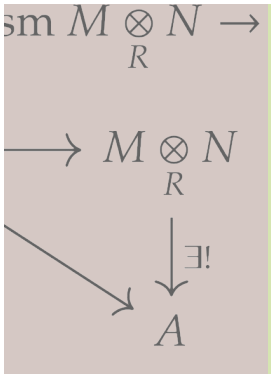
Yanqi Lake Lectures on Algebra

/ Wen-Wei Li



Part 1

Galois theory
Modules
Noncommutative rings
Representation of finite groups

中国科学院大学
University of Chinese Academy of Sciences

Errata

Version: 2020-03-15

The author is grateful to Professor Yongquan Hu for indicating many mistakes.

- **Exercise 1.4.2** Need an extra condition $p > 2$, otherwise there are obvious counterexamples.
- **Theorem 3.5.6** There are gaps in this proof. Please refer to J. Neukirch, *Algebraic Number Theory*, Chapter IV. §3 (especially (3.3) Theorem) for a complete proof which involves the use of Pontryagin duality, etc.
- **Section 8.2** The exposition here is in chaos. Please see the Part 3, §3.2 of these lecture notes for an improved version.
- **Section 9.4** In the definition of Galois action on W, we should assume Γ' to be of finite index and open in Γ. Also, the action should be additive, i.e. $\sigma(w_1 + w_2) = \sigma(w_1) + \sigma(w_2)$.
- **Proof of Theorem 9.4.1** The last step concerning the bijectivity between Hom-sets is unnecessary.
- **Lemma 12.2.3** The definition of $\mathrm{ind}_H^G(W) \to P(W)$ should map f to $\sum_{\bar{g} \in H\backslash G} g^{-1} \otimes f(g)$, where g is any representative of the coset $\bar{g}$.

  The inverse map $P(W) \to \mathrm{ind}_H^G(W)$ is obtained as follows: write $FG \otimes_{FH} W = \bigoplus_{\bar{g} \in H\backslash G} g^{-1}FH \otimes_{FH} W$. Given $g \in G$, let $\bar{g} \in H\backslash G$ be the coset it belongs to. Then g furnishes an isomorphism from the summand $g^{-1}FH \otimes_{FH} W = g^{-1} \otimes W$ to W, namely by discarding the first tensor slot g^{-1}. This allows us to associate to any element of $FG \otimes_{FH} W$ a function $f : G \to W$, which is readily seen to be in $\mathrm{ind}_H^G(W)$.

Yanqi Lake Lectures on Algebra

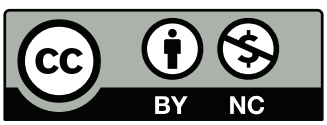
Part 1

Wen-Wei Li

Chinese Academy of Sciences

Email: wwli@math.ac.cn

Version: 2015-01-14



CONTENTS

FOREWORD

These lecture notes were prepared for the graduate course ALGEBRA I (210002H) during September 2014 – January 2015 at the University of Chinese Academy of Sciences, Yanqi Lake campus. The last few chapters on non-commutative rings and representation theory are based on earlier lectures during 2013-2014. Each lecture, or more appropriately each chapter in these notes, took roughly one week.

This is NOT a standalone lecture series on algebra. We presume some knowledge about:

(i) undergraduate abstract algebra, including the notions of groups and rings;
(ii) rudimentary set theory, namely some familiarity with cardinalities;
(iii) a certain "common sense" about categories and functors — the student is expected to take some statements for granted.

For the relevant backgrounds we will often refer to [11, 12, 16]; however, there was no prescribed textbook during our course. The author bene ted a lot from [16, 12, 14, 15, 22], as well as other textbooks in Chinese which are not included in the bibliography due to TEXnical di culties.

Our course was taught in 90% Taiwanese-accented mandarin and the lecture notes were delivered weekly. As a result these notes were written rather hastily with lots of mistakes in both mathematics and English, and they re ect the author's eccentric mathematical taste as well. Due to the manner in which these notes were prepared, there are minor inconsistencies in notations and there are no cross-references between di erent chapters. Categories are mentioned but the discussion is far from adequate; the expositions on representation theory are especially unsatisfactory. The author takes full responsibility for all these defects.

As for the photos and pictures in these notes (usually irrelevant), their sources are explicitly stated whenever possible.

These notes are certainly not intended for publication. Nonetheless some courageous people might nd them useful. The author would like to express his deep gratitude to all the students attending this course for their patience, tolerance and constant support, as well as many corrections.

* The cover page uses the fonts *Bebas Neue* and *League Gothique*, both licensed under the SIL Open Font License.

Wen-Wei Lı
Zhongguancun, Beijing,
January 2015

BACKGROUNDS

Throughout this course, the reader is assumed to have acquaintance with undergraduate algebra, namely the basic notions about sets, groups, rings and modules. Details can be found in any decent textbook such as [11]. In order to recall the relevant notions (in English!) and to x the notations, we give a recapitulation below.

Sets We work in the framework of ZFC set theory. The usual operations on sets are: $\cap$, $\cup$, $\times$, $\sqcup$ (= disjoint union); the Cartesian product (resp. intersection, union, disjoint union) of a family of sets $\{E_i : i \in I\}$ is denoted by $\prod_{i\in I} E_i$ (resp. $\bigcap_{i\in I} E_i$, $\bigcup_{i\in I} E_i$, $\bigsqcup_{i\in I}$); the set of maps from X to Y are denoted by Y^X. The cardinality of a set E is denoted by $|E|$ or $\#E$. For the most part in this course, we neglect set-theoretic issues such as proper classes, etc.

If $f : X \to Y$ is a map and $E \subset Y$, we write $f^{-1}(E) := \{x \in X : f(x) \in E\}$; when $E = \{y\}$ we use the shorthand $f^{-1}(y) = f^{-1}(\{y\})$, commonly called the *ber* of f over y.

The symbol $A := B$ reads as "A is de ned to be B". The arrow $\hookrightarrow$ (resp. $\twoheadrightarrow$) means an injection (resp. surjection), and $x \mapsto y$ means that the element x is mapped to y. If $\sim$ is an equivalence relation on a set E, the corresponding quotient set is denoted by $E/\sim$.

We admit *Zorn's Lemma*: let $(P, \leq)$ be a partially ordered set. If every chain (i.e. totally ordered subset) of P has an upper bound in P, then there exists a maximal element in P. Zorn's Lemma is known to be equivalent to the Axiom of Choice.

Group A group is a set G endowed with a binary operation ("multiplication") $(x, y) \mapsto x \cdot y = xy$, such that

- ⋆ associativity holds: $x(yz) = (xy)z$, so that one may safely write them as xyz;
- ⋆ the unit element 1 exists: $x \cdot 1 = 1 \cdot x = x$ for all x — we refrain from the common but awkward symbol e for the unit;
- ⋆ every element $x \in G$ is invertible: there exists $x^{-1} \in G$, necessarily unique, such that $xx^{-1} = x^{-1}x = 1$.

If we remove the existence of inverses, the structure so-obtained is called a *monoid*. When G is commutative/abelian, i.e. $xy = yx$ holds true for all $x, y \in G$, it is

customary to write the group operations in the additive manner: $x + y$, 0, $-x$ instead of xy, 1 and x^{-1}, respectively. In this case we say G is an additive group.

The notation $H \lhd G$ means that H is a normal subgroup of G. The symmetric group on n letters, say $\{1, \ldots, n\}$, will be denoted by $\mathfrak{S}_n$.

Rings Unless otherwise specified, the rings are assumed to have multiplicative unit element 1. Therefore, a ring R is an additive group $(R, +, 0)$ together with a multiplication map $(x, y) \mapsto x \cdot y = xy$ that makes $(R, \cdot, 1)$ into a monoid. These structures are related by *distributivity*:

$$x(y + z) = xy + xz, \quad z(x + y) = zx + zy.$$

The standard example for a commutative ring is the ring of integers $\mathbb{Z}$, the non-commutative case is best illustrated by the ring of $n \times n$-matrices. An element $x \in R$ is called *invertible* (or a *unit* of R) if $\exists y \in R,\ xy = yx = 1$; in this case y is unique and we denote it as x^{-1}. The units form a group under multiplication, denoted as $R^\times$.

Fields When $R \smallsetminus \{0\} = F^\times$, we call R a *division ring*; a field is a commutative division ring. We shall write

$$\mathbb{Q}, \mathbb{R}, \mathbb{C}$$

for the fields of rational, real and complex numbers. The finite field with q elements (q: a prime power) is denoted as $\mathbb{F}_q$.

Let $F[X]$ stand for the *ring of polynomials* in the indeterminate X with coefficients in F. Its field of fractions is denoted by $F(X)$, called the ring of *rational functions* in X. By construction, $F(X)$ consists of quotients P/Q where $P, Q \in F[X]$ and $Q \neq 0$. Likewise, one can define their multivariate avatars $F[X, Y, \ldots]$ and $F(X, Y, \ldots)$. We will also encounter the broader case of the polynomial ring $R[X, \cdots]$ over a commutative ring R.

Homomorphisms are maps that respect algebraic structures, namely the conditions such as $\varphi(xy) = \varphi(x)\varphi(y)$ and $\varphi(1) = 1$ are imposed. For a homomorphism φ between groups (resp. rings), we denote its *kernel* and *image* by $\ker(\varphi) := \varphi^{-1}(1)$ (resp. $\ker(\varphi) := \varphi^{-1}(0)$) and $\mathrm{im}(\varphi)$.

There is also a notion of "substructures", namely the subgroups, subrings, etc. A subgroup $N \subset G$ is called *normal* if $xNx^{-1} \subset N$ for all $x \in G$, in which case we write $N \lhd G$. To a normal subgroup one associates the *quotient group* G/N.

As for rings, it turns out that the two-sided *ideals* play a rôle similar to that of normal subgroups. Let R be a ring. An additive subgroup I of R is called a (two-sided) ideal if $xI \subset I$ and $Ix \subset I$ for all $x \in R$. For commutative rings one may simply speak of ideals, without specifying the sides. The quotient ring R/I is the additive quotient group R/I equipped with the multiplication $(x + I)(y + I) = xy + I$.

The two-sided ideal generated by elements $x_1, \ldots, x_n \in R$ will be written as

$$(x_1, \ldots, x_n).$$

Further discussions on rings and ideals will be deferred to another lecture.

LECTURE 1

FIELD EXTENSIONS

1.1 Fields

We begin by reviewing the rudiments of field theory. Any ring R admits exactly one homomorphism from $\mathbb{Z}$, namely

$$\begin{aligned} \mathbb{Z} &\longrightarrow R \\ a &\longmapsto a \cdot 1. \end{aligned}$$

Its image must be of the form $\mathbb{Z}/p\mathbb{Z}$ for a uniquely determined integer $p \geq 0$. Assume that R has no zero-divisors, i.e. $xy = 0 \iff x = 0 \vee y = 0$, then so is $\mathbb{Z}/p\mathbb{Z}$, and one concludes immediately that p is either a prime number or zero.

Definition 1.1.1. Let F be a field. Its *characteristic* is the number p above. Denote it by $\mathrm{char}(F)$.

Definition 1.1.2. An intersection of subfields of F is still a subfield, thus it makes sense to talk about the smallest subfield inside F. Call it the *prime field* of F.

Any subfield must contain $1, 0$ and every expression that can be obtained from field-theoretic operations. Thus

- ⋆ either $\mathrm{char}(F) = 0$, in which case $\mathbb{Z} \hookrightarrow F$ and we obtain a copy of $\mathbb{Q}$ inside F by inverting the nonzero integers;
- ⋆ or $\mathrm{char}(F) = p > 0$, in which case we obtain a copy of $\mathbb{Z}/p\mathbb{Z} =: \mathbb{F}_p$ inside F.

Summing up, the prime field of F is $\mathbb{Q}$ or $\mathbb{F}_p$, according to whether $\mathrm{char}(F)$ is zero or a prime number p.

Next comes the notion of *compositum*.

Definition 1.1.3. Let F, F' be two subfields of an ambient field L. Their compositum, written as FF', is the smallest subfield of L containing both F and F'. More concretely, the elements of FF' take the form

$$\frac{x_1x_1' + \cdots x_nx_n'}{y_1y_1' + \cdots y_my_m'} \in L$$

with $x_i, y_i \in F$, $x_i', y_i' \in F'$ such that the denominator is nonzero.

Likewise, the compositum of an arbitrary family of sub elds inside L can be de ned.

Note that a ring homomorphism between elds $\varphi : F \to E$ must have kernel equal to $\{0\}$. Thus, instead of talking about homomorphisms, one may concentrate on *embeddings* of a eld F into another eld. If $E \supset F$, we say that E is a (eld) extension of F; it is customary to write such an extension as E/F — do not confuse with quotients! Field extensions will be the main concern of this lecture.

Let E/F be an extension. Note that E forms an F-vector space: the addition in E and the scalar multiplication of F on E come from their ring structures.

De nition 1.1.4. The *degree* of E/F is de ned as $\dim_F E$, also written as $[E : F]$. Extensions of nite degree are called *nite extensions*.

Here $[E : F]$ is regarded as a cardinal number.

Lemma 1.1.5 (Tower property)**.** *If $F \subset E \subset L$ are elds, then*

$$[L : F] = [L : E][E : F]$$

as cardinal numbers. In particular, L/F is nite if and only if L/E and E/F are both nite.

Proof. Choose a basis B (resp. C) of the F-vector space E (resp. of the E-vector space L). Every element $v \in L$ has a be uniquely expression

$$v = \sum_{c \in C} \gamma_c c \quad (\text{ nite sum}),\ \gamma_c \in E.$$

Expanding each γ_c as an F-linear combination $\gamma_c = \sum_{b \in B} \gamma_{b,c} b$, we arrive at a unique expression

$$v = \sum_{\substack{b \in B \\ c \in C}} \gamma_{b,c} bc, \quad \gamma_{b,c} \in F.$$

This provides a basis for L which is in bijection with $B \times C$, proving our assertions. □

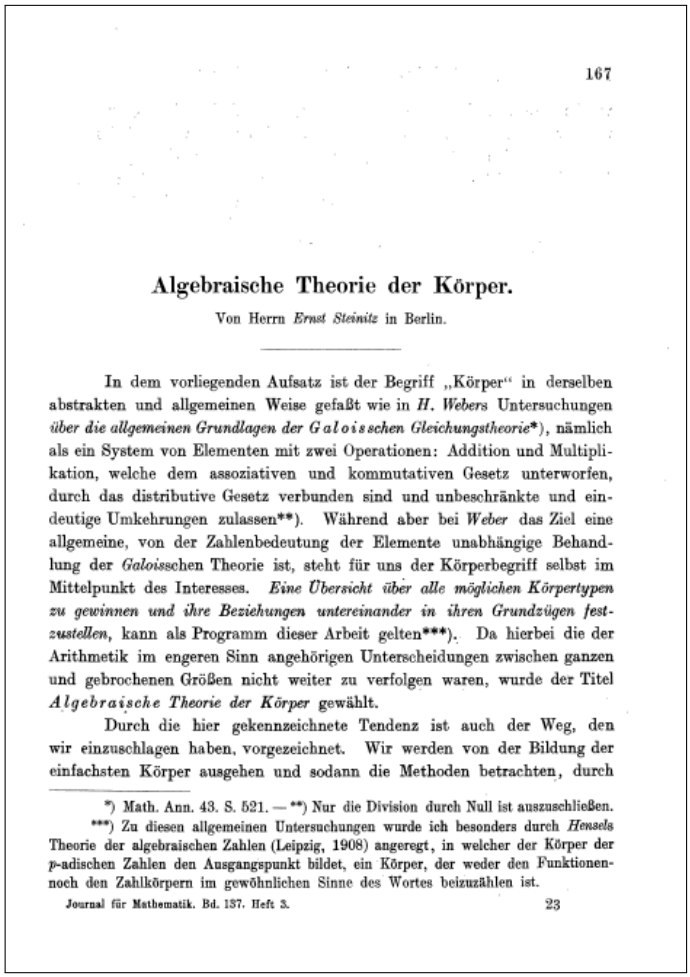
1.2 Algebraicity

The innocent-looking notion of niteness is directly related to *algebraicity*, as reviewed below. Consider an extension E/F. For any element $u \in E$, we write $F(u)$ as the sub eld generated by u, that is:

$$F(u) = \bigcap_{\substack{F \subset E' \subset E \\ u \in E'}} E' \subset E.$$

Its elements can be expressed as $P(u)/Q(u)$, where $P, Q \in F[X]$ are polynomials and $Q(u) \neq 0$. On the other hand, we denote

$$F[u] := \{P(u) : P \in F[X]\}$$



167

Algebraische Theorie der Körper.

Von Herrn *Ernst Steinitz* in Berlin.

In dem vorliegenden Aufsatz ist der Begriff „Körper" in derselben abstrakten und allgemeinen Weise gefaßt wie in *H. Webers* Untersuchungen *über die allgemeinen Grundlagen der Galoisschen Gleichungstheorie**), nämlich als ein System von Elementen mit zwei Operationen: Addition und Multiplikation, welche dem assoziativen und kommutativen Gesetz unterworfen, durch das distributive Gesetz verbunden sind und unbeschränkte und eindeutige Umkehrungen zulassen**). Während aber bei *Weber* das Ziel eine allgemeine, von der Zahlenbedeutung der Elemente unabhängige Behandlung der *Galois*schen Theorie ist, steht für uns der Körperbegriff selbst im Mittelpunkt des Interesses. *Eine Übersicht über alle möglichen Körpertypen zu gewinnen und ihre Beziehungen untereinander in ihren Grundzügen festzustellen*, kann als Programm dieser Arbeit gelten***). Da hierbei die der Arithmetik im engeren Sinn angehörigen Unterscheidungen zwischen ganzen und gebrochenen Größen nicht weiter zu verfolgen waren, wurde der Titel *Algebraische Theorie der Körper* gewählt.

Durch die hier gekennzeichnete Tendenz ist auch der Weg, den wir einzuschlagen haben, vorgezeichnet. Wir werden von der Bildung der einfachsten Körper ausgehen und sodann die Methoden betrachten, durch

*) Math. Ann. 43. S. 521. — **) Nur die Division durch Null ist auszuschließen.
***) Zu diesen allgemeinen Untersuchungen wurde ich besonders durch *Hensels* Theorie der algebraischen Zahlen (Leipzig, 1908) angeregt, in welcher der Körper der p-adischen Zahlen den Ausgangspunkt bildet, ein Körper, der weder den Funktionen- noch den Zahlkörpern im gewöhnlichen Sinne des Wortes beizuzählen ist.

Figure 1.1: Ernst Steinitz (1871-1928) initiated the axiomatic study of fields (in German: *der Körper*) in [25]. He also introduced the fundamental concepts such as prime fields, transcendence degree, etc. (DOI: 10.1515/crll.1910.137.167)

which is a subring of $F(u)$. Furthermore, we may allow more than one generators $u, \ldots,$, and obtain $F(u, \ldots)$ and $F[u, \ldots]$ in the evident manner.

The element u is said to be *algebraic* over F, if there exists a nonzero polynomial $P \in F[X]$ such that $P(u) = 0$. Non-algebraic elements are called *transcendental*. When $E = \mathbb{C} \supset \mathbb{Q} = F$, we recover the familiar notion of algebraic numbers.

Lemma 1.2.1. *If $u \in E$ is algebraic over F, there exists an irreducible polynomial $P \in F[X]$, unique up to multiplication by $F^\times$, such that*

$$[Q \in F[X],\ Q(u) = 0] \iff P|Q.$$

We may normalize P so that P is "monic": $P(X) = X^n + a_{n-1}X^{n-1} + \cdots a_0$. Call it the minimal polynomial *of u.*

Proof. Let P be a polynomial satisfying $P(u) = 0$ with lowest possible degree. It must be irreducible. If $Q(u) = 0$, Euclidean division furnishes $R \in F[X]$ with $\deg R < \deg P$ and $P|Q - R$. The minimality of $\deg P$ thus implies R is the zero polynomial. □

Conversely, finite extensions may be constructed by taking an irreducible $P \in F[X]$ and form the quotient ring $F[X]/(P)$, which is a field and contains $F = F \cdot (1 + (P))$. Indeed, the irreducibility of P implies that $F[X]/(P)$ is a field, by a standard result in algebra.

Proposition 1.2.2. *Let $u \in E$ be as above. Then u is algebraic over F if and only if $F(u)/F$ is finite; in this case $F(u) = F[u]$ and there is a ring isomorphism*

$$\begin{aligned} F[X]/(P) &\xrightarrow{\sim} F(u) \\ Q &\longmapsto Q(u), \end{aligned} \tag{1.1}$$

where P is the minimal polynomial of u. In particular, $[F(u) : F] = \deg P$.

Proof. Assume u algebraic and let $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ be the monic minimal polynomial of u. We claim that every element in $F[u] \smallsetminus \{0\}$ is invertible, and therefore $F(u) = F[u]$. Indeed, if $Q(u) \neq 0$, then $P \nmid Q$ and irreducibility of P together with the Euclidean division entail that

$$1 = PU + QV$$

for some $U, V \in F[X]$. Evaluation at u furnishes $Q(u)V(u) = 1$, whence our claim. It follows that the homomorphism (1.1) is surjective. The previous Lemma implies the injectivity of (1.1). Therefore $F[X]/(P) \xrightarrow{\sim} F(u)$.

Conversely, if $F(u)/F$ is finite, then there must be an F-linear relation between $1, u, u^2, \ldots$ which affords the required algebraic equation for u. □

On the other hand, the structure of $F(u)$ in the transcendental case is simpler — it is just the field of rational functions.

Proposition 1.2.3. *An element $u \in E$ is transcendental over F if and only if*

$$\begin{aligned} F(X) &\longrightarrow F(u) \\ Q/R &\longmapsto Q(u)/R(u), \quad Q, R \in F(X),\ R \neq 0 \end{aligned}$$

defines a ring homomorphism, in which case it is actually an isomorphism.

Proof. Since $F(u)$ consists of the "rational functions" in u, the map will be a surjective ring homomorphism provided that it is well-defined, which is in turn equivalent to that $R = 0 \iff R(u) = 0$ for any $R \in F[X]$. The last condition is clearly equivalent to the transcendence of u over F; it also implies that $F(X) \to F(u)$ is injective, thus is an isomorphism. □

Proposition 1.2.4. *Let E/F be an extension. If $\alpha, \beta \in E$ are algebraic over F, then*

- ⋆ $\alpha + \beta$,
- ⋆ $\alpha\beta$,
- ⋆ α^{-1} *(when $\alpha \neq 0$)*

are all algebraic over F. Consequently, a compositum of algebraic extensions is still algebraic.

Proof. Consider the extensions $F \subset F(\alpha) \subset F(\alpha, \beta)$. The elements listed above all belong to $F(\alpha, \beta)$. Note that β is algebraic over $F(\alpha)$ (of course, enlarging the base field preserves algebraicity). By Proposition 1.2.2, both $[F(\alpha) : F]$ and $[F(\alpha, \beta) : F(\alpha)]$ are finite. The assertion follows from Lemma 1.1.5. □

Note that this is just an abstract result: it is not so easy to determine the minimal polynomial of $\alpha+\beta$, etc. in practice. Another consequence is that the algebraic elements in E forms a subextension E^{alg}/F.

