have $s \cdot f(m) = f(ms)$ and $(f \cdot t)(m) = f(m)t$.
(ii) $\mathrm{Hom}_T({}_RN_T, {}_SP_T)$ is an S-R-bimodule, where for all $s \in S$, $r \in R$, $n \in N$ and $g \in \mathrm{Hom}_T(N, P)$, we have that $s \cdot g(n) = sg(n)$ and $(g \cdot r)(n) = g(rn)$.
(iii) ${}_RM_S \otimes_S {}_SP_T$ is an R-T-bimodule, where for all $r \in R$, $t \in T$, $m \in M$ and $n \in N$, we have $r \cdot (m \otimes n) = rm \otimes n$ and $(m \otimes n) \cdot t = m \otimes nt$.

Proposition 1.6.20. *Let R, S be two rings, let $\alpha : R \to S$ be a ring homomorphism and M an S-R-bimodule. Then*

$$\mathrm{Hom}_S({}_SS_R, {}_SM_R) \cong {}_RM_R,$$

as R-R-bimodules.

Proposition 1.6.21 ([79], Proposition 18.44)**.** *Let R, S, T be rings, let M be an R-S-bimodule, N an S-T-bimodule and P an R-module. Then*

$$\mathrm{Hom}_R(M \otimes_S N, P) \cong \mathrm{Hom}_S(N, \mathrm{Hom}_R(M, P)),$$

as T-modules.

Proposition 1.6.22 ([58], Chapter I, Example 2.2(4), Proposition 2.13)**.** *Let R, R' be commutative rings, $\alpha : R \to R'$ a ring homomorphism and P, Q two finitely generated projective R-modules. Then*

$$\mathrm{Hom}_R(P, Q) \otimes_R R' \cong \mathrm{Hom}_{R'}(P \otimes_R R', Q \otimes_R R'),$$
$$(P \otimes_R Q) \otimes_R R' \cong (P \otimes_R R') \otimes_{R'} (Q \otimes_R R'),$$

as R'-modules.

1.6.7 Projective covers and injective hulls

Definition 1.6.23. *Let M be an R-module. A* superfluous submodule *of M is an R-module $S \subseteq M$ such that*

$$\forall N \leq M : (S + N = M \Rightarrow N = M).$$

If S is a superfluous submodule of M, we write $S \subseteq_s M$.

Definition 1.6.24. *Let M be an R-module. A* projective cover *of M is a pair (P, ϕ), where P is a projective R-module, $\phi : P \twoheadrightarrow M$ is an epimorphism, and $\ker(\phi) \subseteq_s P$.*

Theorem 1.6.25 ([57], Proposition 24.10, Example 24.11(3), Theorem 24.18)**.** *Let R be a ring.*

(i) *If R is left-artinian, then any R-module has a projective cover.*
(ii) *Let M be an R-module. Suppose (P, ϕ) and (P', ϕ') are two projective covers of M. Then there exists an isomorphism $\alpha : P' \to P$ such that $\phi' = \phi\alpha$.*
(iii) *Let $M_1, \ldots, M_n$ be R-modules. Suppose (P_i, ϕ_i) is a projective cover of M_i, for all $1 \leq i \leq n$. Then $(\bigoplus_{i=1}^n P_i, \bigoplus_{i=1}^n \phi_i)$ is a projective cover of $\bigoplus_{i=1}^n M_i$.*

Definition 1.6.26. *Let M be an R-module. An* essential extension *of M is an R-module $E \supseteq M$ such that*

$$\forall F \leq E : (F \cap M = 0 \Rightarrow F = 0)$$

If E is an essential extension of M, we write $M \subseteq_e E$.

Theorem 1.6.27 ([57], Theorem 3.30)**.** *Let R be a ring and $M \subseteq I$ two R-modules. Then the following are equivalent:*

(i) *I is maximal essential over M, i.e. $I \supseteq_e M$ and no module properly containing I can be an essential extension of M.*
(ii) *I is injective, and is essential over M.*
(iii) *I is minimal injective over M, i.e. I is injective and if I' is an injective module such that $M \subseteq I' \subseteq I$, then $I = I'$.*

Definition 1.6.28. *Let M be an R-module. An* injective hull *of M is an R-module $I \supseteq M$ satisfying one of the conditions of Theorem 1.6.27.*

Theorem 1.6.29 ([57], Lemma 3.29, Corollary 3.32, Example 3.38)**.** *Let R be a ring.*

(i) *Every R-module has an injective hull.*
(ii) *Let M be an R-module. Suppose I and I' are two injective hulls of M. Then there exists an isomorphism $I \to I'$ which is the identity on M.*
(iii) *Let $M_1, \ldots, M_n$ be R-modules. Suppose I_j is an injective hull of M_j, for all $1 \leq j \leq n$. Then $\bigoplus_{j=1}^n I_j$ is an injective hull of $\bigoplus_{j=1}^n M_j$.*

Theorem 1.6.30 ([56], Lemma 3.28, Theorem 3.30)**.** *Let R be a ring and M an R-module. Let I be an injective hull of M. Then M is injective if and only if $M = I$.*

1.7 Quasi-Frobenius rings

Theorem 1.7.1 ([56], Theorems 15.1, 15.9, Remark 15.10)**.** *Let R be a ring. Then the following are equivalent:*

(i) *R is left-noetherian and left self-injective.*
(ii) *R is right-noetherian and left self-injective.*
(iii) *R is left-noetherian and right self-injective.*
(iv) *R is right-noetherian and right self-injective.*
(v) *all projective R-modules are injective.*
(vi) *all injective R-module are projective.*

Definition 1.7.2. *Let R be a ring. If R satisfies any of the conditions of Theorem 1.7.1, then R is said to be a* quasi-Frobenius ring.