Exercise 1.2.5. Determine the minimal polynomial of the algebraic number $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$.

An extension E/F is called algebraic if every element $u \in E$ is algebraic over F. Proposition 1.2.2 implies that E/F is algebraic if and only if it is a union of finite extensions of F.

Exercise 1.2.6. If L/E and E/F are both algebraic, then L/F is algebraic as well.

At the other extreme, given a field F and a possibly infinite set Γ, we may form the field $F(\Gamma)$ of rational functions with indeterminates in Γ; when $\Gamma = \{X_1, \dots, X_n\}$ we recover the familiar $F(X_1, \dots, X_n)$. Unlike the algebraic setting, Γ is *algebraically independent*: there are no non-trivial polynomial relations among elements in Γ. It can be shown that every field extension E/F has a decomposition

$$E \underset{\text{algebraic}}{\supset} F(\Gamma) \supset F$$

for some algebraically independent subset $\Gamma \subset E$; moreover the cardinality of Γ is uniquely determined by E/F, called the *transcendence degree* of E/F. This should be compared with the the notio of bases and dimensions in linear algebra.

1.3 The algebraic closure

Definition 1.3.1. A field F is called *algebraically closed* if every polynomial $P \in F[X]$ has a root in F. This is equivalent to that every $P \in F[X]$ splits into linear factors (i.e. of degree one).

Equivalently, being algebraically closed means that every $P \in F[X]$ factors into linear factors: $P(X) = \prod_{i=1}^{\deg P}(X - a_i)$ where $a_i \in F$. The best known example is $\mathbb{C}$.

Henceforth we fix our "ground field" F and study various extensions thereof. Let E/F, E'/F be two extensions, an F-embedding is an embedding $E \to E'$ of fields which induces id on F. Likewise we have the notion of F-isomorphisms, etc.

Lemma 1.3.2. *Consider an extension $F(u)/F$ where u is algebraic with minimal polynomial P. If E/F is an extension and $v \in E$ satisfies $P(v) = 0$, then there exists a unique F-embedding $\iota : F(u) \to E$ such that $\iota(u) = v$.*

Proof. The uniqueness is clear. In view of Proposition 1.2.2, we may construct ι by the diagram

$$\begin{array}{ccccccc} & & & \overset{\iota}{\frown} & & & \\ F(u) & \xleftarrow{\sim} & F[X]/(P) & \xrightarrow{\sim} & F(v) & \hookrightarrow & E \\ u & \longleftarrow\!\shortmid & X & \shortmid\!\longrightarrow & v & & \end{array}$$

in which every arrow is an F-embedding. □

De nition 1.3.3. An algebraic extension $\bar{F}/F$ is called an *algebraic closure* of F if $\bar{F}$ is algebraically closed.

The basic example is the eld of algebraic numbers in $\mathbb{C}$ that forms an algebraic closure of $\mathbb{Q}$.

Theorem 1.3.4 (E. Steinitz)**.** *For every eld F, there exists an algebraic closure $\bar{F}$ of F. Moreover, $\bar{F}$ is unique up to F-isomorphisms.*

Proof. Establish the uniqueness rst. Let $\bar{F}, \bar{F}'$ be two algebraic closures. Introduce the relation $\leq$ on the nonempty set $\mathcal{P}$ of F-embeddings $E \to \bar{F}'$, where E/F is a subextension of $\bar{F}/F$, by stipulating that

$$(\iota : E \to \bar{F}') \leq (\iota_1 : E_1 \to \bar{F}') \iff [E \subset E_1,\ \iota_1|_E = \iota]\,.$$

It is easy to see that $(\mathcal{P}, \leq)$ is a partially ordered set. We want to apply Zorn's Lemma to get a maximal $\iota : E \to \bar{F}'$; indeed, every chain in $(\mathcal{P}, \leq)$ has an upper bound — simply take union! By Lemma 1.3.2, maximality implies $E = \bar{F}$.

It remains to show that $\iota(\bar{F}) = \bar{F}'$. To see this, note that the algebraically-closeness of $\bar{F}$ transports to $\iota(\bar{F})$. This implies $\iota(\bar{F}) = \bar{F}'$, since for every $u \in \bar{F}'$, the roots of the minimal polynomial of u over F already lie in $\iota(\bar{F})$.

As for the existence of $\bar{F}$, one seeks some sort of "maximal algebraic extension" of F and the construction is again based on Zorn's Lemma. However, manipulating the collection (hum?) of all algebraic extensions of F is somehow hazardous. So we appeal to the following device: there exists a set Ω such that for every algebraic extension E/F, the set E is in bijection with a subset of Ω. The basic idea is sketched as follows. write

$$E = \bigcup_{n \geq 1} E_n, \quad E_n := \{u \in E : [F(u) : F] = n\}.$$

For every n, the map that associates $u \in E_n$ with its minimal polynomial over F is at most n-to-1, so everything boils down to bound the cardinaltiy of $F[X] = \bigcup_{n \geq 1}\{P : \deg P = n\}$.

Now we consider the nonempty partially ordered set formed by algebraic extensions E/F, where $E \subset \Omega$ set-theoretically, and $\leq$ is de ned by eld extension. Again, Zorn's Lemma implies the existence of some maximal E/F. If E is not algebraically closed, we may construct an extension E'/E with $\infty > [E' : E] > 1$ by Lemma 1.2.2. The set E' being algebraic over E, thus over F by Exercise 1.2.6, it can be re-embedded into Ω; this would violate the maximality of E. □

See [16, p.231] for another famous proof due to E. Artin. It also relies on Zorn's Lemma, however.

Lemma 1.3.5. *Let K/F be an algebraic extension, then every F-embedding $\iota : K \to K$ is an F-automorphism.*

Proof. Let $v \in K$ and denote its minimal polynomial over F by P. Enumerate the roots of P inside K as $v = v_1, \ldots, v_n$ and set $K_0 := F(v_1, \ldots, v_m)$, which is nite over F. It follows that ι induces an F-embedding $K_0 \to K_0$, which must be an F-automorphism for dimensional reasons. As v is arbitrary, the surjectivity follows at once. □

1.4 Splitting elds and normality

De nition 1.4.1. An algebraic extension E/F is called *normal* if every irreducible polynomial in $F[X]$ splits into linear factors whenever it has a root in E.

Exercise 1.4.2. Let p be a prime number and $a \in \mathbb{Z}_{\geq 1}$ which is not a p-th power. Show that $\mathbb{Q}(a^{\frac{1}{p}})$ is not a normal extension of $\mathbb{Q}$.

De nition 1.4.3. Let $P \in F[X]$. An extension E/F is called a *splitting eld* for P if there exists $n = \deg P$ roots $u_1, \ldots, u_n \in E$ of P, and that $E = F(u_1, \ldots, u_n)$.

More generally, let $\{P_i : i \in I\}$ be a family of polynomials in $F[X]$. An extension E/F is called a splitting eld thereof if each P_i splits into linear factors over E and E is generated by the roots of all the P_i ($i \in I$) over F.

For the study of splitting elds and normality, it is often convenient to choose an algebraic closure $\bar{F}/F$. Note that the splitting eld inside $\bar{F}$ of a family of polynomials in $F[X]$ is truly canonical: simply add to F the roots of these polynomials in $\bar{F}$. It is actually the compositum inside $\bar{F}$ of the splitting elds of each P_i.

Lemma 1.4.4. *Splitting elds for a family $(P_i)_{i\in I}$ exist and is unique up to F-isomorphisms.*

Proof. To prove the existence, we x $\bar{F}/F$ and take the subextension of $\bar{F}/F$ generated by the roots of every P_i, as mentioned above.

To show the uniqueness, let E/F and E'/F be two splitting elds for $(P_i)_{i\in I}$. Take algebraic closures $\bar{E}/F$ and $\bar{E}'/F$; note that they are also algebraic closures of F. Hence there exists an F-isomorphism $\sigma : \bar{E} \xrightarrow{\sim} \bar{E}'$ by Theorem 1.3.4. The image $\sigma(E)$ is still a splitting eld of $(P_i)_{i\in I}$ sitting inside $\bar{F}'$ — such argument is known as *transport of structure*. Therefore we have $\sigma(E) = E'$ by the previous discussion about splitting elds inside an algebraic closure, and $\sigma : E \xrightarrow{\sim} E'$ is the required F-isomorphism. □

Proposition 1.4.5. *Let E/F be an algebraic extension, and choose an algebraic closure $\bar{F}$ of E. The following are equivalent.*

(i) *E/F is normal.*

(ii) *Every F-embedding ι of E into $\bar{F}$ satis es $\iota(E) = E$, thus induces an F-automorphism of E.*

(iii) *E is the splitting eld inside $\bar{F}$ of a family of polynomials in $F[X]$.*

Proof. (i) $\iff$ (ii): Assume (i). Given an F-embedding $\iota : E \to \bar{F}$, for any $u \in E$ with minimal polynomial $P \in F[X]$, we see that $\iota(u)$ is still a root of P since P has coe cients in F. By assumption, P splits into linear factors over E, hence $\iota(u) \in E$ and we conclude by Lemma 1.3.5 since u is arbitrary. Conversely, assume (ii) and let $P \in F[X]$ be irreducible with a root $u \in E$. For any root $v \in \bar{F}$ of P, Lemma 1.3.2 furnishes an F-embedding $E \to \bar{F}$ mapping u to v, therefore $v \in E$ as well. It follows that P splits into linear factors over E. The case of reducible P follows at once.

(ii) $\implies$ (iii): We contend that E is the splitting eld (in $\bar{F}$) of the family $\{P_u : u \in E\}$, where $P_u \in F[X]$ is the minimal polynomial of u. The inclusion $E \subset K$ is clear.

Conversely, the splitting field of P_u lies in E for every $u \in E$ since we have seen that (ii) implies (i).

(iii) $\Longrightarrow$ (ii): Suppose that E is the splitting field of $\{P_i : \in I\}$ inside $\bar{F}$. Let $\iota : E \to \bar{F}$ be an F-embedding, it suffices to show that ι induces an F-automorphism of the splitting field of each P_i. This is clear since ι permutes the roots of P_i. □

LECTURE 2

SEPARABILITY AND FINITE GALOIS EXTENSIONS

2.1 Separability

We always fix a ground field F. If E, E' are two extensions of F, we denote by $\mathrm{Hom}_F(E, E')$ the set of F-embeddings $E \to E'$. Similarly, we define the group of F-automorphisms $\mathrm{Aut}_F(E)$, etc.

Consider a finite extension $F(u)/F$ generated by a single element u, and let L/F be an algebraic extension in which P, the minimal polynomial of u over F, splits into linear factors. Recall that we have established the bijection

$$\begin{aligned} \mathrm{Hom}_F(F(u), L) &\xrightarrow{\sim} \{v \in L : P(v) = 0\} \\ \varphi &\longmapsto \varphi(u). \end{aligned}$$

In particular, $|\mathrm{Hom}_F(F(u), L)| \leq \deg P$. Strict inequality can hold when the characteristic $p := \mathrm{char}(F)$ is positive. This leads to the notion of *separability*.

Definition 2.1.1. Let $P \in F[X]$, $P(X) = \sum_{k=0}^{n} a_k X^k$. Define its derivative formally as

$$P'(X) := \sum_{k=1}^{n} k a_k X^{k-1} \quad \in F[X].$$

The rules $(P+Q)' = P' + Q'$, $(PQ)' = PQ' + P'Q$ and $(cP)' = cP'$, $c' = 0$ (for $c \in F$) still hold.

For $P, Q \in F[X]$, we have the notion of their *greatest common divisor* (P, Q); it is unique only up to $F[X]^\times = F^\times$. To obtain uniqueness, one may normalize (P, Q) to be a monic polynomial whenever $(P, Q) \neq 0$. Also note that $(P, 0) = P$.

Lemma 2.1.2. *Let L/F be an extension in which $P \in F[X]$ splits into linear factors. Then P has multiple roots in L if and only if $(P, P') \neq 1$. When P is irreducible, the latter condition holds if and only if $P' = 0$.*

Notice that the criterion $(P, P') \neq 1$ can be checked inside the ground field F, say by the Euclidean division procedure.

Proof. Write $P \in L[X]$ as $\prod_{k=1}^{n}(X - a_k)$ with $a_1, \ldots, a_n \in L$ being the roots. A straightforward manipulation gives the first assertion. When P is irreducible, $(P, P') \neq 1 \implies P | P' \implies P' = 0$ since $\deg P' < \deg P$. □

Definition 2.1.3. A polynomial $P \in F[X]$ is called *separable* if it has no multiple roots, i.e. $(P, P') = 1$.

We turn to the study of irreducible polynomials $P(X) = \sum_k a_k X^k$ with $P' = 0$. This is equivalent to $ka_k = 0$ for all $k \geq 1$. When $\mathrm{char}(F) = 0$, the only candidates are the constant polynomials. Assume hereafter that

$$p := \mathrm{char}(F) \text{ is a prime number.}$$

Then the polynomials P with $P' = 0$ take the form

$$P(X) = \sum_{\substack{k \geq 0 \\ p | k}} a_k X^k.$$

Write $P = P_1(X^p)$ by taking $P_1(X) = \sum_{p|k} a_k X^{k/p}$. If $P_1' = 0$, the procedure can be iterated so that eventually

$$P(X) = P^\flat(X^{p^m}), \quad P^\flat \in F[X], \ (P^\flat)' \neq 0. \tag{2.1}$$

for some $m \in \mathbb{Z}_{\geq 0}$. Note that $P^\flat$ is irreducible since P is. Fix an algebraic closure $\bar{F}/F$. It turns out that

$$\{\alpha \in \bar{F} : P(\alpha) = 0\} = \{\beta^{p^{-m}} : P^\flat(\beta) = 0\}, \tag{2.2}$$

where $\beta^{p^{-m}}$ is *the* p^m-th root of β in $\bar{F}$. In fact, we have

$$X^{p^m} - \beta = \left(X - \beta^{p^{-m}}\right)^{p^m}$$

over $\bar{F}$; this is because $p \cdot 1 = 0$ in $\bar{F}$ and the binomial coefficient $\binom{x}{y} = \frac{x!}{(x-y)!y!}$ satisfies

$$p \mid \binom{p}{a}, \quad 0 < a < p,$$

hence

$$(u + v)^p = u^p + v^p \quad \text{holds true in any extension of } F. \tag{2.3}$$

If the roots in (2.2) are to be counted with multiplicities, each $\beta^{p^{-m}}$ should appear p^m times. Summing up, the study of an inseparable irreducible P breaks into two stages: (i) the study of $P^\flat$, which is irreducible separable, and (ii) the study of "purely inseparable" polynomials of the form $X^{p^m} - b$.

Exercise 2.1.4. The study of purely inseparable polynomials can be further reduced to the case $b \notin F^p$. Under this assumption, show that the polynomial $X^{p^m} - b$ is irreducible. Use this to produce examples of inseparable fields.

Now we revert to the case of general characteristic and resume the study of embeddings.

Definition 2.1.5. Let E/F be an algebraic extension, define its *separable degree* as $[E : F]_s := |\mathrm{Hom}_F(E, \bar{F})|$. This is independent of the choice of the algebraic closure $\bar{F}/F$.

Lemma 2.1.6 (Tower property)**.** *For a tower $L/E/F$ of algebraic extensions, we have $[L : F]_s = [L : E]_s[E : F]_s$ as cardinal numbers.*

Proof. Extending the inclusion $F \hookrightarrow \bar{F}$ to $\tau : L \to \bar{F}$ is equivalent to (i) extending it to various $\sigma : E \to \bar{F}$, and then (ii) extending each $E \xrightarrow{\sigma} \sigma(E) \hookrightarrow \bar{F}$ to $\tau : L \to \bar{F}$. There are $[E : F]_s$ choices for the first step. As regards the second step, since $[L : E]_s$ is independent of the choice of the embedding of E into $\bar{F} = \bar{E}$, there are $[L : E]_s$ choices for each σ. □

Definition-Proposition 2.1.7. Let E/F be a finite extension, then $[E : F]_s | [E : F]$. Call E/F a *separable extension* if $[E : F]_s = [E : F]$.

Proof. Choose $u_1, \ldots, u_n$ so that $E = F(u_1, \ldots, u_n)$. Using the tower

$$E = F(u_1, \ldots, u_n) \supset F(u_1, \ldots, u_{n-1}) \supset \cdots \supset F(u_1) \supset F \tag{2.4}$$

and the tower properties of $[E : F]_s$ and $[E : F]$, we reduce immediately to the case $E = F(u)$. Let $P \in F[X]$ be the minimal polynomial of u, and express it as $P(X) = P^\flat(X^{p^m})$ as in the earlier discussions, where $P^\flat$ is separable. It follows that $\deg P = [F(u) : F]$ equals $[E : F]_s = \deg P^\flat$ (which is the number of distinct roots of P) times $[E : F]_i := p^m$. □

We have just used the observation that $F(u)/F$ is separable if and only if u has separable minimal polynomial. In this case we say u is a separable element. If $u \in E$ is separable over F, then u is separable over any intermediate field between E and F — indeed, if a polynomial has no multiple roots, then the same holds for its factors.

Lemma 2.1.8. *A finite extension E/F is separable if and only if every $u \in E$ is separable.*

Proof. Consider the tower (2.4). If every u_i has separable minimal polynomial over F (hence over any intermediate field), the tower properties will give $[E : F]_s = [E : F]$. Conversely, we may realize any given $u \in E$ as the u_1 in (2.4). The tower property, the hypothesis $[E : F]_s = [E : F]$ together with the bounds $[\cdots]_s \leq [\cdots]$ imply $[F(u_1) : F]_s = [F(u_1) : F]$, whence the separability of $u = u_1$. □

Hence we may extend the notion of separability to arbitrary algebraic extensions as follows.

Definition 2.1.9. An algebraic extension E/F is called separable if every element in E is separable over F.

Exercise 2.1.10. If L/E and E/F are separable, then so is L/F.

Exercise 2.1.11. Suppose E is generated by a family $\{u_i : i \in I\}$ over F, show that E/F is separable if each u_i is. Hence a compositum of separable extensions is still separable.

We say a field L is *separably closed* if any separable irreducible polynomial has a root in L. As in the case of algebraic extensions, there is a notion of *separable closure* F^{sep}/F, which is a separable extension with F^{sep} separably closed. Again, we have:

- ⋆ Existence of F^{sep}/F: simply take the subextension of $\bar{F}/F$ generated by all separable elements, or the compositum of all separable subextensions of $\bar{F}/F$. In fact, this is the only choice of a separable closure sitting inside $\bar{F}$!
- ⋆ Uniqueness up to F-isomorphisms: let F_1^{sep} and F_2^{sep} be two separable closures. Embed them into algebraic closures, say $F_i^{\mathrm{sep}} \subset \bar{F}_i$ for $i = 1, 2$. Since there exists an F-isomorphism $\tau : \bar{F}_1 \xrightarrow{\sim} \bar{F}_2$, we reduce immediately to the case that $F_1^{\mathrm{sep}}, F_2^{\mathrm{sep}} \subset \bar{F}$, and it has been observed that $F_1^{\mathrm{sep}} = F_2^{\mathrm{sep}}$ in this case.

Proposition 2.1.12. *The separable closure F^{sep}/F is a normal extension.*

Proof. We may assume $F^{\mathrm{sep}} \subset \bar{F}$. Then it is the splitting field of the family of separable irreducible polynomials over F. □

2.2 Purely inseparable extensions

In this section we assume $p := \mathrm{char}(F) > 0$, otherwise everything would be separable.

Definition 2.2.1. Call an algebraic extension E/F *purely inseparable* if every element $u \in E$ satisfies $u^{p^m} \in F$ for some m.

We use the shorthand $E \subset F^{1/p^\infty}$ for the last condition defining pure inseparability. It makes perfect sense if E is embedded into an algebraic closure $\bar{F}$ and F^{1/p^∞} is taken to be $\bigcup_m \{u \in \bar{F} : u^{p^m} \in F\}$, which forms a subfield by (2.3).

Note that $[E : F]_s = 1$ if E is purely inseparable, since we have observed that a polynomial of the form $X^{p^m} - b$ has only one root in $\bar{F}$. The assertions below are immediate.

Exercise 2.2.2. If L/E and E/F are purely inseparable, then so is L/F. A compositum of purely inseparable extensions of F is still purely inseparable.

For a finite extension E/F, we set the *inseparable degree* to be

$$[E : F]_i := [E : F]/[E : F]_s.$$

It is an integer by Definition-Proposition 2.1.7. Since the degree and separable degree both satisfy tower property (Lemma 2.1.6), so do the inseparable degree for finite extensions: we have $[L : F]_i = [L : E]_i[E : F]_i$.

Proposition 2.2.3. *Suppose E/F is an algebraic extension with $p := \mathrm{char}(F) > 0$. Let E_s be the maximal separable subextension, which makes sense by the preceding exercises. Then E/E_s is purely inseparable. When E/F is finite, we have $[E : F]_s = [E_s : F]$ and $[E : F]_i = [E : E_s]$.*

Proof. Let $u \in E$. By (2.1), there exists $m \geq 0$ such that u^{p^m} has a separable minimal polynomial $P^\flat \in F[X]$, thus $u \in (E_s)^{1/p^\infty} \cap E$. We conclude that E/E_s is purely inseparable. The rest follows readily by tower properties. □

Exercise 2.2.4. A field is called *perfect* if every algebraic extension of F is separable. Show that a field F with $p := \mathrm{char}(F) > 0$ is perfect if and only if $F = F^p := \{x^p : x \in F\}$.

2.3 The primitive element theorem

Theorem 2.3.1 (Steinitz). *Let L/F be a finite extension. There exists an element $u \in E$ with $L = F(u)$ if and only if there are only finitely many intermediate fields E (that is, $L \subset E \subset F$).*

Proof. To begin with, we assume F finite. Then there are only finitely many intermediate fields between L and F. On the other hand,a well-known fact (eg. [11, Theorem 2.18]) says that the finite group $L^\times$ is cyclic; any generator of $L^\times$ will then generate L as an extension of F.

Assume F in finite and $L = F(u)$. For any intermediate field E we set $P_E \in E[X]$ to be the minimal polynomial of u over E, thus $P_E | P_F$; recall that the minimal polynomials are normalized to have leading coefficient one. We claim that $E = E(c_0, \ldots)$ where $c_0, \ldots$ are the coefficients of P_E. Indeed, P_E is irreducible over $E(c_0, \ldots) \subset E$, so

$$[L : E] = \deg P_E = [L : E(c_0, \ldots)]$$

which implies $E = E(c_0, \ldots)$. It follows that the map

$$\begin{aligned} \{\text{intermediate fields}\} &\longrightarrow \{\text{monic factors of } P_F \text{ in } \bar{F}[X]\} \\ E &\longmapsto P_E \end{aligned}$$

is injective. The right-hand side is finite.

Conversely, if F is in finite and there are only finitely many intermediate fields, we may choose $u \in L$ o the (finite) union of proper subextension of L, by using the next exercise, Then $F(u) = L$. □

Exercise 2.3.2. Let F be an in finite field, $n \geq 1$ and $f(X_1, \ldots, X_n) \in F[X_1, \ldots, X_n]$ be a nonzero polynomial. Show that there exists $(x_1, \ldots, x_n) \in F^n$ with $f(x_1, \ldots, x_n) \neq 0$.

Example 2.3.3. Let $\Bbbk$ be a field with characteristic $p > 0$. Consider the field of rational functions $F := \Bbbk(X, Y)$ in two variables. Take $x = X^{1/p}$ and $y = Y^{1/p}$ inside an algebraic closure $\bar{F}$, and form the extension $F(x, y)/F$. Note that

- ⋆ $[F(x, y) : F] = [F(x, y) : F(x)][F(x) : F] = p^2$, and
- ⋆ every $\gamma \in F(x, y)$ satisfies $\gamma^p \in F$.

Therefore there is no element $u \in F(x, y)$ such that $F(x, y) = F(u)$.

Theorem 2.3.4. *Let E/F be a separable finite extension. There exists $u \in E$ such that $E = F(u)$. If F is in finite and $E = F(u_1, \ldots, u_n)$, then u can be taken to be an F-linear combination of $u_1, \ldots, u_n$.*

Proof. As in the proof of Theorem 2.3.1, we may assume F in nite. Let us begin with the case $E = F(u, v)$. Let $P, Q \in F[X]$ be the minimal polynomials of u and v, respectively. We set out to show that for "general" $t \in F^\times$ we have $v \in F(u + tv)$, then it follows that $u = (u + tv) - tv \in F(u + tv)$ as well, hence $F(u, v) = F(u + tv)$.

Embed $F(u, v)$ into $\bar{F}$ and consider the polynomials

$$P(u + tv - tX), Q(X) \in F(u + tv)[X].$$

Form their greatest common divisor R. Since v is a common root of $P(u + tv - tX)$ and $Q(X)$ in $\bar{F}$, we have $\deg R \geq 1$. We proceed to show that $\deg R = 1$, which will imply that $R(X) = X - v$ and thus $v \in F(u + tv)$ as required.

If $\deg R > 1$, then the fact $R|Q$ and the separability of Q would imply that some root $v' \neq v$ in $\bar{F}$ is also a root of R. Hence $P(u + t(v - v')) = 0$, and

$$(u - u') + t(v - v') = 0, \quad u \neq u' : \text{roots of } P, \quad v \neq v' : \text{roots of } Q. \tag{2.5}$$

in $\bar{F}$. Since F is in nite, we can always choose $t \in F^\times$ to rule out (2.5) for any pairs of roots $u \neq u'$ and $v \neq v'$. In general, this procedure yields a sequence $v_1, \ldots, v_{n-1} \in L$ such that

$$\begin{aligned} E &= F(u_1, \ldots, u_{n-2})(u_{n-1}, u_n) = F(u_1, \ldots, u_{n-2})(v_1) = F(u_1, \ldots)(u_{n-2}, v_1) \\ &= F(u_1, \ldots, u_{n-3})(v_2) = \cdots = F(v_{n-1}) \end{aligned}$$

and v_{n-1} is an F-linear combination of $u_1, \ldots, u_n$, as required. □

This result can also be deduced from Theorem 2.3.1 by taking the Galois closure (De nition 2.4.3) of E and appeal to results in Galois theory, namely the Lemma 2.4.5.

2.4 Galois extensions and Galois groups

Let E/F be an extension, we write $\mathrm{Aut}_F(E)$ for the group of F-automorphisms, the binary operation being the composition of automorphisms $(\sigma, \tau) \mapsto \sigma \circ \tau$. We shall write $\mathrm{Aut}(E)$ for the group of all eld automorphisms of E; it equals $\mathrm{Aut}_{\Bbbk}(E)$ where $\Bbbk$ stands for the prime eld of E, so this is actually a special case.

The relation called "transport of structure" (after N. Bourbaki)

$$\mathrm{Aut}_{\sigma(K)}(E) = \sigma \mathrm{Aut}_K(E) \sigma^{-1}, \quad \sigma \in \mathrm{Aut}_F(E) \tag{2.6}$$

holds true for any intermediate eld $E \supset K \supset F$.

There are two basic operations.

1. To any subgroup H of $\mathrm{Aut}_F(E)$ we attach the corresponding *xed eld*

$$E^H := \{\alpha \in E : \forall \tau \in H,\ \tau(\alpha) = \alpha\}.$$

   Obviously E^Γ is a subextension of E/F.

2. To any subextension K/F of E we attach the subgroup $\mathrm{Aut}_K(E)$ of $\mathrm{Aut}_F(E)$.

There operations satisfy

$$\begin{aligned} H_1 \subset H_2 &\implies E^{H_1} \supset E^{H_2}, \\ K_1 \subset K_2 &\implies \mathrm{Aut}_{K_1}(E) \supset \mathrm{Aut}_{K_2}(E). \end{aligned} \tag{2.7}$$

De nition 2.4.1. By a *Galois extension* of F we mean a normal and separable algebraic extension. The *Galois group* of a Galois extension E/F is $\mathrm{Gal}(E/F) := \mathrm{Aut}_F(E)$.

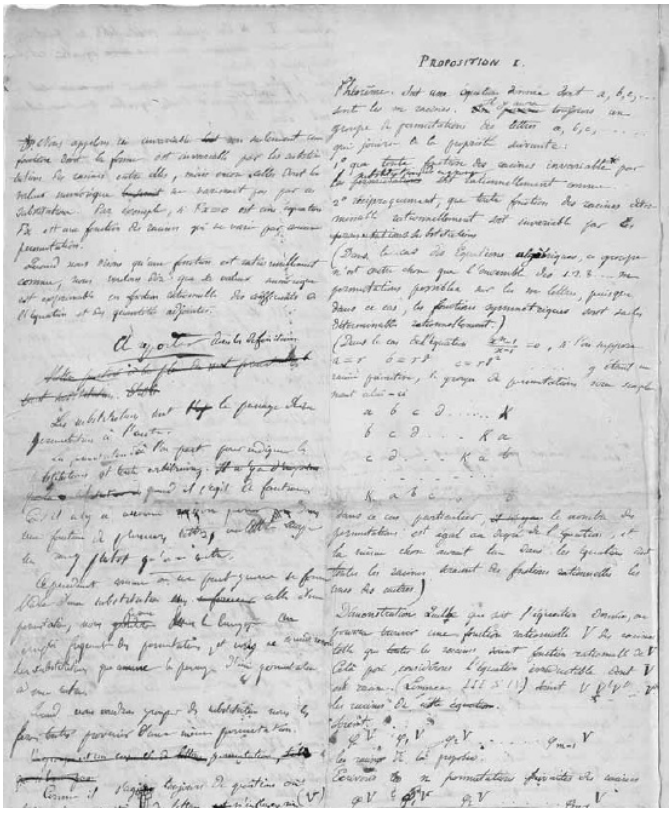


Figure 2.1: Fragments of É. Galois' First Memoir. Source: [20, IV.1].

Exercise 2.4.2. Show the following properties.

(i) Consider the tower $L \supset E \supset F$. If L/F is Galois, then so is L/E.
(ii) If L/F is Galois and E/F is normal, then E/F is Galois.
(iii) Composita of Galois extensions of F are still Galois.

De nition 2.4.3. Let E/F be a separable extension. The *Galois closure* inside some algebraic closure $\bar{F}$ is the smallest Galois extension containing E; it is given by the compositum of $\sigma(E)$, $\sigma \in \mathrm{Hom}_F(E, \bar{F})$.

Fix an algebraic closure $\bar{F}/F$, then the normality implies that $\mathrm{Gal}(E/F)$ equals the set $\mathrm{Hom}_F(E, \bar{F})$, and separability implies that the latter set has cardinality $[E : F]$ when E/F is nite. Hence

$$|\mathrm{Gal}(E/F)| = [E : F] \quad \text{for nite extensions.} \tag{2.8}$$

Remark 2.4.4. In Galois' original de nition, he only considered the splitting elds of a single polynomial, and the Galois group was in terms of permutations of roots. The interpretation via automorphisms was later conceived by Dedekind and appeared in Weber's work *Lehrbuch der Algebra* (1895).

Lemma 2.4.5. *Let E/F be a Galois extension, then $E^{\mathrm{Gal}(E/F)} = F$. Furthermore, the map that sends an intermediate eld K to the subgroup $\mathrm{Gal}(E/K)$ of $\mathrm{Gal}(E/F)$ is an injection.*

Proof. Evidently $F \subset E^{\mathrm{Gal}(E/F)}$. For any $u \in E^{\mathrm{Gal}(E/F)}$, denote its minimal polynomial by $P \in F[X]$, which must be separable. If $v \in \bar{F}$ (a chosen algebraic closure) is a root of P, we have seen that there is an F-embedding $F(u) \to \bar{F}$ mapping u to v; it extends to an element σ of $\mathrm{Gal}(E/F) = \mathrm{Aut}_F(E)$. By assumption $v = \sigma(u) = u$. Therefore $\deg P = 1$ and $u \in F$.

Since for any intermediate eld K, we have seen that E/K is Galois and $K = E^{\mathrm{Gal}(E/K)}$, the second assertion follows immediately. □

Notice that the map $K \mapsto \mathrm{Gal}(E/K)$ is not surjective in general for in nite Galois extensions.

Lemma 2.4.6 (E. Artin)**.** *Let E be a eld and $H \subset \mathrm{Aut}(E)$ is a nite subgroup. Then E/E^H is a Galois extension of degree $|H|$, with Galois group $\mathrm{Gal}(E^H/E) = H$.*

Proof. Let $u \in E$ and consider the nite H-orbit $O := \{\tau(u) : \tau \in H\}$ (without multiplicities) in E. Let $P_u(X) := \prod_{\alpha \in O}(X - \alpha) \in E[X]$. Notice that $\mathrm{Aut}(E)$ acts on the ring $E[X]$ by acting on the coe cients of polynomials. Thus P_u is H- xed so $P_u \in E^H[X]$; moreover P_u is separable of degree $= |O| \leq |H|$. It is clear that

$$H \subset \mathrm{Gal}(E/E^H). \tag{2.9}$$

Next, we claim that $[E : E^H] \leq |H|$. Indeed, pick any $u \in E$ with largest possible $[E^H(u) : E^H]$ (bounded by $|H|$). We must have $E = E^H(u)$, otherwise there exists $v \in E$ with a tower $E^H(u, v) \supsetneq E^H(u) \supset E^H$. By Theorem 2.3.4 we have $E^H(u, v) = E^H(w)$ for some $w \in E$, which contradicts the maximality of $[E^H(u) : E^H]$. All in all, E/E^H is nite and

$$[E : E^H] \leq |H| \underset{(2.9)}{\leq} |\mathrm{Gal}(E/E^H)| \underset{(2.8)}{=} [E : E^H].$$

Therefore equalities hold everywhere, and we conclude $\mathrm{Gal}(E/E^H) = H$. □

Remark 2.4.7. The upshot of the proof is $[E : E^H] \leq |H|$; a slick proof due to Artin is also prevalent, cf. [11, p.236, Lemma 2].

Theorem 2.4.8 (Galois correspondence for nite extensions)**.** *Let E/F be a nite Galois extension.*

(i) There are mutually inverse bijections

$$\begin{aligned} \{\textit{intermediate elds}\} &\overset{1:1}{\longleftrightarrow} \{\textit{subgroups of } \mathrm{Gal}(E/F)\} \\ [E \supset K \supset F] &\longmapsto \mathrm{Gal}(E/K) \\ E^H &\longmapsto [H \subset \mathrm{Gal}(E/F)], \end{aligned}$$

which are order-reversing in the sense of (2.7).

(ii) *For any intermediate field K and $\sigma \in \mathrm{Gal}(E/F)$, we have*

$$\mathrm{Gal}(E/\sigma(K)) = \sigma\mathrm{Gal}(E/K)\sigma^{-1};$$

the extension K/F is Galois if and only if $\mathrm{Gal}(E/K) \lhd \mathrm{Gal}(E/F)$ ("$\lhd$" = be normal subgroup of...)

(iii) *Furthermore, we have a bijection*

$$\begin{aligned} \mathrm{Gal}(E/F)/\mathrm{Gal}(E/K) &\xrightarrow{\sim} \mathrm{Hom}_F(K, E) \\ \sigma \cdot \mathrm{Gal}(E/K) &\mapsto \sigma|_K \end{aligned}$$

between pointed sets. It induces a group isomorphism $\mathrm{Gal}(E/F)/\mathrm{Gal}(E/K) \xrightarrow{\sim} \mathrm{Gal}(K/F)$ when K/F is Galois.

Proof. Thanks to Lemma 2.4.5 and 2.4.6, the maps in (i) above are mutually inverse.

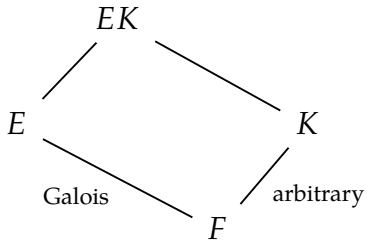
Let K be an intermediate field between E and F. The assertion $\mathrm{Gal}(E/\sigma(K)) = \sigma\mathrm{Gal}(E/K)\sigma^{-1}$ is a special case of (2.6). Also note that K/F is separable, and

$$\begin{aligned} [K/F \text{ is normal}] &\iff [\forall \sigma \in \mathrm{Gal}(E/F) = \mathrm{Hom}_F(E, \bar{F}),\ \sigma(K) = K] \\ &\iff \left[\begin{array}{l} \forall \sigma \in \mathrm{Gal}(E/F), \\ \mathrm{Gal}(E/\sigma(K)) = \sigma\mathrm{Gal}(E/K)\sigma^{-1} = \mathrm{Gal}(E/K) \end{array} \right], \end{aligned}$$

in which the last equivalence follows from the aforementioned Galois correspondence, whence (ii).

As regards (iii), consider the map $\mathrm{Gal}(E/F) \ni \sigma \mapsto \sigma|_K$. It surjects onto $\mathrm{Hom}_F(K, E)$ since every F-embedding $K \to E$ extends to $E \to E$ by the normality of E/F. One readily checks that $\sigma|_K = \tau|_K$ if and only if $(\tau^{-1}\sigma)|_K = \mathrm{id}$, which is equivalent to $\sigma\mathrm{Gal}(E/K) = \tau\mathrm{Gal}(E/K)$. For normal extensions K/F, we obtain a group isomorphism onto $\mathrm{Hom}_F(K, E) = \mathrm{Gal}(K/F)$. □

Proposition 2.4.9. *Consider the diagram of field extensions*



inside some ambient field, say $\bar{F}$. Then EK/K is Galois as well, and the restriction map $\sigma \mapsto \sigma|_E$ defines a group isomorphism $\mathrm{Gal}(EK/K) \xrightarrow{\sim} \mathrm{Gal}(E/E \cap K) \subset \mathrm{Gal}(E/F)$.

Proof. Since E is generated by separable elements over F, so is EK over K (see the remarks after Definition-Proposition 2.1.7). Similarly, E is the splitting field a family of polynomials $(P_i \in F[X])_{i\in I}$, hence so is EK for the family $(P_i \in K[X])_{i\in I}$. This entails that EK/K is a Galois extension. The restriction-to-E map $\mathrm{Gal}(EK/K) \to \mathrm{Gal}(E/E \cap K)$

is a well-de ned group homomorphism. Observe that if $\sigma \in \mathrm{Gal}(EK/K)$ satis es $\sigma|_E = \mathrm{id}_E$, then $\sigma(\gamma) = \gamma$ for every $\gamma \in EK$ since γ must be of the form

$$\gamma = \frac{x_1 y_1 + \cdots + x_n y_n}{x_1' y_1' + \cdots x_n' y_n'}, \quad x_i, x_i' \in E,\ y_i, y_i' \in K.$$

The injectivity follows at once.

Let us show the surjectivity. We assume $[E : F]$ nite in what follows. The idea is to show that the xed eld of $H := \mathrm{im}\,[\mathrm{Gal}(EK/K) \to \mathrm{Gal}(E/F)]$ is precisely $E \cap K$; it will then follow that $H = \mathrm{Gal}(E/E \cap K)$ by Theorem 2.4.8. Let $u \in E^H$, then u regarded as an element of EK is xed by $\mathrm{Gal}(EK/K)$, hence $u \in K$ by Lemma 2.4.5. The reverse inclusion $E^H \supset E \cap K$ has already been observed. This completes the proof for nite E/F. □

Note that the niteness intervenes only in the application of Theorem 2.4.8. For general Galois extensions E/F, one appeals to the easy observation that H is a closed in the Hausdor space $\mathrm{Gal}(E/F)$ under the *Krull topology*, since it is the continuous image of the compact group $\mathrm{Gal}(EK/K)$. The Galois correspondence continues to hold under this set-up. These stu s will be introduced in our discussion on in nite Galois theory.

Exercise 2.4.10 (Cf. [16, VI. Theorem 1.14])**.** Let E, E' be Galois extensions of F inside some ambient eld. Then EE'/F is Galois and the map

$$\begin{aligned} \mathrm{Gal}(EE'/F) &\longrightarrow \mathrm{Gal}(E/F) \times \mathrm{Gal}(E'/F) \\ \sigma &\longmapsto (\sigma|_E, \sigma|_{E'}) \end{aligned}$$

de nes an injective homomorphism between groups. Moreover, it is an isomorphism if $E \cap E' = F$. Hint: for the surjectivity, show that $\mathrm{Gal}(E/F) \times \{1\}$ and $\{1\} \times \mathrm{Gal}(E'/F)$ are both contained in the image by invoking Proposition 2.4.9.

Example 2.4.11. Let $\omega \in \mathbb{C}$, $\omega^3 = 1$ and $\omega \neq 1$. Consider the eld extension $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$. It is surely separable since we are in characteristic zero, normal since it is the splitting eld of the irreducible polynomial $X^3 - 2 \in \mathbb{Q}[X]$. Note that the sub eld $\mathbb{Q}(\omega)$ is also Galois over $\mathbb{Q}$: it is the splitting eld of $X^2 + X + 1$. Hence we have a tower of eld extensions

$$\begin{array}{c} \mathbb{Q}(\sqrt[3]{2}, \omega) \\ \Big| \text{ Galois} \\ \mathbb{Q}(\omega) \\ \Big| \text{ Galois, degree 2} \\ \mathbb{Q} \end{array}$$

We begin by determining $G := \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$. Tower property gives

$$[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q})] = [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2}))][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2}))].$$

The degree $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2}))]$ equals either 2 or 1; if it equals 1, then $\omega \in \mathbb{Q}(\sqrt[3]{2})$, which is impossible since $[\mathbb{Q}(\sqrt[3]{2} : \mathbb{Q}] = 3$ whereas $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$. We conclude that $|G| = [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = 6$.

Any $\sigma \in G$ must send ω to $\omega^{\pm 1}$, and send $\sqrt[3]{2}$ to $\omega^k\sqrt[3]{2}$ for some $k = 0, 1, 2$. There are jointly $2 \cdot 3$ possibilities of σ, which exhaust G since $|G| = 6$. It follows that G is generated by the normal subgroup $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}(\omega)) \simeq \mathbb{Z}/3\mathbb{Z}$ given by

$$\omega \mapsto \omega, \quad \sqrt[3]{2} \mapsto \omega^k\sqrt[3]{2}, \quad k = 0, 1, 2$$

together with the subgroup $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \mathbb{Q}(\sqrt[3]{2})) \simeq \mathbb{Z}/2\mathbb{Z}$

$$\omega \mapsto \omega^{\pm 1}, \quad \sqrt[3]{2} \mapsto \sqrt[3]{2}.$$

By taking semi-direct products, it is easy to check G must be isomorphic to the dihedral group D_6, or equivalently with the permutation group $\mathfrak{S}_3$. By the Galois correspondence, the intermediate fields are:

$$\mathbb{Q}(\sqrt[3]{2}, \omega), \mathbb{Q},$$
$$\mathbb{Q}(\omega) : \text{the only Galois subextension over } \mathbb{Q},$$
$$\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\omega\sqrt[3]{2}), \mathbb{Q}(\omega\sqrt[3]{2}) : \text{conjugate under the subgroup } \sqrt[3]{2} \mapsto \omega^k\sqrt[3]{2}.$$

LECTURE 3

SUPPLEMENTS ON GALOIS THEORY

Notation: for a subset E of some group, $\langle E \rangle$ will stand for the subgroup generated by E. When $E = \{x, y, \ldots\}$ we abbreviate $\langle E \rangle$ as $\langle x, y, \ldots \rangle$.

3.1 In nite Galois extensions

Let E/F be a Galois extension. So far we have seen that

- ⋆ $K/F \mapsto \mathrm{Gal}(E/K)$ satis es $E^{\mathrm{Gal}(E/K)} = K$, thus is an injection from intermediate elds to the subgroups of $\mathrm{Gal}(E/F)$;
- ⋆ it is a surjection when E/F is nite;
- ⋆ $\mathrm{Gal}(E/K)$ is normal if and only if K/F is Galois (the same arguments as in the nite case).

It is highly desirable to develop a full- edged theory as in the nite case. For example, it is of utmost importance to understand the *absolute Galois group* $\Gamma_F := \mathrm{Gal}(F^{\mathrm{sep}}/F)$ together with its subgroups of the form $\mathrm{Gal}(F^{\mathrm{sep}}/K)$. As a special case, the algebraic number theory is largely the study of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, whose structure remains a mystery so far.

The key insight here is that every element u in E lies in some nite Galois subextension K/F. Therefore, the action of $\mathrm{Gal}(E/F)$ on u can be reduced to that of $\mathrm{Gal}(K/F)$ for various K. A convenient formulation of this idea is to introduce a topology on $\mathrm{Gal}(L/F)$ as follows.

De nition 3.1.1 (Krull topology)**.** Equip $\mathrm{Gal}(E/F)$ with the topology such that the normal subgroups

$$\mathrm{Gal}(E/K), \quad K/F : \text{ nite Galois subextension}$$

form a local base at $1 \in \mathrm{Gal}(E/F)$, and that $\mathrm{Gal}(E/F)$ be comes a topological group.

Being a topological group means that the operations of multiplication and taking inverse are both continuous. Thus we obtain the local bases $(g\mathrm{Gal}(E/K))_{K/F}$ at each $g \in \mathrm{Gal}(E/F)$. The Krull topology may be understood as:

σ and τ in $\mathrm{Gal}(E/F)$ are "close to each other", if
$\sigma\|_K = \tau\|_K$ for "large" nite Galois subextension K/F.

The restriction maps $\sigma \mapsto \sigma|_K$ induces a group homomorphism

$$\mathrm{Gal}(E/F) \longrightarrow \prod_{\substack{E \supset K \supset F \\ [K:F]<\infty}} \mathrm{Gal}(K/F).$$

It is injective by our earlier key insight (sic). Moreover, if we equip the right-hand side with the product topology, where each $\mathrm{Gal}(K/F)$ is endowed with its discrete topology, then the induced topology on $\mathrm{Gal}(E/F)$ is nothing but the Krull topology — check this! When E/F is nite, this yields the discrete topology on $\mathrm{Gal}(E/F)$.