Example 1.7.3. The following rings are quasi-Frobenius:

(i) fields,
(ii) $\mathbb{Z}/n\mathbb{Z}$, for $n \in \mathbb{Z}_{>0}$,
(iii) semisimple rings,
(iv) $\mathcal{M}_n(R)$, for R a quasi-Frobenius ring and $n \in \mathbb{Z}_{\geq 0}$,
(v) the group ring $R[G]$, for R a quasi-Frobenius ring and G a finite group,
(vi) Galois rings (see Note 6.2.59).

1.8 Frobenius algebras and symmetric algebras

Let k be a commutative ring and A a k-algebra that is finitely generated projective as a module over k. The k-dual, $\mathrm{Hom}_k(A,k)$, is an A-A-bimodule. The left module structure is given by

$$a \cdot f = (x \mapsto f(xa)),$$

and the right module structure is given by

$$f \cdot a = (x \mapsto f(ax)),$$

where $a \in A$ and $f \in \mathrm{Hom}_k(A,k)$. These two actions are compatible: for any $a, a', x \in A$, we have $((a \cdot f) \cdot a')(x) = f(a'xa) = (a \cdot (f \cdot a'))(x)$.

Comparing the A-A-bimodule structures of A and $\mathrm{Hom}_k(A,k)$ leads to the following two notions.

Definition 1.8.1. *Let k be a commutative ring and A a k-algebra that is finitely generated projective as a module over k. If $A \cong \mathrm{Hom}_k(A,k)$ as left A-modules, then we say A is a* Frobenius algebra. *If $A \cong \mathrm{Hom}_k(A,k)$ as A-A-bimodules, then we say A is a* symmetric algebra.

Theorem 1.8.2 ([56], Theorems 16.54)**.** *Let k be a commutative ring and A a k-algebra that is finitely generated projective as a module over k. Then A is a symmetric algebra over k if and only if there exists a k-bilinear map $B : A \times A \to k$ such that*

(i) *B is symmetric, i.e. for all $x, y \in A$, we have $B(x,y) = B(y,x)$,*
(ii) *B is nonsingular, i.e. the map $A \to \mathrm{Hom}_k(A,k)$, given by $x \mapsto (y \mapsto B(x,y))$ is a k-module isomorphism,*
(iii) *B is associative, i.e. for all $x, y, z \in A$, we have $B(xy,z) = B(x,yz)$,*

Example 1.8.3 ([56], 16.56-59)**.** (Symmetric algebras)

1. Let k be a field and G a finite group. Then the group ring $A = k[G]$ is a symmetric k-algebra. To see this, consider the map $B : A \times A \to k$ given by $B(\sum_{g\in G} a_g g, \sum_{h\in G} b_h h) = \sum_{g\in G} a_g b_{g^{-1}}$, where for all $g \in G$, we have $a_g, b_g \in k$.
2. Let k be a field and $A = \mathcal{M}_n(k)$, for some $n \in \mathbb{Z}_{>0}$. Then A is a symmetric k-algebra. To see this, consider the map $B : A \times A \to k$, given by $B(X,Y) = \mathrm{tr}(XY)$, where tr denotes the usual trace map.
3. Let k be a field. Then any finite-dimensional semisimple k-algebra is symmetric.

1.8.1 Generators and progenerators

Definition 1.8.4. *Let R be a ring and M and R-module. The* trace ideal *of M over R is defined to be*

$$\mathfrak{T}_R(M) := \sum_{f \in \mathrm{Hom}_R(M,R)} \mathrm{im}(f).$$

Note 1.8.5. It is easy to check that $\mathfrak{T}_R(M)$ is a two-sided ideal of R.

Definition 1.8.6. *Let R be a ring. An R-module M is an* R-generator *if $\mathfrak{T}_R(M) = R$. If, in addition, M is finitely generated and projective, then it is said to be an* R-progenerator.

Note 1.8.7. Over a commutative ring R, any faithful finitely generated projective module is a progenerator. The converse also holds.

1.9 Duality

Let R be a finite ring. Denote by ${}^{\mathrm{fg}}_{R}\mathfrak{M}$ and $\mathfrak{M}^{\mathrm{fg}}_{R}$ the categories of finitely generated left, respectively right, R-modules.

Definition 1.9.1. *Let R be a finite ring and denote by ${}^{\mathrm{fg}}_{R}\mathfrak{M}$ and $\mathfrak{M}^{\mathrm{fg}}_{R}$ the categories of finitely generated left and right R-modules, respectively. We define the* character functors

$$\widehat{\ }\colon {}^{\mathrm{fg}}_{R}\mathfrak{M} \rightleftharpoons \mathfrak{M}^{\mathrm{fg}}_{R}, \quad M \mapsto \widehat{M} := \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z}).$$

The module $\widehat{M}$ is called the character module *of M.*

Theorem 1.9.2 ([56], §19C,D)**.** *Let R be a finite ring. Consider the contravariant functors*

$$F : {}^{\mathrm{fg}}_{R}\mathfrak{M} \longrightarrow \mathfrak{M}^{\mathrm{fg}}_{R} \quad \textit{and} \quad G : \mathfrak{M}^{\mathrm{fg}}_{R} \longrightarrow {}^{\mathrm{fg}}_{R}\mathfrak{M}, \tag{1.2}$$

defined by taking character modules. Then $G \circ F$ and $F \circ G$ are naturally equivalent to the identity functors, i.e. F and G define a duality between ${}^{\mathrm{fg}}_{R}\mathfrak{M}$ and $\mathfrak{M}^{\mathrm{fg}}_{R}$.