Lemma 3.1.2. *The embedding above realizes* $\mathrm{Gal}(E/F)$ *as a closed subgroup of* $\prod_{\substack{E \supset K \supset F \\ [K:F]<\infty}} \mathrm{Gal}(K/F)$.

Proof. The image of $\mathrm{Gal}(E/F)$ is characterized as

$$\left\{\sigma = (\sigma_K \in \mathrm{Gal}(K/F))_K : K_1 \supset K \implies \sigma_{K_1}|_K = \sigma_K\right\}.$$

Therefore it is de ned by a family of equations of the form $f(\sigma) = g(\sigma)$, where f, g are continuous maps emanating from $\prod_K \mathrm{Gal}(K/F)$. Since $\prod_K \mathrm{Gal}(K/F)$ is Hausdor , the image of $\mathrm{Gal}(E/F)$ must be closed. □

Remark 3.1.3. In high-tech terms, this means that $\mathrm{Gal}(E/F)$ can be identi ed with the *projective limit* $\varprojlim_K \mathrm{Gal}(K/F)$.

Lemma 3.1.4. *For any nite subextension* K/F *with* $K \subset E$, *the subgroup* $\mathrm{Gal}(E/K)$ *is open.*

Proof. Firstly we notice that for every $\alpha \in E$, the stabilizer $\mathrm{Stab}(\alpha) := \{\sigma \in \mathrm{Gal}(E/F) : \sigma(\alpha) = \alpha\}$ is open. Indeed, α lies in some nite Galois extension K'/F with $K' \subset E$, therefore $\mathrm{Stab}(\alpha) \supset \mathrm{Gal}(E/K')$. Writing $\mathrm{Stab}(\sigma)$ as a union of cosets of $\mathrm{Gal}(E/K')$, each of whom is open, we deduce the openness of $\mathrm{Stab}(\alpha)$.

Next, write $K = F(\alpha_1, \ldots, \alpha_n)$. We have $\mathrm{Gal}(E/K) = \bigcap_{i=1}^n \mathrm{Stab}(\alpha_i)$, whence the openness of $\mathrm{Gal}(E/K)$. □

Lemma 3.1.5. *The topological group* $G := \mathrm{Gal}(E/F)$ *satis es the following properties.*

(i) G *is compact and Hausdor .*
(ii) Every open subgroup is closed of nite index.
(iii) G *is totally disconnected.*
(iv) For any intermediate eld K, *the subgroup* $\mathrm{Gal}(E/K)$ *is closed; it is open if and only if* K/F *is nite.*

Proof. Embed G into $\prod_{\substack{E \supset K \supset F \\ [K:F]<\infty}} \mathrm{Gal}(K/F)$. The right-hand side is compact and Hausdor since each $\mathrm{Gal}(K/F)$ is (Tychono 's theorem), this proves (i).

To prove (ii), let H be an open subgroup of G. Decompose $G \smallsetminus H$ into $\bigcup_{g \notin H} gH$. Since each gH is a translate of H, thus open, we see that $G \smallsetminus H$ is open as well. Furthermore, these open cosets cover the closed subset $G \smallsetminus H$, which is compact since G is, hence we may extract a nite subcover. The niteness follows immediately.

The assertion (iii) follows since G has a local base at 1 consisting of open and closed subsets — please consult your local topologist.

As to (iv), note that $\mathrm{Gal}(E/K) = \bigcap_{K'} \mathrm{Gal}(E/K')$ where K'/F ranges over the finite subextensions of K, thus $\mathrm{Gal}(E/K)$ is closed by (ii) and Lemma 3.1.4. When K/F is finite, $\mathrm{Gal}(E/K)$ is open by definition. Conversely, openness of $\mathrm{Gal}(E/K)$ implies the finiteness of $\mathrm{Gal}(E/F)/\mathrm{Gal}(E/K)$ by (ii); the latter is known to be in bijection with $\mathrm{Hom}_F(K, E)$. It remains to remark that $\mathrm{Hom}_F(K, E)$ is finite if and only if K/F is finite. □

Theorem 3.1.6 (The Galois correspondence)**.** *For any Galois extension L/F, the assignments*

$$\begin{aligned} \{\textit{intermediate fields}\} &\overset{1:1}{\longleftrightarrow} \{\textit{closed subgroups of } \mathrm{Gal}(E/F)\} \\ [E \supset K \supset F] &\longmapsto \mathrm{Gal}(E/K) \\ E^H &\longmapsfrom H \end{aligned}$$

are mutually inverse, order-reversing bijections. The open subgroups correspond to finite extensions.

Proof. In view of the preceding discussions, the bulk of the proof is to show that, for every closed subgroup $H \subset \mathrm{Gal}(E/F)$ we have

$$H = \mathrm{Gal}(E/E^H).$$

The inclusion $H \subset \mathrm{Gal}(E/E^H)$ is evident. Conversely, let $\sigma \in \mathrm{Gal}(E/E^H)$. For any finite Galois subextension K/F, we may restrict everything to K and obtain the images $\bar{H} \subset \mathrm{Gal}(K/F)$ and $\bar{\sigma} \in \mathrm{Gal}(K/K^{\bar{H}})$. The Galois correspondence for K/F implies $\bar{\sigma} \in \bar{H}$, or: σ is "close to" some element in H. Varying K/F, we conclude that $\sigma \in H$ since H is closed. □

3.2 Linear independence of characters

Let $(G, \cdot)$ be a *monoid*, that is, a set with an associative multiplication law $\bullet$ that has a unit 1, but not necessarily with inverses. Let E be a field. By a *character* of G with values in E, we mean a map $\chi : G \to E$ with

- ⋆ $\chi(gh) = \chi(g)\chi(h)$ for all $g, h \in G$,
- ⋆ $\chi(1) = 1$.

Theorem 3.2.1 (E. Artin)**.** *Let G be a monoid and E be a field. Let $(\chi_i)_{i\in I}$ be a family of distinct characters of G with values in E. Then $(\chi_i)_{i\in I}$ is linearly independent in the following sense: if*

$$\sum_{i\in I} a_i \chi_i(\cdot) = 0, \quad (\textit{finite sum}), \quad a_i \in E,$$

then $a_i = 0$ for each $i \in I$.

Proof. Suppose that $\sum_{i\in I} a_i\chi_i(\cdot) = 0$ as above. Let $J := \{i \in I : a_i \neq 0\}$. Assume $|J| \geq 2$. Let j, j' be distinct elements of J and choose $g \in G$ such that $\chi_j(g) \neq \chi_{j'}(g)$. Then

$$\sum_{i\in J} a_i\chi_i(g)\chi_i(\cdot) = \sum_{i\in J} a_i\chi_i(g\,\cdot) = 0,$$
$$\sum_{i\in J} a_i\chi_j(g)\chi_i(\cdot) = \chi_j(g)\sum_{i\in J} a_i\chi_i(\cdot) = 0.$$

Subtraction gives a new linear relation between χ_i with fewer nonzero coe cients, whereas the coe cient of $\chi_{j'}$ is $a_{j'}(\chi_{j'}(g) - \chi_j(g)) \neq 0$. This procedure eventually leads us to the case $|J| = 1$, which is clearly impossible. □

This result will be applied to the case $G = (E, \cdot)$, in which case the set $\mathrm{Aut}(E)$ furnishes characters.

N.B. Do not confuse with the linear independence of the characters of group representations, which we will encounter later in this course.

3.3 Norm and trace

Let E/F be any nite extension.

De nition 3.3.1. For any $\alpha \in E$, let $m_\alpha : E \to E$ be the F-linear map de ned by $m_\alpha(x) = x\alpha$. Set

$$\mathrm{N}_{E/F}(\alpha) := \det(m_\alpha)$$
$$\mathrm{Tr}_{E/F}(\alpha) := \mathrm{Tr}(m_\alpha),$$

called the *norm* and *trace* of α, respectively. They take values in F.

We begin with some easy observations:

- ⋆ $\mathrm{N}_{E/F}(\alpha\beta) = \mathrm{N}_{E/F}(\alpha)\mathrm{N}_{E/F}(\beta)$ (multiplicativity);
- ⋆ $\mathrm{Tr}_{E/F}(\alpha + \beta) = \mathrm{Tr}_{E/F}(\alpha) + \mathrm{Tr}_{E/F}(\beta)$ (additivity);
- ⋆ $\alpha \in F$ implies $\mathrm{N}_{E/F}(\alpha) = \alpha^{[E:F]}$ and $\mathrm{Tr}_{E/F}(\alpha) = [E : F]\mathrm{Tr}_{E/F}(\alpha)$;

Lemma 3.3.2 (Transitivity)**.** *Let L/E and E/F be nite extensions, then*

$$\mathrm{N}_{E/F} \circ \mathrm{N}_{L/E} = \mathrm{N}_{L/F}, \quad \mathrm{Tr}_{E/F} \circ \mathrm{Tr}_{L/E} = \mathrm{Tr}_{L/F}.$$

Proof. We shall prove a more general statement: let V be a nite-dimensional E-vector space and $T : V \to V$ be an E-linear endomorphism, then T is F-linear as well. Write $\det_E(T)$, $\mathrm{Tr}_E(T)$ to denote its determinant and trace as an E-linear map. Idem for $\det_F(T)$, $\mathrm{Tr}_F(T)$. We contend that

$$\mathrm{N}_F(T) = \mathrm{N}_{E/F}(\det_E(T)), \quad \mathrm{Tr}_F(T) = \mathrm{Tr}_{E/F}(\mathrm{Tr}_E(T)).$$

Let $n = \dim_E V$. Fix a basis of V over E and identify T with a $n \times n$ matrix over E. The assertions are trivially true when $n = 0, 1$. Firstly, consider the case for $\det_F$ for general n. By the elementary row and column permutations, we may express T as a product of matrices (over E) of the form

(i) upper or lower triangular matrices with diagonal elements = 1;
(ii) diagonal matrices;
(iii) row (resp. column) transposition matrices: that is, the matrix obtained from I_n by exchanging the i-th and j-th rows (resp. columns), for some $1 \le i, j \le n$.

In each case the equality $\mathrm{N}_{E/F} \det_E = \det_F$ holds. Indeed, for (i), both sides equal 1; the case (ii) reduces to the case $n = 1$, whereas both sides of (iii) equal $(-1)^{[E:F]}$ — this requires some veri cation. Therefore $\mathrm{N}_{E/F} \det_E(T) = \det_F(T)$ since both sides are multiplicative in T.

Now consider the case for Tr_F. Since Tr_F and $\mathrm{Tr}_{E/F}\mathrm{Tr}_E$ are both additive, we readily reduce to the case where T has only one nonzero entry. If the entry lies o the diagonal, both $\mathrm{Tr}_F(T)$ and $\mathrm{Tr}_E(T)$ vanish; otherwise we reduce to the case $n = 1$. □

Proposition 3.3.3. *Consider a nite extension of the form $F(\alpha)/F$. Write the minimal polynomial of α as $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$, then*

$$\mathrm{N}_{F(\alpha)/F}(\alpha) = (-1)^n a_0, \quad \mathrm{Tr}_{F(\alpha)/F}(\alpha) = -a_{n-1}.$$

Proof. This is essentially linear algebra, namely the theory of *rational canonical forms*. Since $\alpha \cdot \alpha^{n-1} = -\sum_{k=0}^{n-1} a_k \alpha^k$, the endomorphism m_α is represented by the matrix

$$\begin{pmatrix} 0 & \cdots & 0 & -a_0 \\ 1 & & & -a_1 \\ & \ddots & & \\ & & 1 & -a_{n-1} \end{pmatrix}$$

under the F-basis $1, \alpha, \cdots \alpha^{n-1}$ for $F(\alpha)$. Its determinant and trace are readily calculated. □

Remark 3.3.4. Note that $(-1)^n a_0$ and $-a_1$ are the product and sum of roots of P, respectively; here the roots are counted with multiplicities.

Proposition 3.3.5. *Let E/F be a nite extension. For any $\alpha \in E$ we have*

$$\mathrm{N}_{E/F}(\alpha) = \prod_{\sigma \in \mathrm{Hom}_F(E, \bar{F})} \sigma(\alpha)^{[E:F]_i},$$
$$\mathrm{Tr}_{E/F}(\alpha) = [E : F]_i \sum_{\sigma \in \mathrm{Hom}_F(E, \bar{F})} \sigma(\alpha)$$

for any choice of algebraic closure $\bar{F}$. Here $[E : F]_i$ stands for the inseparable degree.

Proof. Consider the case of $\mathrm{N}_{E/F}$ rst. Let $P \in F[X]$ be the minimal polynomial of α. By Lemma 3.3.2 and Remark 3.3.4, we have

$$\begin{aligned} \mathrm{N}_{E/F}(\alpha) &= \mathrm{N}_{F(\alpha)/F}\mathrm{N}_{E/F(\alpha)}(\alpha) = N_{F(\alpha)/F}(\alpha)^{[E:F(\alpha)]} \\ &= \prod_{\substack{\nu \in \bar{F},\ P(\nu)=0 \\ \text{with multiplicities}}} \nu^{[E:F(\alpha)]} \end{aligned}$$

Recall that the roots of P are in bijection with $\mathrm{Hom}_F(F(\alpha), \bar{F})$: to each embedding σ we associate $\nu := \sigma(\alpha)$. Also, in our derivation of the identity $P(X) = P^\flat(X^{p^m})$ with $(P^\flat)' \neq 0$ in the previous Lecture (say in the case of characteristic $p > 0$, otherwise we always have multiplicity one), we have seen that each root $\nu = \sigma(\alpha)$ of P has multiplicity with $p^m = [F(\alpha) : F]_i$. Therefore the last term above equals

$$\prod_{\sigma \in \mathrm{Hom}_F(F(\alpha), \bar{F})} \sigma(\alpha)^{[F(\alpha):F]_i [E:F(\alpha)]}. \tag{3.1}$$

Consider the restriction map $\mathrm{Hom}_F(E, \bar{F}) \to \mathrm{Hom}_F(F(\alpha), \bar{F})$. By the much-used property that every F-embedding $F(\alpha) \to \bar{F}$ extends to $E \to \bar{F}$, the map is surjective. Moreover, the ber over each $\sigma : F(\alpha) \to \bar{F}$ has cardinality $[E : F(\alpha)]_s$: indeed, this is exactly how the separable degree was de ned! Writing

$$[E : F(\alpha)] = [E : F(\alpha)]_s [E : F(\alpha)]_i$$

and using the tower property of inseparable degrees, we infer that (3.1) equals

$$\prod_{\sigma \in \mathrm{Hom}_F(F(\alpha), \bar{F})} \sigma(\alpha)^{[E:F(\alpha)]_s [E:F(\alpha)]_i [F(\alpha):F]_i} = \prod_{\sigma \in \mathrm{Hom}_F(E, \bar{F})} \sigma(\alpha)^{[E:F]_i}.$$

The case for $\mathrm{Tr}_{E/F}$ is the same: just switch to the additive version of the arguments above. □

Exercise 3.3.6. Assume $\mathrm{char}(F) \neq 2$ and E/F is nite separable. Show that the map

$$\begin{aligned} E \times E &\longrightarrow F \\ (x, y) &\longmapsto \mathrm{Tr}_{E/F}(xy) \end{aligned}$$

is a non-degenerate F-quadratic form. It is called the *trace form* of the nite extension E/F. Hint: apply Proposition 3.3.5 and Theorem 3.2.1.

Exercise 3.3.7. Show that $\mathrm{Tr}_{E/F}$ can be identically zero without the hypothesis of separability.

3.4 Finite elds

Every nite eld must have positive characteristic, otherwise it would contain a copy of $\mathbb{Q}$. Let us x a prime number p in what follows.

Theorem 3.4.1. *Every nite eld F of characteristic p has cardinality $q = p^m$ for some $m \geq 1$. Moreover, there exists a nite eld with q elements for every p-power q, which is unique up to isomorphism.*

Nowadays it is standard to write $\mathbb{F}_q$ for a nite eld with q elements. Unless otherwise speci ed, all the embeddings and isomorphisms below are over the prime eld $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

Proof. Given $q = p^m$, $m \in \mathbb{Z}_{\geq 1}$, let $F/\mathbb{F}_p$ be the splitting field of $X^q - X \in \mathbb{F}_p[X]$. By the identity $(u+v)^q = u^q + v^q$ in characteristic p, the roots $\{x \in F : x^q = x\}$ form a subfield; it must equal F itself. On the other hand, $(X^q - X)' = -1 \neq 0$, thus it has q distinct roots in F. We infer that $|F| = q$.

Conversely, given a finite field F with characteristic p, we must have $|F| = q := p^m$ where $m := [F : \mathbb{F}_p]$. We claim that F is a splitting field of the polynomial $X^q - X \in \mathbb{F}_p[X]$; the uniqueness of F will follow directly. Indeed, since $|F^\times| = q - 1$, every $x \in F$ satisfies $x^q = x$. As $X^q - X$ has exactly q roots in its splitting field, F is a splitting field of $X^q - X$ by counting. Note that our arguments imply that $F/\mathbb{F}_p$ is normal and separable, hence Galois. □

Theorem 3.4.2. *Let E/F be an extension of finite fields with characteristic p. Set $q := |F|$, then E/F is a Galois extension and $\mathrm{Gal}(E/F)$ is the cyclic group generated by $x \mapsto x^q$.*

The automorphism $x \mapsto x^q$ is called the *Frobenius automorphism*.

Proof. It has been remarked that $E/\mathbb{F}_p$ is Galois, hence so is E/F. Let $n := [E : F]$. Set $\sigma := [x \mapsto x^q]$; one readily checks that $\sigma \in \mathrm{Gal}(E/F)$. Claim: σ is of order n in $\mathrm{Gal}(E/F)$. If $\sigma^d = \mathrm{id}_E$ for some $d \mid n$, then all elements in E are roots of $X^{q^d} - X$. As observed above, $X^{q^d} - X$ has q^d distinct roots, therefore $d = n$ since $|E| = q^n$. Since E/F is Galois of degree n, we must have $\mathrm{Gal}(E/F) = \langle \sigma \rangle$ by a counting argument. □

Corollary 3.4.3. *Let F be a finite field. All algebraic extensions of F are separable.*

Fields with this property are called *perfect fields*.

Corollary 3.4.4. *Let E/F be an extension of finite fields. Let $q := |F|$, $q^n := |E|$. For every $d|n$ there exists a unique intermediate field K with $[K : F] = d$, and every intermediate field is so obtained.*

Proof. Apply the Galois correspondence to $\mathrm{Gal}(E/F) \simeq \mathbb{Z}/n\mathbb{Z}$. □

Remark 3.4.5. Pick an algebraic closure $\bar{\mathbb{F}}_q$ of $\mathbb{F}_q$. The precedent results show that the finite subextensions of $\bar{\mathbb{F}}_q/\mathbb{F}_q$ are of the form $\mathbb{F}_{q^n}/\mathbb{F}_q$ with

- ⋆ $\mathbb{F}_{q^m} \subset \mathbb{F}_{q^n}$ if and only if $m|n$,
- ⋆ $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \mathbb{Z}/n\mathbb{Z}$.

By Lemma 3.1.2, the absolute Galois group of $\mathbb{F}_q$ can thus be realized as the additive group

$$\left\{ (\sigma_n \in \mathbb{Z}/n\mathbb{Z})_{n\geq 1} \in \prod_{n \in \mathbb{Z}_{\geq 1}} \mathbb{Z}/n\mathbb{Z} : \ m|n \implies \sigma_n \xmapsto{\text{mod } n\mathbb{Z}/m\mathbb{Z}} \sigma_m \right\}$$

under pointwise addition. In fact, it can be made into a huge ring using the ring structures on each $\mathbb{Z}/n\mathbb{Z}$, known as the *Prüfer ring* $\hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}$. It is canonically isomorphic to $\prod_{\ell:\text{prime}} \mathbb{Z}_\ell$, where $\mathbb{Z}_\ell$ stands for the ring of ℓ-adic integers.

The Frobenius automorphism $x \mapsto x^q$ may be identified with the family $(1 + n\mathbb{Z})_n \in \hat{\mathbb{Z}}$. The Frobenius automorphism generates a copy of $\mathbb{Z}$ inside $\hat{\mathbb{Z}}$, which turns out to be a dense subgroup; it cannot correspond to any intermediate field under Theorem 3.1.6.

3.5 Abstract Kummer theory

We will follow [19, IV.3] closely. In what follows, we x a separable closure F^{sep}/F and the elds under consideration are all assumed to sit inside F^{sep}.

De nition 3.5.1. Let E/F be a Galois extension. We say that E/F is

- ⋆ *abelian*, if $\mathrm{Gal}(E/F)$ is an abelian group;
- ⋆ *cyclic*, if $\mathrm{Gal}(E/F)$ is a cyclic group.

An abelian extension E/F is called of *exponent* n if $\mathrm{Gal}(E/F)$ is a group of exponent n, i.e. $\sigma^n = 1$ for every $\sigma \in \mathrm{Gal}(E/F)$. Subextensions of cyclic (resp. abelian of exponent n) extensions are still cyclic (resp. abelian of exponent n).

Exercise 3.5.2. Show that compositum of a family abelian extensions of F is again abelian; it is of exponent n if every E_i/F is. Deduce the notion of the maximal abelian extension inside F^{sep}/F. Do the same for abelian extensions of a given exponent n. Hint: the Galois group of the compositum embeds into $\prod_i \mathrm{Gal}(E_i/F)$.

We present a somehow axiomatic framework for Kummer theory as follows. Let $(A, \cdot)$ be a abelian group on which the absolute Galois group $\Gamma_F := \mathrm{Gal}(F^{\mathrm{sep}}/F)$ acts; it is reasonable to set $\Gamma_E := \mathrm{Gal}(F^{\mathrm{sep}}/E)$ for any E/F, since F^{sep} is also a separable closure of E.

Denote this action as $\Gamma_F \times A \ni (\sigma, a) \mapsto \sigma(a)$. More precisely, we require that

- ⋆ $(\sigma\tau)(a) = \sigma(\tau(a))$,
- ⋆ $\sigma(ab) = \sigma(a)\sigma(b)$,
- ⋆ $1(a) = a$, for all $\sigma, \tau \in \Gamma_F$ and $a, b \in A$;
- ⋆ $A = \bigcup_{\substack{E/F \\ [E:F]<\infty}} A_E$ where $A_E := A^{\Gamma_E}$ is the xed subgroup.

The last assertion amounts to saying that every element of A has an open stabilizer under Γ_F; therefore Γ_F acts continuously on A if A is endowed with discrete topology. It will justify the use of in nite Galois correspondence in what follows.

Note that when E/F is Galois, the action of Γ_F on A_E factors through $\mathrm{Gal}(E/F) = \Gamma_F/\Gamma_E$. One may check that $A_L^{\mathrm{Gal}(L/E)} = A_E$. For every $L \supset E$ with $[L : F] < \infty$, we have the "norm" map (do not confuse with the earlier notion!)

$$\begin{aligned} \mathcal{N}_{L/E} : A_L &\longrightarrow A_E \\ a &\longmapsto \prod_{\sigma \in \Gamma_E/\Gamma_L} \sigma(a). \end{aligned}$$

We adopt the convention

$$(\sigma + \sigma')a := \sigma(a)\sigma'(a), \quad \text{etc.} \tag{3.2}$$

whose usefulness is illustrated in the following arguments.

De nition 3.5.3 (Tate cohomology at degree -1)**.** Given a nite Galois extension E/F, de ne the group

$$\hat{H}^{-1}(E/F, A_E) := \ker\left(\mathcal{N}_{E/F}\right) \Big/ \langle (\sigma - 1)(a) : a \in A_E,\ \sigma \in \mathrm{Gal}(E/F) \rangle.$$

N.B. This awkward notation originates from the theory of *Galois cohomology*.

Lemma 3.5.4. *When E/F is cyclic, $\langle(\sigma-1)(a) : a \in A_E,\ \sigma \in \mathrm{Gal}(E/F)\rangle$ equals $(\tau-1)A_E$ where τ is any generator of* $\mathrm{Gal}(E/F)$.

Proof. For $\sigma = \tau^k \in \mathrm{Gal}(E/F)$, apply the identity $(\tau^k-1)a = (\tau-1)(1+\cdots+\tau^{k-1})a$. □

De nition 3.5.5. Let $\wp : A \to A$ be a homomorphism satisfying
(i) $\wp$ is surjective,
(ii) $\wp(\sigma(a)) = \sigma(\wp(a))$ for all $\sigma \in \Gamma_F$ and $a \in A$,
(iii) $\mu_\wp := \ker(\wp) \simeq \mathbb{Z}/n\mathbb{Z}$ for some positive integer n, and $\mu_\wp \subset A_F$.

For every subset $S \subset A$, we want to talk about the subextension $F(S)$ "generated" by S. This can be done via Galois correspondence: $F(S)$ is de ned as the xed eld of the closed subgroup $\{\sigma \in \Gamma_F : \forall s \in S,\ \sigma(s) = s\}$ of Γ_F. Therefore $S \mapsto F(S)$ de nes an order-preserving map from subsets of A to intermediate elds. Also note that $F(A_E) \subset E$ for all E/F.

The core of Kummer theory is the assignment $a \mapsto \chi_a$ from A_F to $\mathrm{Hom}_{\mathrm{cont}}(\Gamma_F, \mu_\wp)$, the latter being de ned as

$$\begin{aligned}\mathrm{Hom}_{\mathrm{cont}}(\Gamma_F, \mu_\wp) &:= \left\{\chi \in \mathrm{Hom}(\Gamma_F, \mu_\rho) : \text{factors through some nite } \mathrm{Gal}(E/F)\right\} \\ &= \{\text{continuous homomorphisms for the Krull topology}\}.\end{aligned}$$

It is an abelian group under pointwise multiplication $\chi\chi' : \sigma \mapsto \chi(\sigma)\chi'(\sigma)$. Now construct χ_a as follows: pick any $\alpha \in \wp^{-1}(a)$, we set

$$\chi_a(\sigma) := (\sigma-1)(\alpha), \quad \gamma \in \Gamma_F.$$

Since $\alpha \in A_E$ for some nite E/F, we see that χ_a factors through $\mathrm{Gal}(E'/F)$ where E'/F is the Galois closure of E. Next, $\wp((\sigma-1)(\alpha)) = (\sigma-1)(\wp(\alpha)) = 1$, thus χ_a has image inside $\mu_\wp$. It is also independent of the choice of α as $\mu_\wp \subset A_F$. The following properties are easily checked:
- ⋆ $\chi_{ab}(\sigma) = \chi_a(\sigma)\chi_b(\sigma)$;
- ⋆ $\chi_a(\sigma\sigma') = \chi_a(\sigma)\chi_a(\sigma')$: use the identity $\sigma\sigma' - 1 = \sigma(\sigma'-1) + (\sigma-1)$;
- ⋆ $a \in \wp(A_F) \iff \alpha \in A_F \iff \chi_a = 1$ (the trivial homomorphism).

Thus we deduce an injective group homomorphism $A_F/\wp(A_F) \to \mathrm{Hom}_{\mathrm{cont}}(\Gamma_F, \mu_\wp)$.

Theorem 3.5.6. *Given $(A, \wp)$ as above. Assume $\hat{H}^{-1}(E/F, A_E) = \{1\}$ for every nite cyclic E/F. Then the map*

$$\begin{aligned}\{\Delta : \wp(A_F) \subset \Delta \subset A_F\} &\longrightarrow \{E/F : \textit{abelian extensions of exponent } n\ \} \\ \Delta &\longmapsto F(\wp^{-1}(\Delta))\end{aligned}$$

is a bijection. Furthermore, if $\Delta \mapsto E$ under this map, then $\wp(A_E) \cap A_F = \Delta$ and the group homomorphism

$$\begin{aligned}\Delta/\wp(A_F) &\longrightarrow \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(E/F), \mu_\wp) \\ a \cdot \wp(A_F) &\longmapsto \chi_a.\end{aligned} \tag{3.3}$$

is an isomorphism.

Here the de nition of $\mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(E/F), \mu_\wp)$ is similar to $\mathrm{Hom}_{\mathrm{cont}}(\Gamma_F, \mu_\wp)$. Extensions of the form $F(\wp^{-1}(\Delta))/F$ are called *Kummer extensions* for the data $(A, \wp)$.

Sketch of the proof. Given Δ on the left-hand side, put $E := F(\wp^{-1}(\Delta))$, the map

$$\begin{aligned} \mathrm{Gal}(E/F) &\longrightarrow \mu_\wp^\Delta \\ \sigma &\longmapsto (\chi_a(\sigma))_{a\in\Delta} \end{aligned}$$

is a group homomorphism. If $\chi_a(\sigma) = 1$ for all $a \in \Delta$, then σ xes every element in $\wp^{-1}(\Delta)$, therefore $\sigma \in \mathrm{Gal}(E/F)$ must be trivial by the de nition of $E = F(\wp^{-1}(\Delta))$. Thus the homomorphism is injective and E/F is abelian of exponent n.

Conversely, given an abelian E/F with exponent n, we put $\Delta := \wp(A_E) \cap A_F \supset \wp(A_F)$ as prescribed in the assertions and contend that $E = F(\wp^{-1}(\Delta))$. Observe that $\wp^{-1}(\Delta) \subset A_E$ since $\mu_\wp \subset A_F$, from which we deduce

$$F(\wp^{-1}(\Delta)) \subset F(A_E) \subset E$$

by Galois correspondence. To show $E \supset F(\wp^{-1}(\Delta))$, note that E/F is a compositum of its nite subextensions. By the structure theory of nite abelian groups, we see that E/F is the compositum of nite cyclic subextensions. Thus it su ces to show $K \subset F(\wp^{-1}(\Delta))$ for every nite cyclic subextension K/F.

Observe that K/F is also of exponent n, thus $[K : F] \mid n$. Let ζ be a generator of $\mu_\wp$ and let $\eta := \zeta^{n/[K:F]}$. Observe that

$$[\eta \in A_F] \implies [N_{K/F}(\eta) = \eta^{[K:F]} = \zeta^n = 1] \implies [\exists \alpha \in A_K,\ \eta = (\tau - 1)(\alpha)]$$

where τ is a generator of $\mathrm{Gal}(K/F)$ (Lemma 3.5.4). For this α we have $K(\alpha) \subset K$, thus the Γ_F-action on $\langle a \rangle$ factors through $\mathrm{Gal}(K/F)$. Since $\tau^k(\alpha) = \eta^k \alpha$ for all $k \geq 0$, it follows that $\{\sigma \in \Gamma_F : \sigma(\alpha) = \alpha\} = \Gamma_K$, so $K = F(\alpha)$. Now

$$(\tau - 1)(\wp(\alpha)) = \wp\left((\tau - 1)(\alpha)\right) = \wp(\eta) = 1,$$

hence $\wp(\alpha) \in \wp(A_K) \cap A_F \subset \Delta$, so $K \subset F(\wp^{-1}(\Delta))$ as required.

Let $E = F(\wp^{-1}(\Delta))$ as above and consider (3.3). Its injectivity has been established, and it is routine to check that χ_a factors through $\mathrm{Gal}(E/F)$ whenever $a \in \Delta$. To show the surjectivity of (3.3), note that every $\chi \in \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(E/F), \mu_\wp)$ must factor through $\mathrm{Gal}(K/F)$ for some nite cyclic K/F. Fix such a K/F and pick a generator τ of $\mathrm{Gal}(K/F)$. As before, $\mu_\wp \in A_F$ implies

$$N_{K/F}(\chi(\tau)) = \chi(\tau)^{[K:F]} = \chi\left(\tau^{[K:F]}\right) = 1,$$

hence $\exists \alpha \in A_K$ with $\chi(\tau) = (\tau - 1)(\alpha)$. Put $a := \wp(\alpha)$, one veri es $(\tau - 1)(a) = \wp(\chi(\tau)) = 1$, hence $a \in \wp(A_E) \cap A_F = \Delta$. Summing up, we have shown $\chi(\tau) = \chi_a(\tau)$, which entails $\chi = \chi_a$. This establishes the surjectivity of (3.3).

By the injectivity of $a \cdot \wp(A_F) \mapsto \chi_a$, we conclude that Δ can be read o from $E = F(\wp^{-1}(\Delta))$ as $\{a \in A_F : \chi_a|_{\Gamma_E} = 1\}$. We have arrived at the bijectivity of $\Delta \mapsto F(\wp^{-1}(\Delta))$. □

We give two well-known examples of this framework.

Kummer theory Let $A := (F^{\mathrm{sep}})^\times$ (multiplicative group) on which Γ_F acts. Then $A_E = E^\times$ and the norm maps $\mathcal{N}_{L/E}$ are nothing but the usual norms for field extensions; cf. Proposition 3.3.5. Take

$$\wp : a \mapsto a^n, \quad n \in \mathbb{Z}_{\geq 1}.$$

We must assume that

- ⋆ F contains all the n-th roots of 1, so that $\mu_\wp \subset A_F$;
- ⋆ n is coprime to $p := \mathrm{char}(F)$ whenever $p > 0$, so that $\wp : A \to A$ is surjective.

Artin-Schreier theory Let $A := F^{\mathrm{sep}}$ (additive group) on which Γ_F acts. As before, $A_E = E$ and $\mathcal{N}_{L/E} = \mathrm{Tr}_{L/E}$. Assume $p = \mathrm{char}(F) > 0$ and take

$$\wp : a \mapsto a^p - a.$$

Note that $\mu_\wp$ is just the prime field $\mathbb{F}_p$ of F in this case. The surjectivity of $\wp$ results from the separability of $X^p - X$.

As what one expects, in either case, the field $F(S)$ generated by a subset $S \subset A$ (Definition 3.5.5) coincides with the compositum of $\{F(x) : x \in S \subset F^{\mathrm{sep}}\}$. The crucial cohomological inputs $\hat{H}^{-1}(E/F, A_E) = \{1\}$ for both cases are settled as follows. Keep the convention (3.2).

Theorem 3.5.7 (Hilbert's Theorem 90: version ×)**.** *Let E/F be a cyclic extension, then every element $a \in E^\times$ with $\mathrm{N}_{E/F}(a) = 1$ takes the form $(\tau - 1)\alpha$ for some $\alpha \in E^\times$, where τ is a generator of $\mathrm{Gal}(E/F)$.*

Proof. Put $n := [E : F]$. By the linear independence (Theorem 3.2.1) of the characters $1, \cdots, \tau^{n-1} \in \mathrm{Gal}(E/F)$, there exists $\gamma \in E^\times$ satisfying

$$\beta := \sum_{k=0}^{n-1} \left(\sum_{0 \leq h < k} \tau^h \right) (a) \cdot \tau^k(\gamma) \neq 0,$$

with the convention $\left(\sum_{0 \leq h < 0} \tau^h\right)(a) = 0(a) = 1$ in the zeroth term.

One verifies $(1 - \tau)(\beta) = a$ using $\mathrm{N}_{E/F}(a) = 1$. Take $\alpha := \beta^{-1}$. □

Theorem 3.5.8 (Hilbert's Theorem 90: version +)**.** *Let E/F be a cyclic extension, then every element $a \in E$ with $\mathrm{Tr}_{E/F}(a) = 0$ takes the form $(\tau - 1)\alpha$ for some $\alpha \in E$, where τ is a generator of $\mathrm{Gal}(E/F)$.*

Proof. By Theorem 3.2.1, there exists $\gamma \in E$ with $\mathrm{Tr}_{E/F}(\gamma) = \sum_{\sigma \in \mathrm{Gal}(E/F)} \sigma(\gamma) \neq 0$. Form

$$\beta := \sum_{k=0}^{n-1} \left(\sum_{0 \leq h < k} \tau^h \right) (a) \cdot \tau^k(\gamma) \neq 0,$$

with the convention $\left(\sum_{0 \leq h < 0} \tau^h\right)(a) = 0(a) = 0$ in the zeroth term.

One readily checks that $(1 - \tau)\beta = \mathrm{Tr}_{E/F}(\gamma)a$. Take $\alpha = -\mathrm{Tr}_{E/F}(\gamma)^{-1}\beta$. □

These results are named after the occurrence of the multiplicative version in [9, Nummer 90], although it was previously known to Kummer.

3.6 Cyclotomic polynomials

We shall review the rudiments of the theory of cyclotomic polynomials here. Warning: the exposition given below is neither the shortest or the cleanest. Please refer to other texts for the details.

Let $\bar{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ inside $\mathbb{C}$.

De nition 3.6.1. Let $n \in \mathbb{Z}_{\geq 1}$. An element $\zeta \in \bar{Q}$ is called an n-th root of unity if $\zeta^n = 1$; furthermore, it is called primitive if $\zeta^d \neq 1$ for all $1 \leq d < n$.

A basic fact is that the n-th roots of unity form a cyclic subgroup $\simeq \mathbb{Z}/n\mathbb{Z}$ of $\bar{\mathbb{Q}}^\times$. Its generators are precisely the primitive n-th roots of unity.

Lemma 3.6.2. *Let ζ_n be a primitive n-th root of unity. The cyclotomic eld $\mathbb{Q}(\zeta_n)$ is Galois over $\mathbb{Q}$.*

Proof. The extension is separable since we are in characteristic zero. Normality can be shown as follows. Every $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ must send ζ_n to another primitive n-th root of unity, say of the form ζ_n^k for some k. Hence $\sigma(\zeta_n) \in \mathbb{Q}(\zeta_n)$ and we deduce $\sigma(\mathbb{Q}(\zeta_n)) \subset \mathbb{Q}(\zeta_n)$. □

The cyclotomic polynomials Φ_n are de ned by requiring that

$$X^n - 1 = \prod_{d|n} \Phi_d(X) \tag{3.4}$$

holds for every $n \in \mathbb{Z}_{\geq 1}$. By Möbius inversion, this amounts to

$$\Phi_n(X) = \prod_{d|n} \left(X^{\frac{n}{d}} - 1\right)^{\mu(d)}$$

where μ stands for the Möbius function:

$$\mu(d) = \begin{cases} 0, & \text{if } d \text{ has square factors } \neq 1, \\ (-1)^k, & \text{if } d \text{ is a product of } k \text{ distinct primes.} \end{cases}$$

The idea of de ning $\Phi_n(X)$ is to remove all imprimitive contributions to $X^n - 1$. A straightforward formula can be given as follows

$$\Phi_n(X) = \prod_{\zeta:\text{primitive } n\text{-th root of 1}} (X - \zeta). \tag{3.5}$$

Indeed, it obviously satis es (3.4).

Recall that Euler's totient function ϕ is de ned as

$$\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times| = |\{0 \leq k < n : (k, n) = 1\}|, \quad n \in \mathbb{Z}_{\geq 1}.$$

Lemma 3.6.3. *For every n, the polynomial Φ_n is monic with integral coe cients. Its degree equals $\phi(n)$.*

Proof. Applying Möbius inversion to (3.4), we may write

$$\Phi_n = \frac{P}{Q}$$

for certain monic polynomials $P, Q \in \mathbb{Z}[X]$. Since $Q|P$ and Q is monic, the Euclidean division shows that the quotient Φ_n is monic with integral coe cients as well. As $\phi(n) = |\{0 \le k < n : (k,n) = 1\}|$, we obtain $\deg \Phi_n = \phi(n)$ by (3.5). □

Lemma 3.6.4. *For every n, the cyclotomic extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ has degree $\phi(n)$. Moreover, Φ_n equals the minimal polynomial of ζ_n.*

We reproduce the proof in [11, p.272] below.

Proof. Let P be the minimal monic polynomial of ζ_n over $\mathbb{Q}$. Since $\Phi_n(\zeta_n) = 0$ by (3.5), we have $P|\Phi_n$. If we can show $\Phi_n|P$, then $P = \Phi_n$ and it will follow that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg \Phi_n = \phi(n)$. It amounts to the assertion that every primitive n-th root of unity ζ is a root of P.

Every such ζ can be written as ζ_n^k with $(k,n) = 1$; by breaking k into a product of prime numbers, it su ces to show the following: for every prime number p with $(p,n) = 1$ and every $\zeta \in \bar{\mathbb{Q}}$,

$$P(\zeta) = 0 \implies P(\zeta^p) = 0.$$

Note that the same property holds if P is replaced by $X^n - 1$. Write $X^n - 1 = P(X)Q(X)$. The famous *Gauss Lemma* for polynomials asserts that $P, Q \in \mathbb{Z}[X]$. Recall the ring homomorphism of "reduction modulo p"

$$\begin{aligned} \mathbb{Z}[X] &\longrightarrow \mathbb{F}_p[X] \\ R(X) = \sum_i a_i X^i &\longmapsto \bar{R}(X) = \sum_i \bar{a}_i X^i. \end{aligned}$$

where $\bar{a}_i$ is the image of $a_i \in \mathbb{Z}$ in $\mathbb{F}_p$. If ζ is a root of P but ζ^p is not, then ζ^p must be a root of Q by our earlier observation. Equivalently, ζ is a common root of $Q(X^p)$ and $P(X)$. Now apply reduction modulo p, we have $\overline{Q(X^p)} = \overline{Q(X)}^p$ since $x^p = x$ holds in $\mathbb{F}_p$. Since $Q(X^p)$ and $P(X)$ has a non-trivial common divisor, which can be taken to be monic in $\mathbb{Z}[X]$ by Gauss Lemma, we conclude that $\overline{Q(X)}$ and $\overline{P(X)}$ has a common root. This is impossible: $\overline{P(X)Q(X)} = \overline{X^n - 1}$, whereas $X^n - 1$ is still separable as an element of $\mathbb{F}_p[X]$ since $(X^n - 1)' = nX^{n-1}$ and $(n,p) = 1$. We are led to contradiction. □

Corollary 3.6.5. *Φ_n is irreducible.*

Corollary 3.6.6. *The group $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is canonically isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$: to each $k \in (\mathbb{Z}/n\mathbb{Z})^\times$ we attach the automorphism characterized by $\zeta_n \mapsto \zeta_n^k$.*

Proof. As observed in the proof of Lemma 3.6.2, every $\mathbb{Q}$-automorphism σ of $\mathbb{Q}(\zeta_n)$ must take the asserted form for some $k \in (\mathbb{Z}/n\mathbb{Z})^\times$, which is unique by the primitivity of ζ_n. Since $|\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$, every $k \in (\mathbb{Z}/n\mathbb{Z})^\times$ is so realized. □

LECTURE 4

MODULES

4.1 Review: rings and ideals

By an *additive group* we mean a commutative group A with binary operation written as $+ : (a, b) \mapsto a + b$, whose unit element is denoted as 0.

A ring is a triple $(R, +, \cdot)$, where $+, \cdot : R \times R \to R$ are binary operations such that $(R, +)$ forms an additive group, and $(R, \cdot)$ forms a monoid satisfying the law of distributivity

$$x(y + z) = xy + xz, \quad (y + z)x = yx + zx.$$

As a rule, one writes R instead of $(R, +, \cdot)$ unless necessary.

In particular, our rings are assumed to have a unit 1 with respect to multiplication. A map $\phi : R \to R'$ is called a ring homomorphism if

- ⋆ $\phi(x + y) = \phi(x) + \phi(y)$,
- ⋆ $\phi(xy) = \phi(x)\phi(y)$,
- ⋆ $\phi(1) = 1$

hold for all $x, y \in R$. The notions of isomorphism, automorphism, etc. are deduced in the usual manner. The kernel of ϕ is $\ker(\phi) := \phi^{-1}(0)$; its image $\mathrm{im}(\phi)$ is a subring of R'.

De nition 4.1.1. A subgroup $\mathfrak{a}$ of a ring R is called a left (resp. right) ideal if $r\mathfrak{a} \subset \mathfrak{a}$ (resp. $\mathfrak{a}r \subset \mathfrak{a}$) for all $r \in R$. If $\mathfrak{a}$ is both a left and right ideal, we call it a two-sided ideal.

Given two ideals (either left, right or two-sided) $\mathfrak{a}$ and $\mathfrak{b}$, their sum is de ned as $\mathfrak{a} + \mathfrak{b} := \{a + b : a \in \mathfrak{a},\ b \in \mathfrak{b}\}$: it is the smallest ideal containing $\mathfrak{a} \cup \mathfrak{b}$. Similarly one can de ne the sum of any family of ideals in R. Intersections and sums of ideals are still ideals.

If $\mathfrak{a}$ is a two-sided ideal of R, the quotient ring $R/\mathfrak{a}$ is the quotient group $(R/\mathfrak{a}, +)$ (whose elements are additive cosets of the form $r + \mathfrak{a}$) equipped with the well-de ned multiplication

$$(r + \mathfrak{a})(r' + \mathfrak{a}) := rr' + \mathfrak{a}$$

for which the coset $1 + \mathfrak{a}$ gives the unit element. The ring structure is de ned so that the quotient map $R \twoheadrightarrow R/\mathfrak{a}$ is a ring homomorphism with kernel $\mathfrak{a}$. Conversely, for every

homomorphism $\phi : R \to R'$ we have the ring isomorphism

$$\begin{aligned} R/\ker(\phi) &\xrightarrow{\sim} \mathrm{im}(\phi) \\ r + \ker(\phi) &\mapsto \phi(r). \end{aligned}$$

The basic theorems on ring homomorphisms can be found in any reasonable textbook on algebra, such as [11, §2.7].

De nition 4.1.2. Let R be a ring, the opposite ring R^{op} is the same underlying additive group $(R, +)$ equipped with the "reversed" multiplication

$$(r, r') \mapsto r'r.$$

We say R is commutative if $R = R^{\mathrm{op}}$.

4.2 Modules: basic de nitions

In what follows, we x a ring R.

De nition 4.2.1. A left R-module is a commutative group $(M, +)$ equipped with a map

$$\begin{aligned} R \times M &\longrightarrow M \\ (r, m) &\longmapsto rm, \end{aligned}$$

called scalar multiplication, satisfying
(i) $r(r'm) = (rr')m$,
(ii) $r(m + m') = rm + rm'$,
(iii) $(r + r')m = rm + r'm$,
(iv) $1 \cdot m = m$
for all $r, r' \in R$ and $m, m' \in M$. If the scalar multiplication is written on the right $(m, r) \mapsto mr$, we deduce the notion of right R-module upon replacing (i) by the condition $(mr)r' = m(rr')$, while retaining the obvious analogues of (ii) and (iii).

Exercise 4.2.2. Explain that a left R-module is nothing but a right R^{op}-module, and vice versa.

For commutative R, there is no need to distinguish between left and right R-modules. To save clutter, the following discussions concern only the left modules; transition to the right ones is straightforward.

Example 4.2.3. The ring R itself can be made into a left (resp. right) R-module: simply take the scalar multiplication a orded by the ring structure. The submodules of R are exactly the left (resp. right) ideals.

De nition 4.2.4. A map $\phi : M \to M'$ between R-modules is called a homomorphism if

- ϕ is a homomorphism between the underlying additive groups,
- $\phi(rm) = r\phi(m)$ for all $r \in R$ and $m \in M$.

One deduces the notions of isomorphisms, automorphisms, etc. The kernel of ϕ is the submodule $\ker(\phi) := \phi^{-1}(0)$ of M.

For a submodule N of M, the quotient module M/N is the quotient additive group M/N endowed with scalar multiplication $r(m+N) := rm+N$, so that the quotient map $M \twoheadrightarrow M/N$ becomes a homomorphism between modules. As in the case of groups, we have the familiar properties on homomorphisms:

1. If $\phi : M \to M'$ is a homomorphism, then $m + \ker(\phi) \mapsto \phi(m)$ gives an isomorphism $M/\ker(\phi) \xrightarrow{\sim} \mathrm{im}(\phi)$.

2. If ϕ is surjective, then there is a bijection

$$\begin{aligned} \{\text{submodules of } M'\} &\overset{1:1}{\longleftrightarrow} \{\text{submodules } N \subset M,\ N \supset \ker(\phi)\} \\ N' &\mapsto \phi^{-1}(N') \\ \phi(N) &\hookleftarrow N; \end{aligned}$$

   under this bijection we have the isomorphism $M/N \xrightarrow{\sim} M'/N'$ given by $m + \ker(\phi) \mapsto \phi(m)$.

3. Let M, N be submodules of some ambient module Ω, then the composition of $M \hookrightarrow M + N \twoheadrightarrow (M + N)/N$ induces an isomorphism

$$M/(M \cap N) \xrightarrow{\sim} (M + N)/N.$$

Detailed but boring proofs can be found everywhere. De ne the *cokernel* of $\phi : M \to M'$ as

$$\mathrm{coker}(\phi) := M'/\mathrm{im}(\phi).$$

One important feature of the category of R-modules (we shall discuss the categories later) is that for every M, M', the set of homomorphisms $\mathrm{Hom}_R(M, M')$ is an additive group: given ϕ, ϕ', de ne $\phi + \phi'$ as the pointwise addition:

$$\phi + \phi' : m \longmapsto \phi(m) + \phi'(m).$$

The unit element in $\mathrm{Hom}_R(M, M')$ is the zero homomorphism $0 : \forall m \mapsto 0$. The composition of homomorphisms $\mathrm{Hom}_R(M'M'') \times \mathrm{Hom}_R(M, M') \to \mathrm{Hom}_R(M, M'')$ is then *bi-additive*, namely

$$\phi(\psi_1 + \psi_2) = \phi\psi_1 + \phi\psi_2, \quad (\psi_1 + \psi_2)\phi = \psi_1\phi + \psi_2\phi.$$

Here we write $\phi\psi = \phi \circ \psi$, etc.

Let us specialize to the case of *endomorphisms* $\mathrm{End}_R(M) := \mathrm{Hom}_R(M, M)$. With the aforementioned operations, $\mathrm{End}_R(M)$ becomes a ring whose unit element 1 is the identity homomorphism id_M.

Finally, we will write 0 for the *zero module* $\{0\}$.

4.3 Direct sums and free modules

Fix a ring R. In what follows, R-modules mean left R-modules.

De nition 4.3.1. Let $(M_i)_{i\in I}$ be a family of R-modules indexed by a set I. De ne its *direct sum* or *coproduct* as

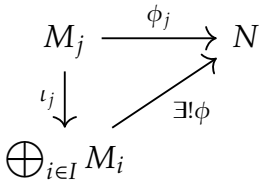
$$\bigoplus_{i\in I} M_i := \left\{ (m_i)_{i\in I} \in \prod_{i\in I} M_i : m_i = 0 \text{ for all but nitely many } i \right\}$$

The direct sum comes equipped with a family of inclusion homomorphisms

$$\iota_j : M_j \longrightarrow \prod_{i\in I} M_i$$
$$m_j \longmapsto (m_i)_{i\in I}, \quad m_i := \begin{cases} m_j, & i = j, \\ 0, & i \neq j. \end{cases}$$

When I is nite, say $I = \{1, \dots, n\}$, we write $M_1 \oplus \cdots \oplus M_n$ for their direct sum. Direct sum satis es the following *universal property*:

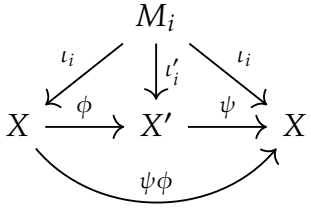
Lemma 4.3.2. *Let $\phi_i : M_i \to N$ $(i \in I)$ be a family of homomorphisms between R-modules. There exists a unique homomorphism $\phi : \bigoplus_{i\in I} M_i \to N$ making the following diagram commute*



for each $j \in I$. Recall that commutativity here signi es that $\phi \circ \iota_j = \phi_j$.

Proof. We must have $\phi(\iota_j(m_j)) = \phi_j(m_j)$ for each $j \in I$. By the de nition of $\bigoplus_i M_i$, this uniquely determines the homomorphism ϕ. □

Remark 4.3.3. It is a typical result in *category theory* that such a universal property characterizes $\bigoplus_{i\in I} M_i$ together with $(\iota_i)_{i\in I}$, up to a unique isomorphism. Although categories will not discussed in this lecture, we can sketch the argument as follows. Consider two R-modules X, X' with families of homomorphisms $\iota_i : M_i \to X$ and $\iota'_i : M_i \to X'$ satisfying the assertion of Lemma 4.3.2. Then taking $N = X$ and X' yields unique arrows $\phi : X \to X'$ and $\psi : X' \to X$ sitting inside commutative diagrams



for every $i \in I$. The uniqueness part of Lemma 4.3.2 (for X) in the case $N = X$ asserts that $\psi\phi = \mathrm{id}_X$. The same reasoning gives $\phi\psi = \mathrm{id}_{X'}$ as well. Hence ϕ and ψ are the required unique isomorphisms.

The universal property may also be summarized as a natural isomorphism

$$\begin{aligned}\mathrm{Hom}_R\left(\bigoplus_{i\in I} M_i, -\right) &\xrightarrow{\sim} \prod_{i\in I} \mathrm{Hom}_R(M_i, -)\\ \phi &\mapsto (\phi\iota_i)_{i\in I}\end{aligned}$$

Similarly, one de nes the *direct product* or simply *product* $\prod_{i\in I} M_i$ by removing the condition "$m_i = 0$ for all but nitely many i" in De nition 4.3.1. It is equipped with a family of projection maps $\pi_j : \prod_{i\in I} M_i \to M_j$ $(j \in I)$. Direct products satisfy the universal property

$$\begin{aligned}\mathrm{Hom}_R\left(-, \bigoplus_{i\in I} M_i\right) &\xrightarrow{\sim} \prod_{i\in I} \mathrm{Hom}_R(-, M_i)\\ \phi &\mapsto (\pi_i\phi)_{i\in I}.\end{aligned}$$

Exercise 4.3.4. Check the universal property above for $\prod_{i\in I} M_i$.

Notice that when I is nite, we have $\bigoplus_{i\in I} M_i = \prod_{i\in I} M_i$.

De nition 4.3.5. An R-module is called *free* with basis X if

- ⋆ the subset X generates M: every element of M can be written as a nite sum $\sum_{x\in X} r_x x$;
- ⋆ X is *linearly independent*: we have $\sum_x r_x x = \sum_x s_x x$ if and only if $r_x = s_x$ for all $x \in X$.

In other words, there is an isomorphism from $R^{\oplus X}$ (the direct sum of X copies of the module R) onto M, sending $\iota_x(1)$ to x for each x.

Exercise 4.3.6. Establish the following universal property for free modules. Let X be a set and form the free module $R^{\oplus X}$; it is endowed with the natural inclusion map $X \hookrightarrow R^{\oplus}$ (between sets). For every R-module M and any map $f : X \to M$, there exists a unique homomorphism $\phi : R^{\oplus X} \to M$ between R-modules making the diagram

$$\begin{array}{ccc} X & \hookrightarrow & R^{\oplus X} \\ & \searrow^{f} & \downarrow{\scriptstyle \exists!\phi} \\ & & M \end{array}$$

commutative.

We say a ring R has left *IBN* (invariant basis number for left modules) if $R^{\oplus X} \simeq R^{\oplus Y} \iff |X| = |Y|$; if that holds, one can well-de ne the notion of rank of free left R-modules. Likewise, there is a notion of right IBN. Rings with this property include the elds, commutative rings, nite rings and division rings, as discussed below.

Example 4.3.7. Let D be a division ring, i.e. $D^\times = D \setminus \{0\}$. A left (resp. right) D-module is called a left (resp. right) D-vector space. When D is a eld (= commutative division ring), we revert to the familiar set-up of linear algebra. Many properties carry over to the noncommutative case, for instance:

- ⋆ every D-vector space V is free, i.e. V admits a basis;
- ⋆ every generating set of V contains a basis, and every linearly independent subset can be enlarged to a basis;
- ⋆ the bases of V have the same cardinality, which we de ne to be the dimension $\dim_D V$ of V.

Life is not always so easy, however. To take one example: can you generalize the determinants to nite-dimensional D-vector spaces? See [24, pp.5–8] for a discussion on the so-called *Dieudonné determinant*.

More detailed discussions on IBN can be found in [14, §1].

4.4 Exact sequences

Hereafter, we x a ring and the R-modules are assumed to be left modules unless otherwise speci ed..

De nition 4.4.1. A sequence of R-modules

$$\cdots \xrightarrow{f^{-2}} X^{-1} \xrightarrow{f^{-1}} X^0 \xrightarrow{f^0} \cdots \to X^i \xrightarrow{f^i} \cdots$$

(possibly in nite or even cyclic, in which case we take $i \in \mathbb{Z}/n\mathbb{Z}$) connected by homomorphisms $f^i : X^i \to X^{i+1}$ is called a *complex* if

$$\forall i,\ \ker(f^{i+1}) \supset \mathrm{im}(f^i), \quad \text{i.e. } f^{i+1}f^i = 0,$$

in which case we set $H^i(X^\bullet) := \ker(f^{i+1})/\mathrm{im}(f^i)$. A complex $(X^\bullet, f^\bullet)$ with $H^i(X^\bullet) = 0$ for all i is called *exact*.

Exact sequence is an indispensable tool in algebra and will be used systematically in what follows. Let us look at some special cases.

1. The sequence $0 \to X \to Y$ is exact if and only if $X \to Y$ is injective. Note that the only arrow that emanates or lands in the zero module 0 is the zero homomorphism.

2. The sequence $X \to Y \to 0$ is exact if and only if $X \to Y$ is surjective.

3. The sequence $0 \to X \xrightarrow{\phi} Y \to 0$ is exact if and only if $\phi : X \to Y$ is an isomorphism.

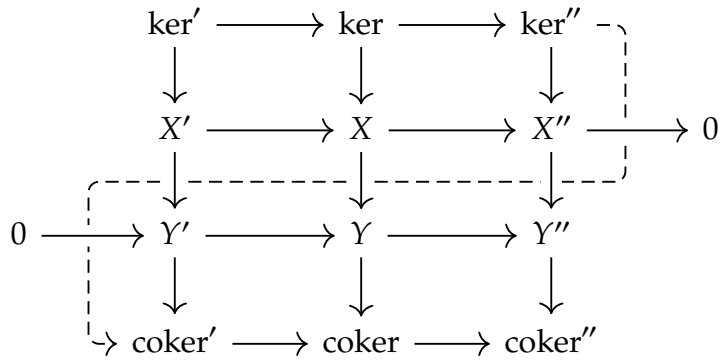
4. *Short exact sequences* are exact sequences of the form

$$0 \to M' \to M \to M'' \to 0.$$

In this case, exactness amounts to saying that M' (resp. M'') can be regarded as a submodule (resp. quotient) of M (cf. the previous two cases.), so that $M'' = M/M'$ under these identi cations.

To illustrate the ideas, consider the commutative diagram

(4.1)



with the self-evident notations

$$\begin{aligned} \ker &:= \ker[X \to Y], \\ \operatorname{coker} &:= \operatorname{coker}[X \to Y] = Y/\operatorname{im}[X \to Y], \end{aligned}$$

etc., and we assume that the rows involving $X^\bullet$, $Y^\bullet$ are both exact.

The de nitions of the maps $\ker' \to \ker$, $\ker \to \ker''$ and $\operatorname{coker}' \to \operatorname{coker}$, $\operatorname{coker} \to \operatorname{coker}''$ can be read o from the commutativity of the diagram, which we leave to the reader. It remains to explain the dashed *connecting homomorphism*:

(i) given $x'' \in \ker''$, choose any $X \ni x \mapsto x''$;
(ii) let $x \mapsto y \in Y$, then the commutativity of the diagram forces $y \mapsto 0 \in Y''$;
(iii) hence $\exists y' \in Y'$, $y' \mapsto y$.

One may check that the assignment $x \rightsquigarrow y'$ induces a homomorphism $\ker'' \to \operatorname{coker}'$ that is independent of all choices.

Proposition 4.4.2 (Snake lemma)**.** *In the diagram* (4.1)*, the sequence*

$$\ker' \to \ker \to \ker'' \to \operatorname{coker}' \to \operatorname{coker} \to \operatorname{coker}''$$

is exact.

The proof is also a typical diagram-chasing. The reader is urged to try it out by him- or herself.

Remark 4.4.3. In practice, we often encounter snake diagrams with short exact sequences $0 \to X' \to X \to X'' \to 0$ and $0 \to Y' \to Y \to Y'' \to 0$. In that case, the resulting "snake sequence" can be augmented to an exact sequence $0 \to \ker' \to \cdots \to \operatorname{coker}'' \to 0$.

4.5 Chain conditions

Retain the earlier conventions on rings and modules.

De nition 4.5.1 (Ascending chain condition)**.** An R-module M is said to be *noetherian* if it satis es the following ascending chain condition, often abbreviated as ACC: every chain

$$M_1 \subset M_2 \subset M_3 \subset \cdots$$

of submodules of M stabilizes, that is, there exists n such that $M_{n'} = M_n$ for all $n' \geq n$.

De nition 4.5.2 (Descending chain condition)**.** An R-module M is said to be *artinian* if it satis es the following descending chain condition, often abbreviated as DCC: every chain

$$M_1 \supset M_2 \supset M_3 \supset \cdots$$

of submodules of M stabilizes, that is, there exists n such that $M_{n'} = M_n$ for all $n' \geq n$.

One of the motivation for chain conditions is E. Artin's generalization of Wedderburn's Theorem on semisimple algebras.

Note that being noetherian is equivalent to that every nonempty family $\mathcal{S}$ of submodules of M contains a maximal element with respect to $\subset$. Indeed, assuming ACC, if $\mathcal{S}$ has no maximal elements, we may take any M_1 from S, then select $\mathcal{S} \ni M_2 \supsetneq M_1$ and so forth, thereby obtain an ascending chain that does not stabilize. Conversely, let $\mathcal{S}$ be the family $\{M_1, M_2, \ldots\}$ with $\forall i,\ M_i \subset M_{i+1}$; if $\mathcal{S}$ has a maximal element M_n, then the chain $M_1 \subset M_2 \subset \cdots$ will stabilize after M_n. In the same manner, being artinian is equivalent to that every nonempty family $\mathcal{S}$ of submodules contains a minimal element. Let us look at some examples.

1. View $\mathbb{Z}$ as a $\mathbb{Z}$-module. It is noetherian since every submodule (= ideal) is of the form $m\mathbb{Z}$ for some $m \in \mathbb{Z}_{\geq 0}$, and

$$m_1\mathbb{Z} \subset m_2\mathbb{Z} \subset m_3\mathbb{Z} \subset \cdots \iff \cdots \mid m_3 \mid m_2 \mid m_1;$$

   thus ACC holds true as m_1 has only nitely many factors. On the other hand, DCC fails obviously: consider the ascending chain $M_i := 2^i\mathbb{Z}$ for $i \in \mathbb{Z}_{\geq 0}$.

2. Let p be a prime number and consider the $\mathbb{Z}$-submodule $\mathbb{Z}_{(p)}/\mathbb{Z}$ of $\mathbb{Q}/\mathbb{Z}$ where

$$\mathbb{Z}_p := \left\{ \frac{a}{p^k} \in \mathbb{Q} : k \geq 0,\ a \in \mathbb{Z} \right\}.$$

   One can show that submodules of $\mathbb{Z}_{(p)}/\mathbb{Z}$ are of the form $p^{-k}\mathbb{Z}/\mathbb{Z}$ for $k \geq 0$. Therefore DCC holds but ACC fails: we have a chain $\frac{1}{p}\mathbb{Z} \subsetneq \frac{1}{p^2}\mathbb{Z} \subsetneq \cdots$.

3. Suppose that R contains some division ring D, so that every R-module M becomes a D-vector space. If $\dim_D M$ is nite, then ACC and BCC both hold by reason of dimensions.

4. Finite modules are both artinian and noetherian.

Exercise 4.5.3. Verify the assertion on the $\mathbb{Z}$-submodules of $\mathbb{Z}_{(p)}/\mathbb{Z}$. Hint: if $(a, p) = 1$, show that $ap^{-k} + \mathbb{Z}$ generates the submodule $p^{-k}\mathbb{Z}/\mathbb{Z}$ of $\mathbb{Z}_{(p)}/\mathbb{Z}$.

Lemma 4.5.4. *An R-module M is noetherian if and only if every submodule N is nitely generated.*

Proof. Suppose M is noetherian and x a submodule N. Consider the family $\mathcal{S}$ consisting of nitely generated submodules of N, it must has a maximal element N'. We claim that $N' = N$: otherwise $N' + Rx$ would be a larger element in $\mathcal{S}$ whenever $x \in N \setminus N'$. This shows the nite generation of N.

Conversely, suppose every $N \subset M$ is nitely generated. Let $M_1 \subset M_2 \subset \cdots$ be an ascending chain of submodules of M. Then $N := \bigcup_{i \geq 1} M_i$ is a submodule as well; let $x_1, \ldots, x_n$ be a set of generators of N. For every $1 \leq i \leq n$, we have $x_i \in M_{k_i}$ for some $k_i \geq 0$, therefore the chain stabilizes after M_k with $k := \max\{k_1, \ldots, k_n\}$. □

Proposition 4.5.5. *Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence. Then M is noetherian (resp. artinian) if and only if M' and M'' are both noetherian (resp. artinian).*

Proof. We shall treat the noetherian case only, the arguments for the artinian case are completely similar.

Suppose M noetherian. Every ascending chain in M' is an ascending chain in M, and every ascending chain $(M''_i)_{i \geq 1}$ of M'' is the image of an ascending chain $(M_i)_{i \geq 1}$ in M with $M_i \supset M'$, so that $M''_i = M''_{i+1} \iff M_i = M_{i+1}$. Hence M' and M'' are noetherian.

Conversely, suppose M' and M'' are noetherian. Let $M_1 \subset M_2 \subset \cdots$ be an ascending chain of submodules in M, then so are $(M_i + M')/M'$ and $M_i \cap M'$ in $M/M' \simeq M''$ and M', respectively. If M' and M'' are both noetherian, then for $i \gg 0$ we have

$$M_{i+1} \cap M' = M_i \cap M', \quad \frac{M_i + M'}{M'} = \frac{M_{i+1} + M'}{M'},$$

therefore there are natural isomorphisms

$$\frac{M_{i+1}}{M_i} = \frac{M_{i+1}/M_{i+1} \cap M'}{M_i/M_i \cap M'} \simeq \frac{(M_{i+1} + M')/M'}{(M_i + M')/M'} = 0.$$

We conclude that M is noetherian as well. □

Corollary 4.5.6. *Let N, M be submodules of some R-module Ω. If M and N are both noetherian (resp. artinian), then $M + N$ is noetherian (resp. artinian) as well.*

Proof. Use the short exact sequence

$$0 \to N \to M + N \to \frac{M + N}{N} \to 0,$$

and note that $(M + N)/N \simeq M/M \cap N$. Now apply Proposition 4.5.5. □

De nition 4.5.7. A ring R is called left noetherian (resp. artinian) if R is noetherian (resp. artinian) as a left R-module. Idem for right noetherian/artinian rings.

Recall that a module M is called nitely generated if there exists $m_1, \ldots, m_n \in M$ such that $M = \bigoplus_{i=1}^{n} Rm_i$. This amounts to saying that M is a quotient of $R^{\oplus n}$ for some $n \in \mathbb{Z}_{\geq 0}$ — use the universal property for free modules (Exercise 4.3.6).

Proposition 4.5.8. *If R is left noetherian (resp. artinian), then every nitely generated left R-module is noetherian (resp. artinian). Idem for right R-modules.*

Proof. Given an exact sequence $R^{\oplus n} \to M \to 0$, we have seen that $R^{\oplus n}$ is noetherian (resp. artinian) by applying the previous Corollary (with induction on n). It remains to apply Proposition 4.5.5. □

4.6 Hilbert basis theorem

When R is a commutative ring, there is no need to distinguish the left and right noetherian or artinian properties. For a commutative ring R, we write $\langle x_1, \ldots, x_n \rangle$ to denote the ideal generated by $x_1, \ldots, x_n \in R$.

For any polynomial $f = \sum_{k=0}^{n} a_k X^k \in R[X]$ with $a_n \neq 0$, we call $\mathrm{in}(f) := a_n$ the *initial* or *leading coe cient* of f.

Theorem 4.6.1 (Hilbert)**.** *Let R be a commutative ring. If R is noetherian, so is the polynomial ring $R[X]$ over R.*

Proof. By Lemma 4.5.4, it su ces to show the nite generation of every ideal $\mathfrak{a}$ of $R[X]$. We choose a sequence of elements $f_1, \ldots \in \mathfrak{a}$ as follows. Choose $f_1 \in \mathfrak{a}$ to be a nonzero element with $\deg f_1$ minimal. Assume that $f_1, \ldots, f_k$ have been chosen. If they already generate $\mathfrak{a}$, our algorithm stops, otherwise choose f_{k+1} to be an element in $\mathfrak{a} \setminus \langle f_1, \ldots, f_i \rangle$ with minimal degree. We contend that the algorithm stops in nitely many steps.

For every $i \geq 1$, let $a_i := \mathrm{in}(f_i)$. The ideal of R generated by $a_1, a_2, \ldots$ is generated by a nite subsequence, say $a_1, \ldots, a_n$. Suppose that one can choose $f_{n+1} \in \mathfrak{a} \neq \langle f_1, \ldots, f_n \rangle$ by the recipe above. There exists $u_1, \ldots, u_n \in R$ such that

$$\mathrm{in}(f_{n+1}) = \sum_{i=1}^{n} u_i a_i.$$

Observe that $\deg f_{n+1} \geq \deg f_i$ for all $1 \leq i \leq n$ by construction, hence

$$f_{n+1} - \sum_{i=1}^{n} u_i f_i \cdot X^{\deg f_{n+1} - \deg f_i}$$

has degree less than $\deg f_{n+1}$; moreover, it lies in $\mathfrak{a} \setminus \langle f_1, \ldots, f_n \rangle$. This leads to a contradiction. We conclude $\langle f_1, \ldots, f_n \rangle = \mathfrak{a}$. □

Remark 4.6.2. It follows that $R[X_1, \ldots, X_n]$ is noetherian if R is noetherian, for every $n \in \mathbb{Z}_{\geq 1}$. Indeed,

$$R[X_1, \ldots, X_n] \simeq (\cdots((R[X_1])[X_2])\cdots)[X_n],$$

and we may argue by induction on n.

Using Hilbert's theorem together with our earlier results, one obtains many examples of noetherian rings, such as the quotient rings of the polynomial ring $\Bbbk[X_1, \ldots, X_n]$ where $\Bbbk$ is a eld.

Exercise 4.6.3. Give an example of non-noetherian commutative ring.

LECTURE 5

TENSOR PRODUCTS AND ALGEBRAS

We will occasionally denote the unit of a ring R as 1_R.

5.1 Categories at a glance

In these lectures, a *category* C is a class of objects $\mathrm{Ob}(C)$ together with a set $\mathrm{Hom}(X, Y)$ of morphisms for every $X, Y \in \mathrm{Ob}(C)$, with the structures below.

- ⋆ There is a *composition map* $\mathrm{Hom}(Y, Z) \times \mathrm{Hom}(X, Y) \to \mathrm{Hom}(X, Z)$ for all $X, Y, Z \in \mathrm{Ob}(C)$, written as $(f, g) \mapsto fg = f \circ g$. It is associative: $f(gh) = (fg)h$ provided that the composites make sense. It is convenient to represent morphisms as arrows:
$$f \in \mathrm{Hom}(X, Y) \leftrightarrow [f : X \to Y] \leftrightarrow \left[X \xrightarrow{f} Y \right].$$
Therefore one can talk about commutative diagrams in a category.
- ⋆ For every object X, there exists an *identity morphism* $\mathrm{id}_X \in \mathrm{Hom}(X, X)$ such that $\mathrm{id}_X \circ f = f$ and $g \circ \mathrm{id}_X = g$ for all $Y \in \mathrm{Ob}(C)$, $f : Y \to X$ and $g : X \to Y$.

Exercise 5.1.1. Show that for each X, the identity morphism id_X is unique.

Remark 5.1.2. Categories whose objects form a set are called *small*. Small categories are not enough for many applications, whereas a category theory with proper classes is somehow messy. A standard practice is to use *Grothendieck universes* to circumvent the set-theoretical di culties; see [17, I.6].

Given a category C, de ne its *opposite* C^{op} as the category with the same objects and morphisms, but the arrows are reversed, namely
$$\mathrm{Hom}_{C^{\mathrm{op}}}(X, Y) := \mathrm{Hom}_C(Y, X),$$
$$\underbrace{f \circ g}_{C^{\mathrm{op}}} := \underbrace{g \circ f}_{C}.$$

Trivially, we have $(C^{\mathrm{op}})^{\mathrm{op}} = C$.
Let us look at some examples.

Category	Objects	Morphisms	Composition
Set	sets	maps	$\circ$
Grp	groups	homomorphisms	
Ring	rings		
R-**Mod**	left R-modules		
Mod-R	right R-modules		
$\Pi_1(X)$	points in a space X	paths up to homotopy	concatenation
$(P, \leq)$: partially ordered	elements of P	$\mathrm{Hom}(x,y) = \begin{cases} \{\leq\}, & x \leq y \\ \emptyset, & x \not\leq y \end{cases}$	transitivity of $\leq$

The notions of isomorphisms, automorphisms, inverses, etc. are de ned in the usual manner in any category. In particular, the automorphisms of an object form a group under composition. For example, the automorphism group of an object x in $\Pi_1(X)$ is nothing but the *fundamental group* $\pi_1(X, x)$ when X is reasonable (path-connected, locally contractible, etc.)

The *universal properties* in algebra can be succinctly interpreted in terms of initial or terminal elements.

De nition 5.1.3. An object X in a category C is an initial (resp. terminal) object if $\mathrm{Hom}(X, Y)$ (resp. $\mathrm{Hom}(Y, X)$) has exactly one element for every $Y \in \mathrm{Ob}(C)$.

Initial and terminal objects are "dual" properties: one can pass in between upon replacing C by C^{op}.

Example 5.1.4. The ring $\mathbb{Z}$ is initial in **Ring**; any set with cardinality one is terminal in **Set**.

Proposition 5.1.5. *Initial elements are unique up to a unique isomorphism. Idem for terminal elements.*

Proof. Let X, X' be two initial elements of C. Then there is a unique morphism $\varphi : X \to Y$ (resp. $\psi : Y \to X$). The composite $\varphi\psi$ is the unique morphism from Y to itself, namely id_Y. Similarly we have $\psi\varphi = \mathrm{id}_X$. Thus φ and ψ are the required unique isomorphisms. To deal with the terminal objects, simply replace C by C^{op}. □

5.2 Functors and natural transformations

According to S. MacLane [17], one of the founders of category theory, categories were introduced in order to explain the *functors*, the latter were in turn designed to account for *natural transformations*. To set up the theory, however, one has to proceed in the reverse direction.

De nition 5.2.1. A *functor* $F : C_1 \to C_2$ between categories is a rule that

- ⋆ assigns an object FX of C_2 for every object X of C_1;
- ⋆ assigns a morphism $Ff : FX \to FY$ for every morphism $f : X \to Y$ in C_1, which sends id_X to id_{FX} and respects compositions: we have $F(fg) = (Ff)(Fg)$.

De nition 5.2.2. A *natural transformation* between functors $F, G : C_1 \to C_2$ is a family $\varphi = (\varphi_X)_{X \in \mathrm{Ob}(C_1)}$ of morphisms $\varphi_X : FX \to GX$, such that the diagram

$$\begin{array}{ccc} FX & \xrightarrow{Ff} & FY \\ {\scriptstyle \varphi_X}\downarrow & & \downarrow{\scriptstyle \varphi_Y} \\ GX & \xrightarrow[Gf]{} & GY \end{array}$$

commutes for every morphism $f : X \to Y$ in C_1.

Natural transformations can be composed by setting $(\varphi\psi)_X = \varphi_X\psi_X$, therefore we deduce the notion of inverses and isomorphisms, denoted in the usual way as $\varphi : F \xrightarrow{\sim} G$, etc. Note that the natural transformations can also be conceived as "morphisms between functors" if we know how to make the functors $C_1 \to C_2$ into a category.

De nition 5.2.3. An equivalence between categories C_1, C_2 is a pair of functors

$$C_1 \underset{G}{\overset{F}{\rightleftarrows}} C_2$$

together with isomorphisms

$$FG \simeq \mathrm{id}_{C_2}, \quad GF \simeq \mathrm{id}_{C_1}$$

(surely, id signi es the identity functors). In this case we say that F and G are quasi-inverses of each other.

Note that the notion above is much more useful than the naive notion of isomorphisms $FG = \mathrm{id}_{C_2}$, $GF = \mathrm{id}_{C_1}$. Quasi-inverses are not unique in general.

Example 5.2.4. Let $\mathbf{Vect}(\mathbb{C})$ be the category of complex vector spaces. The assignment

$$D : V \longmapsto V^\vee := \mathrm{Hom}_{\mathbb{C}}(V, \mathbb{C})$$

extends to a functor from $\mathbf{Vect}(\mathbb{C})$ to its opposite, namely to each linear map $f : V \to W$ we attach its dual $f^\vee : W^\vee \to V^\vee$, which sends a linear functional $\lambda : V \to \mathbb{C}$ to $f^\vee(\lambda) := \lambda \circ f : W \to \mathbb{C}$. As is well-known, there is a canonical embedding

$$V \hookrightarrow V^{\vee\vee}$$

for each vector space V into its bidual. It is actually a natural transformation

$$\mathrm{id} \to DD,$$

which is an isomorphism exactly when $\dim V$ is nite. By restricting D to the subcategory $\mathbf{Vect}_f(\mathbb{C})$ of nite-dimensional spaces, D yields an equivalence between $\mathbf{Vect}_f(\mathbb{C})$ and its opposite.

5.3 Bimodules

We have de ned the notion of left and right modules over a ring. A bimodule is a structure endowed with left and right scalar multiplications which commute with each other.

De nition 5.3.1. An (R, S)-bimodule is an additive group M which is simultaneously a left R-module and a right S-module, satisfying

$$r(ms) = (rm)s, \quad m \in M,\ r \in R,\ s \in S.$$

The formula above can thus be written as rms, conceived as some sort of associativity. There are evident notions of homomorphisms, isomorphisms and quotients, etc. for (R, S)-bimodules. The category so obtained will be written as (R, S)-**Mod**.

De nition 5.3.2. A map $\varphi : M \to M'$ between (R, S)-bimodules is called a homomorphism if it is simultaneously a homomorphism between left R-modules and right S-modules.

Example 5.3.3. Every left R-module M has a unique structure of $(R, \mathbb{Z})$-bimodule: we can and must set $ma := am$, where $m \in M$, $a \in \mathbb{Z}$. Since the natural homomorphism $\mathbb{Z} \to R$ lands in the center of R, we see M is indeed a bimodule. Similarly, right R-modules are nothing but $(\mathbb{Z}, R)$-bimodules.

All these identi cations can be stated in terms of equivalences (or even isomorphisms) between categories of modules.

Example 5.3.4. When R is commutative, every R-module M is naturally an (R, R)-bimodule: simply set $rmr' := rr'm$.

Convention 5.3.5. Hereafter, we will often use the notation ${}_RM$ (resp. M_S, ${}_RM_S$) to denote that M is a left R-module (resp. right S-module, (R, S)-bimodule).

5.4 Balanced products and tensor products

Balanced products generalize the notion of bilinear maps in linear algebra. Our main reference is [12, §3.7]. The modern notion of tensor products is commonly attributed to H. Whitney [28].

De nition 5.4.1. Let R be a ring. Consider modules M_R, ${}_RN$ and an additive group A. A map

$$B : M \times N \to A$$

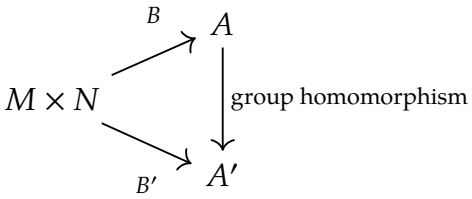
is called a *balanced product* if it satis es

(i) $B(x + x', y) = B(x, y) + B(x', y)$,
(ii) $B(x, y + y') = B(x, y) + B(x, y')$,
(iii) $B(xr, y) = B(x, ry)$,

where $x, x' \in M$, $y, y' \in N$ and $r \in R$ are arbitrary. The set of all balanced products $B : M \times N \to A$ is denoted by $\mathrm{Bil}(M, N; A)$. It forms an additive group.

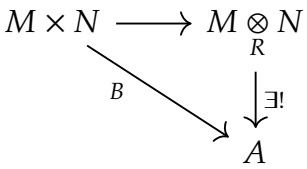
When $R = \mathbb{Z}$, we recover the notion of bi-additive maps from $M \times N$ to A where M, N, A are all additive groups.

Given M_R, ${}_R N$ as above, a *morphism* from $B \in \mathrm{Bil}(M, N; A)$ to $B' \in \mathrm{Bil}(M, N; A')$ is de ned as a commutative diagram



Such morphisms can be composed in the obvious manner, thereby making the balanced products with domain $M \times N$ into a category $\mathbf{Bil}(M, N; *)$.

De nition 5.4.2. The *tensor product* of M and N is a balanced product $M \times N \to M \underset{R}{\otimes} N$ satisfying the following universal property: for every balanced product $B : M \times N \to A$, there exists a unique group homomorphism $M \underset{R}{\otimes} N \to A$ making



commutative. In other words, it is an initial object in the category $\mathbf{Bil}(M, N; *)$.

Proposition 5.4.3. *Tensor products of M and N, if they exist, are unique up to a unique isomorphism.*

Proof. Invoke Proposition 5.1.5. □

It is customary to say that $M \underset{R}{\otimes} N$ *is* the tensor product. Nevertheless, one should bear in mind that tensor products make little sense without the accompanying map $M \times N \to M \underset{R}{\otimes} N$, which we often write as $(x, y) \mapsto x \otimes y$.

Lemma 5.4.4. *For all M_R, ${}_R N$, tensor product $M \times N \to M \underset{R}{\otimes} N$ exists.*

Proof. Consider the free $\mathbb{Z}$-module (i.e. additive group) F with the set $M \times N$ as its basis. De ne I to be the submodule generated by elements of the form

$$(x + x', y) - (x, y) - (x', y)$$
$$(x, y + y') - (x, y) - (x, y')$$
$$(xr, y) - (x, ry)$$

where $(x, y) \in M \times N$ and $r \in R$. Put $M \underset{R}{\otimes} N := F/I$ and denote the image of $(x, y) \in M \times N$ in F/I as $x \otimes y$. We claim that the map $M \times N \to M \underset{R}{\otimes} N$ sending (x, y) to $x \otimes y$ is the tensor product.

By construction, we obviously have the properties $(x + x') \otimes y = x \otimes y + x' \otimes y$, $x \otimes (y + y') = x \otimes y + x \otimes y'$ and $xr \otimes y = x \otimes ry$ inside $M \underset{R}{\otimes} N = F/I$, thus $(x, y) \mapsto x \otimes y$ is indeed a balanced product. Now let $B : M \times N \to A$ be any balanced product. By the universal property of free modules, there exists a unique homomorphism

$$\begin{aligned} F &\longrightarrow A \\ (x, y) &\longmapsto B(x, y). \end{aligned}$$

By the de nition of I together with the fact that B is balanced, one sees $I \subset \ker(F \to A)$. Hence there is a unique homomorphism

$$\begin{aligned} M \underset{R}{\otimes} N &\longrightarrow A \\ x \otimes y &\longmapsto B(x, y). \end{aligned}$$

In other words, there is a unique homomorphism of balanced products from $M \times N \to M \underset{R}{\otimes} N$ to B. □

5.5 Functorial properties of tensor products

Consider bimodules ${}_R M_S$ and ${}_S N_T$ where R, S, T are rings. We have de ned the additive group $M \underset{S}{\otimes} N$. As the notation suggests, the scalar multiplications by R and T should pass to $M \underset{S}{\otimes} N$.

Lemma 5.5.1. *There exists an (R, T)-bimodule structure on $M \underset{S}{\otimes} N$, characterized by*

$$\begin{aligned} r(x \otimes y) &= rx \otimes y, \\ (x \otimes y)t &= x \otimes (yt) \end{aligned}$$

for all $(x, y) \in M \times N$ and $r \in R$, $t \in T$.

Proof. One may tend to use the explicit construction in the proof of Lemma 5.4.4. A slicker way is to exploit the universal property as follows. Recall that $M \times N \to M \underset{S}{\otimes} N$ is a balanced product. Given $r \in R$, the map

$$L_r : (x, y) \mapsto rx \otimes y$$

is also balanced, thus induces a group homomorphism $\lambda_r : x \otimes y \mapsto rx \otimes y$. The relation $\lambda_{r_1 r_2} = \lambda_{r_1} \lambda_{r_2}$ is then evident, and it is also clear that $\lambda_1 = \mathrm{id}$. This gives the left R-module structure.

Likewise, the maps

$$R_t : (x, y) \mapsto x \otimes yt, \quad t \in T$$

furnish a family of homomorphisms $(\rho_t : x \otimes y \mapsto x \otimes yt)_{t \in T}$, therefore equip $M \underset{S}{\otimes} N$ with a right T-module structure. It remains to show $\lambda_r \rho_t = \rho_t \lambda_r$ for all r, t, which is also clear: both sides send $x \otimes y$ to $(rx) \otimes (yt)$. □

Note that taking $R = T = \mathbb{Z}$ reverts to the earlier situation.

Lemma 5.5.2. *Let $\varphi : {}_RM_S \to {}_RM'_S$ and $\psi : {}_SN_T \to {}_SN'_T$ be homomorphisms. There exists a unique homomorphism of (R,T)-bimodules satisfying*

$$\begin{aligned} \varphi \otimes \psi : M \underset{S}{\otimes} N &\longrightarrow M' \underset{S}{\otimes} N' \\ x \otimes y &\longmapsto \varphi(x) \otimes \psi(y). \end{aligned}$$

Such homomorphisms behave well under composition: we have $(\varphi \otimes \psi)(\alpha \otimes \beta) = (\varphi\alpha) \otimes (\psi\beta)$ provided that the compositions $\varphi\alpha$ and $\psi\beta$ make sense.

Proof. Use universal property: the composite

$$M \times N \xrightarrow{(\varphi,\psi)} M' \times N' \to M' \underset{S}{\otimes} N'$$

de nes a balanced product, therefore induces a homomorphism $\varphi \otimes \psi : M \underset{S}{\otimes} N \to M' \underset{S}{\otimes} N'$ uniquely characterized by

$$x \otimes y \longmapsto \varphi(x) \otimes \psi(y), \quad x \in M,\ y \in N.$$

From this one can check

$$(\varphi \otimes \psi)(rx \otimes yt) = \varphi(rx) \otimes \psi(yt) = r\varphi(x) \otimes \psi(y)t,$$

thus $\varphi \otimes \psi$ is a homomorphism between bimodules (cf. Lemma 5.5.1). The assertion on compositions can be checked in the same manner. □

Summing up, we have shown that the tensor product furnishes a functor

$$\begin{aligned} \otimes : (R,S)\textbf{-Mod} \times (S,T)\textbf{-Mod} &\longrightarrow (R,T)\textbf{-Mod} \\ (M,N) &\longmapsto M \underset{S}{\otimes} N \quad \text{(on objects)} \\ (\varphi,\psi) &\longmapsto \varphi \otimes \psi \quad \text{(on morphisms)}. \end{aligned}$$

Exercise 5.5.3. Clarify the meaning of direct product $\times$ of categories in the displayed formula.

We remark that the precise construction of tensor products is immaterial here; simply x a choice of $M \times N \to M \underset{S}{\otimes} N$ for all ${}_RM_S, {}_SN_T$, what matters is that $\varphi \otimes \psi$ is pinned down by Lemma 5.5.2.

Lemma 5.5.4 (Unit constraint)**.** *Regard a ring S as an (S,S)-bimodule, then there is a canonical isomorphism*

$$\begin{aligned} M \underset{S}{\otimes} S &\xrightarrow{\sim} M \\ m \otimes s &\mapsto ms \end{aligned}$$

between (R,S)-bimodules, for every ${}_RM_S$. Similarly we have $R \underset{R}{\otimes} M \xrightarrow{\sim} M$ as (R,S)-bimodules.

Here, canonical (sometimes called "functorial") means that the isomorphisms for various M t into a natural transformation $- \underset{S}{\otimes} S \to \mathrm{id}$ between functors. It is called a *constraint* since the identi cation is given as a canonical isomorphism, instead of strict identity =. In practice, however, it is almost safe to treat them as equalities: in general, such an abuse is justi ed by MacLane's Coherence Theorem [17, VII.2].

Proof. The inverse is given by $m \otimes 1 \mapsto m$. The veri cation of the required properties is straightforward. □

Lemma 5.5.5 (Associativity constraint)**.** *There are canonical isomorphisms*

$$\begin{aligned}(M \underset{R}{\otimes} M') \underset{S}{\otimes} M'' &\xrightarrow{\sim} M \underset{R}{\otimes} (M' \underset{S}{\otimes} M'')\\ (x \otimes y) \otimes z &\mapsto x \otimes (y \otimes z),\end{aligned}$$

for all M_R, ${}_RM'_S$ and ${}_SM'$.

The adjective "canonical" has a similar meaning as before. The proof is left to the reader.

Now assume R commutative. By Example 5.3.4, the tensor product $M \underset{R}{\otimes} N$ is de ned for all R-modules M and N, and $M \underset{R}{\otimes} N$ itself is again an R-module by Lemma 5.5.1. Thus it makes sense to talk about commutativity of tensor products.

Lemma 5.5.6 (Commutativity constraint)**.** *Let R be a commutative ring. There are canonical isomorphisms*

$$\begin{aligned}M \underset{R}{\otimes} N &\xrightarrow{\sim} N \underset{R}{\otimes} M\\ x \otimes y &\mapsto y \otimes x\end{aligned}$$

between R-modules, for any R-modules M and N.

Proof. The homomorphism $x \otimes y \mapsto y \otimes x$ stems from the fact that $(x, y) \mapsto y \otimes x$ is a balanced product, thanks to the commutativity of R. Its inverse is simply $y \otimes x \mapsto x \otimes y$. □

5.6 Algebras

Throughout this section, R is a commutative ring. We abbreviate $M \underset{R}{\otimes} N$ as $M \otimes N$ in what follows.

De nition 5.6.1. An (associative, unital) R-algebra is a ring A which is equipped with an R-module structure, such that the multiplication is balanced (i.e. R-linear): we have

$$\begin{aligned}x(ry) &= (xr)y \quad (r \in R,\ x, y \in A)\\ &= (rx)y \quad \text{by the prescription in Example 5.3.4}\\ &= r(xy).\end{aligned}$$

A homomorphism between R-algebras is a ring homomorphism which is also R-linear.

Figure 5.1: Hassler Whitney (1907–1989) is also a keen mountaineer. The picture shows the *Whitney–Gilman Ridge* (YDS: 5.7) in New Hampshire, named after Whitney and his cousin Bradley Gilman who made a famous ascent on August 3, 1929, nowadays considered as a classic route. Source: mountainproject.com

Alternatively, the R-algebra structure of A can be speci ed by giving a ring homomorphism $\eta : R \to A$ with image in the center of A; the corresponding R-module structure on A is $r \cdot a = \eta(r)a$ for all $r \in R$, $a \in A$.

Note that by the universal property of $\otimes$, an R-bilinear multiplication as above amounts to a homomorphism $\mu : A \otimes A \to A$ between R-modules, namely via $\mu(x \otimes y) = xy$. The theory of R-algebras has an alternative axiomatization as follows. We are given an R-module A together with homomorphisms

$$\begin{aligned} \mu : A \otimes A \to A \quad & \text{(multiplication)}, \\ \eta : R \to A \quad & \text{(unit)} \end{aligned}$$

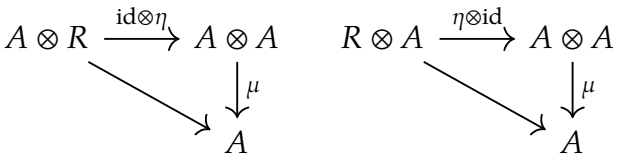
between R-modules, subject to the following conditions.

Associativity The diagram

$$\begin{array}{ccc} (A \otimes A) \otimes A & \xrightarrow{\mu \otimes \mathrm{id}} & A \otimes A \\ {\scriptstyle \mathrm{id} \otimes \mu}\downarrow & & \downarrow{\scriptstyle \mu} \\ A \otimes A & \xrightarrow[\mu]{} & A \end{array} \tag{5.1}$$

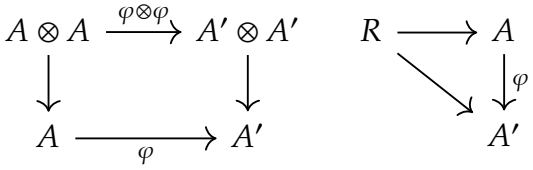
commutes, where we invoked the associativity constraint (Lemma 5.5.5) to identify $(A \otimes A) \otimes A$ with $A \otimes (A \otimes A)$, interpreting $\mu \otimes \mathrm{id}_A$ and $\mathrm{id}_A \otimes \mu$ accordingly.

Units The diagrams

(5.2)


both commute, where the arrows ↘ stand for the unit constraint (Lemma 5.5.4).

Indeed, we have remarked that μ accounts for the multiplication, whereas η prescribes the unit $1_A \in A$ via $1_A = \eta(1_R)$. In the same vein, a homomorphism between R-algebras $\varphi : A \to A'$ is a morphism φ in R-**Mod** making the diagrams

(5.3)


commutative.

What is this paraphrase good for? The axioms above are *arrow-theoretic* — they carry over to categories with a reasonable operation $\otimes$ admitting a "unit" (such as the R for R − **Mod**), called *monoidal categories* or *tensor categories*. For an introduction to these subjects, see [17, VII].

Example 5.6.2. Let $\Bbbk$ be a eld. The ring of $n \times n$-matrices over $\Bbbk$ becomes a $\Bbbk$-algebra under scalar multiplication. More generally, if R is a commutative ring and $\varphi : R \to A$ is a ring homomorphism with $\mathrm{im}(\varphi)$ central in A, then multiplication via φ makes A into an R-algebra.

De nition 5.6.3. Reversal of arrows leads to the notion of *coalgebras*. More precisely, an R-coalgebra is a triple (A, Δ, ϵ) where A is an R-module equipped with homomorphisms $\Delta : A \to A \otimes A$ (comultiplication) and $\epsilon : A \to R$ (counit), such that the reversed versions of (5.1), (5.2) commute. Reversal of (5.3) yields the notion of homomorphisms between coalgebras.

Exercise 5.6.4. Write down the precise conditions to be satis ed by the comultiplication and counit.

De nition 5.6.5. Let A and B be R-algebras. Their tensor product is the R-module $A \otimes B$ equipped with

- ⋆ the multiplication determined by

$$(A \otimes B) \otimes (A \otimes B) \xrightarrow{\sim} (A \otimes A) \otimes (B \otimes B) \xrightarrow{\mu_A \otimes \mu_B} A \otimes B$$

(Lemmas 5.5.5 and 5.5.6 intervene here), or more concretely by

$$(x \otimes y) \cdot (x' \otimes y) = xx' \otimes yy';$$

- ⋆ the unit given by

$$R \xrightarrow{\sim} R \otimes R \xrightarrow{\eta_A \otimes \eta_B} A \otimes B$$

where Lemma 5.5.4 intervene, or more concretely by $1_{A\otimes B} = 1_A \otimes 1_B$.

Exercise 5.6.6. Check that $A \otimes B$ is indeed an R-algebra. Show that the assignment $x \otimes y \mapsto y \otimes x$ induces a canonical isomorphism $A \otimes B \xrightarrow{\sim} B \otimes A$ as R-algebras.

Exercise 5.6.7. De ne the tensor product of coalgebras.

Next, consider a homomorphism $\varphi : R \to S$ between commutative rings. Then S becomes an R-algebra (namely, R acts on S by scalar multiplication via φ). Furthermore, S can be enriched into an (S, R)-bimodule. Hence we obtain the *base change* for modules, which is the functor

$$\begin{aligned} S \underset{R}{\otimes} - : R\textbf{-Mod} &\longrightarrow S\textbf{-Mod} \\ M &\longmapsto S \underset{R}{\otimes} M \\ [f : M \to N] &\longmapsto \mathrm{id}_S \otimes f. \end{aligned}$$

The same can be said for algebras. For any R-algebra A, we have seen that $S \underset{R}{\otimes} A$ is also an R-algebra. It is routine to check that it is actually an S-algebra: the multiplication is S-linear. Hence $S \underset{R}{\otimes} -$ induces a functor $R\textbf{-Alg} \to S\textbf{-Alg}$.

For the next result, rst observe that if A is an R-algebra, then so is its opposite ring A^{op}. Also note that by Example 5.1.4, every ring is canonically a $\mathbb{Z}$-algebra, and vice versa.

Proposition 5.6.8. *Let A and B be rings. The category (A, B)-**Mod** is equivalent to $(A \underset{\mathbb{Z}}{\otimes} B^{op})$-**Mod**: to each (A, B)-bimodule M, the corresponding left $A \otimes B^{op}$-module structure on M is given by*

$$(a \otimes b)m = amb, \quad m \in M,\ a \in A,\ b \in B$$

and vice versa.

Proof. Straightforward. □

Thus the theory of bimodules can be subsumed into that of modules. For example, we may deduce the notion of free bimodules, etc.

LECTURE 6

SIMPLE, SEMISIMPLE AND INDECOMPOSABLE MODULES

Throughout this lecture, we x a ring R (nonzero, unital). By "R-modules" we always mean left R-modules. The composition of homomorphisms is taken in the standard order, namely $fg = f \circ g$. Warning: in the future lectures the opposite notation will be used occasionally.

6.1 Simple and semisimple modules

Simple modules can be conceived as some sort of building blocks in module theory.

De nition 6.1.1. An R-module M is called *simple* if $M \neq 0$ and M has no submodules other than M and $\{0\}$.

Looking for examples? Read on.

- Let $\mathfrak{a}$ be a left ideal of R. The quotient R-module $R/\mathfrak{a}$ is simple if and only if $\mathfrak{a}$ is maximal.
- When R is a division ring, an R-module (= vector space) is simple if and only if it is of dimension one.
- Let $R = M_n(D)$, the ring of $n \times n$-matrices with entries in a division ring D. Consider

$$M := D^n = \left\{ \text{column vectors } \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix} : \ d_1, \ldots, d_n \in D \right\}.$$

It becomes an R-module via matrix multiplication, say $R \times M \ni (A, x) \mapsto Ax \in M$. It is a trivial exercise (try it out!) in linear algebra to show that for $m \in M \setminus \{0\}$ we have $Rm = M$. Hence M is simple. Note: to get a similar R-module, consider row vectors instead.

Theorem 6.1.2 (Schur's Lemma)**.** *Let M_1, M_2 be simple R-modules and $\varphi : M_1 \to M_2$ is a homomorphism. Then either $\varphi = 0$ or φ is an isomorphism. In particular, the endomorphism ring of a simple R-module is a division ring.*

Proof. If $\ker(\varphi) = M_1$ then $\varphi = 0$, otherwise $\ker(\varphi) = 0$ and in this case $\mathrm{im}(\varphi) \neq \{0\}$, thus $\mathrm{im}(\varphi) = M_2$ and φ is bijective. □

Homomorphisms between direct sums of simple modules can be described in terms of matrices. Let us illustrate the idea by the case of endomorphisms.

Corollary 6.1.3. *Let $M = M_1^{\oplus n_1} \oplus \cdots \oplus M_r^{\oplus n_r}$ where $M_1, \ldots, M_r$ are distinct (up to $\simeq$) simple R-modules. Put $D_i := \mathrm{End}_R(M_i)$ for all i, which is a division ring by Schur's Lemma. There is a ring isomorphism*

$$\begin{aligned} \mathrm{End}_R(M) &\xrightarrow{\sim} \prod_{i=1}^{r} M_{n_i}(D_i) \\ \varphi &\longmapsto \left[\left(\alpha_{jk}^{(i)} \right)_{j,k} \in M_{n_i}(D_i) \right]_{1 \leq i \leq r} \end{aligned}$$

where $\alpha_{j,k}^{(i)}$ denotes the homomorphism

$$M_i \xrightarrow{\text{as the k-th summand}} M_i^{\oplus n_i} \xrightarrow{\varphi} M_i^{\oplus n_i} \xrightarrow{\text{project to the j-th summand}} M_i;$$

note that $\varphi(M_i^{\oplus n_i})$ must land in $M_i^{\oplus n_i}$ by Schur's Lemma.

Proof. Indeed, this is completely analogue to the case where R is a field, which is just the classical theory of matrices. □

For the next result, recall first that we have defined the sum $\sum_i M_i$ of a family of submodules M_i inside some M. The homomorphism $\bigoplus_i M_i \to M$ induced from the universal property of $\bigoplus$ is an isomorphism if and only if (i) $\sum_i M_i = M$, and (ii) $M_i \cap \sum_{j \neq i} M_j = \{0\}$ for all i. Condition (ii) is equivalent to that

$$\left[\sum_i x_i = 0,\ x_i \in M_i \right] \iff \forall i,\ x_i = 0;$$

in other words, there are no linear relations among the summands M_i. In this circumstance, the "internal sum" $\sum_i M_i$ and the "external direct sum" $\bigoplus_i M_i$ may be naturally identified.

Definition-Proposition 6.1.4 (Semisimple modules)**.** The following are equivalent for an R-module M.

(i) M is a sum of simple submodules.

(ii) M is a direct sum of simple submodules.

(iii) For every submodule $M' \subset M$, there exists another submodule $M'' \subset M$ such that $M = M' \oplus M''$.

Under any one of these conditions, we call M a *semisimple* R-module.

Before undertaking the proof, let us record a simple observation.

Lemma 6.1.5. *The property (iii) above passes to submodules and quotients of M.*

Proof. Assume (iii) holds for M and consider a submodule M' of M. Let M'_0 be any submodule of M' and write $M = M'_0 \oplus N$ for some N. Since $M'_0 \subset M'$, it follows that

$$M' = M'_0 \oplus (N \cap M').$$

Hence M' also satis es (iii). Since every quotient of M is isomorphic to some submodule of M, by (iii), the case of quotients follows. □

Proof of De nition-Proposition 6.1.4. For (i) $\implies$ (ii), suppose that $M = \sum_{i\in I} M_i$ in which each M_i is simple. Set

$$\mathcal{J} := \left\{ J \subset I : \sum_{j\in J} M_i = \bigoplus_{j\in J} M_i \right\}.$$

It is nonempty: every singleton in I belongs to $\mathcal{J}$. We contend that every totally ordered subset (=chain) in the partially ordered set $(\mathcal{J}, \subset)$ has upper bound: indeed, if $\mathcal{J}'$ is a chain, then $J := \bigcup_{J'\in\mathcal{J}'} J'$ belongs to $\mathcal{J}$ — the condition $M_i \cap \sum_{j\neq i} M_j = \{0\}$ for the directness of $\sum_{j\in J} M_j$ may be checked in the nite subsets of J, each lies in some $J' \in \mathcal{J}'$. Hence there exists a maximal element $J \in \mathcal{J}$.

If $\sum_{i\in J} M_i = \bigoplus_{i\in J} M_i \neq M$, then $M_h \not\subset \sum_{i\in J} M_i$ for some $h \in I$. Since M_h is simple, that would imply $M_h \cap \sum_{i\in J} M_i = \{0\}$ from which we infer $J \sqcup \{h\} \in \mathcal{J}$, a contradiction.

For (ii) $\implies$ (iii), let $M' \subset M$ and assume $M = \bigoplus_{i\in I} M_i$. Set

$$\mathcal{J} := \left\{ J \subset I : M' + \bigoplus_{j\in J} M_j \text{ is direct} \right\}.$$

As before, Zorn's Lemma furnishes a maximal element $J \in \mathcal{J}$, and we contend that $M'' := \bigoplus_{j\in J} M_j$ satis es $M = M' \oplus M''$. If not, there will exist $h \in I$ with $M_h \not\subset M' \oplus M''$ and one may argue that $J \sqcup \{h\} \in \mathcal{J}$ as before.

For (iii) $\implies$ (i), we let M_0 be the sum of all simple submodules of M and contend that $M_0 = M$. There exists $M' \subset M$ with $M = M' \oplus M_0$. We must show that $M' = \{0\}$. If we can show that

every nonzero submodule of M contains a simple submodule,

then M' will contain a simple submodule which is necessarily contained in M_0, contradiction. To prove the assertion above, one reduces immediately to the case where the submodule in question takes the form $M' = Rv$ for some $v \in M$. There is an isomorphism

$$\begin{aligned} R/\mathfrak{a} &\longrightarrow Rv = M' \\ r + \mathfrak{a} &\longmapsto rv \end{aligned}$$

of R-modules, where $\mathfrak{a} := \ker[r \mapsto rv]$ is a left ideal of R.

By Zorn's Lemma, there exists a maximal left ideal $\mathfrak{m} \supset \mathfrak{a}$. Let $M'' := \mathfrak{m}v \hookrightarrow Rv = M'$. Condition (iii) holds true for M' by virtue of Lemma 6.1.5, hence we may write $M' = M'' \oplus N$ for some submodule N. It is the required simple submodule since

$$N \simeq M'/M'' \simeq \frac{R/\mathfrak{a}}{\mathfrak{m}/\mathfrak{a}} = R/\mathfrak{m}.$$

□

Exercise 6.1.6. Justify the existence of the maximal left ideal $\mathfrak{m}$ containing $\mathfrak{a}$ used in the proof.

Corollary 6.1.7. *Submodules and quotients of a semisimple R-module M are still semisimple.*

Proof. Done by Lemma 6.1.5. □

6.2 Schreier's re nement theorem

This section paves the way to the proof of the Jordan-Hölder theorem for modules. We shall concentrate on the case of *groups*, which is actually harder and rarely covered in our undergraduate curricula. The concept of groups with operators in [12] provides a unifying framework; we do not pursue that approach.

Let G be a group, whose binary operation we write as multiplication. Write $N \lhd G$ to denote that N is a normal subgroup of G. A *normal series* (also known as subnormal series...) of G is a nite chain of subgroups

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_{s+1} = \{1\}$$

verifying

$$\forall 0 \leq i \leq s,\ G_{i+1} \lhd G_i.$$

The corresponding set of *subquotients* is

$$\{G_0/G_1, G_1/G_2, \ldots, G_s/G_{s+1}\}$$

as a set with multiplicities, meaning that repetitions are allowed in the $\{\cdots\}$. Two normal series $(G_i)_{i=0}^s$, $(H_i)_{i=0}^t$ of G are called *equivalent* if $s = t$ and their subquotients are isomorphic up to permutation — surely, multiplicities are taken into account.

By a *re nement* of a normal series $(G_i)_i$, we mean a new normal series obtained by successive insertions of the form

$$[\cdots \supset G_i \supset G_{i+1} \supset \cdots] \longrightarrow [\cdots \supset G_i \supset H \supset G_{i+1} \supset \cdots]$$

for some $H \lhd G_i$. If, at each step, the inserted term H equals either G_i or G_{i+1}, the resulting re nement is called *trivial*.

Theorem 6.2.1 (Schreier)**.** *Let G be a group. Any two normal series of G have re nements which are equivalent to each other.*

We employ the so-called Zassenhaus Lemma or Butterfly Lemma to prove the refinement theorem. Recall that given two subgroups $H, K \subset G$, we put $HK = \{hk : h \in H,\ k \in K\}$ which is a subset of G; it is actually a subgroup when H normalizes K, that is, when H is contained in the *normalizer*

$$N_G(K) := \{g \in G : gKg^{-1} \subset K\}$$

of K in G.

Lemma 6.2.2 (Zassenhaus)**.** *Fix a group G, consider its subgroups U, V and their normal subgroups $u \lhd U$, $v \lhd V$. We have*

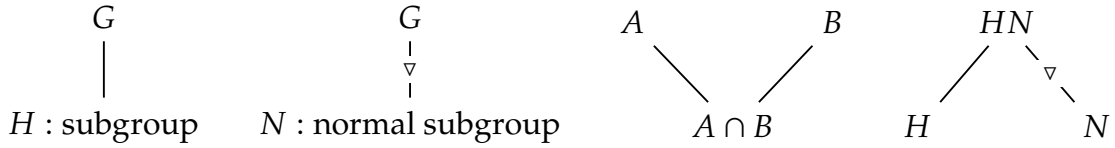
$$u(U \cap v) \lhd u(U \cap V),$$
$$(u \cap V)v \lhd (U \cap V)v,$$

each term being a subgroup of G. Moreover, there is a natural isomorphism

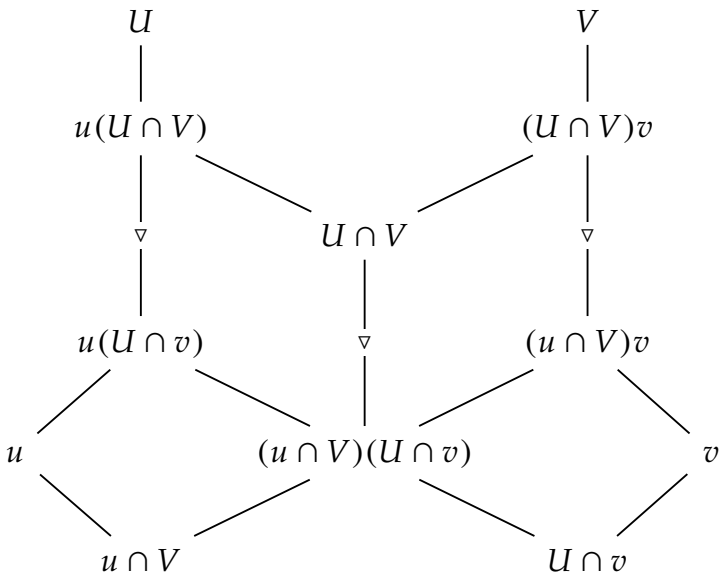
$$\frac{u(U \cap V)}{u(U \cap v)} \simeq \frac{(U \cap V)v}{(u \cap V)v}$$

of groups.

Proof. Visualize the relations among various subgroups by the following rules



where we assume that H normalizes N. Claim: we have the diagram



taken from [16, p.21]; it resembles some Jedi Starfighter rather than a butterfly.

First, observe that $U \cap V \subset N_G(u) \cap N_G(v)$, etc. Hence the terms $u(U \cap V)$, etc. in the diagram are subgroups. The first rule of our diagrams is then obvious. It is routine to check that

$$\begin{aligned} u(U \cap v) \cap (U \cap V) &= (u \cap V)(U \cap v) = (U \cap V) \cap (u \cap V)v, \\ u \cap (u \cap V)(U \cap v) &= u \cap V, \\ (u \cap V)(U \cap v) \cap v &= U \cap v. \end{aligned}$$

Thus the third rule for our diagram (concerning intersections) also holds true. Similarly one verifies the fourth rule. As for the second rule concerning normal subgroups, one infers from $v \lhd V$ that $U \cap v \lhd U \cap V$, therefore $u(U \cap v) \lhd u(U \cap V)$; in the same manner we get $(u \cap V)v \lhd (U \cap V)v$, Taking intersection yields $(u \cap V)(U \cap v) \lhd U \cap V$. The claim is now established.

Please gaze at the two parallelograms in our diagram. The familiar isomorphism theorems in group theory give isomorphisms

$$\begin{array}{ccc} \dfrac{u(U \cap V)}{u(U \cap v)} & & \dfrac{(U \cap V)v}{(u \cap V)v} \\ & \searrow^{\simeq} \quad \swarrow_{\simeq} & \\ & \dfrac{U \cap V}{(u \cap V)(U \cap v)} & \end{array}$$

and this completes the proof. □

Proof of Theorem 6.2.1. Consider two normal series $(G_i)_{i=0}^s$ and $(H_j)_{j=0}^t$. For each $0 \le i \le s$, $0 \le j \le t$, we define

$$\begin{aligned} G_{i,j} &:= G_{i+1}(H_j \cap G_i), \\ H_{j,i} &:= (G_i \cap H_j)H_{j+1}. \end{aligned}$$

Look at $G_{i,j}$ first. One may check that $G_{i,j}$ is a subgroup, $G_{i,j+1} \lhd G_{i,j}$ and that

$$G_{i,0} = G_{i+1}(G \cap G_i) = G_i, \quad G_{i,s+1} = G_{i+1}.$$

In fact, these assertions are implied by Lemma 6.2.2 (see below). Hence we obtain a refinement of $(G_i)_{i=0}^s$:

$$\mathcal{G} := [\cdots \supset G_i = G_{i,0} \supset G_{i,1} \supset \cdots G_{i,s} \supset G_{i,s+1} = G_{i+1} \supset \cdots].$$

Similarly, $H_{j,i}$ gives a refinement of $(H_j)_{j=0}^t$, which we denote as $\mathcal{H}$. For every given pair (i, j), take $u := G_{i+1}$, $U := G_i$ and $v := H_{j+1}$ and $V := H_j$ in Lemma 6.2.2 to deduce that

$$\frac{G_{i,j}}{G_{i,j+1}} = \frac{u(U \cap V)}{u(U \cap v)} \simeq \frac{(U \cap V)v}{(u \cap V)v} = \frac{H_{j,i}}{H_{j,i+1}}.$$

When (i, j) varies, each subquotient of $\mathcal{G}$ (resp. $\mathcal{H}$) appears exactly once on the left (resp. right) hand side. Hence $\mathcal{G}$ is equivalent to $\mathcal{H}$ as asserted. □

6.3 Jordan-Hölder theorem

We continue to work with groups.

De nition 6.3.1. Assume $G \neq \{1\}$. A *composition series* of G is a normal series $(G_i)_{i=0}^{s}$ with $G_i \supsetneq G_{i+1}$ and G_i/G_{i+1} simple (i.e. has no normal subgroups except $\{1\}$ and G_i/G_{i+1}). The subquotients of a composition series are called the *composition factors* or *Jordan-Hölder factors* of G, denoted by $\mathrm{JH}(G)$ as a set with multiplicities.

Note that not every G admits a composition series (eg. the additive group $\mathbb{Z}$). The use of de nite article "the" for $\mathrm{JH}(G)$ is justi ed by the next result.

Theorem 6.3.2. *Let G be a group admitting composition series. Then any two composition series of G are equivalent.*

Proof. Observe that a composition series has no non-trivial re nement and apply Theorem 6.2.1. □

Exercise 6.3.3. Show that the additive groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$ have the same Jordan-Hölder factors, namely $\{\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}\}$, but they are not isomorphic.

Now switch to the category of R-modules. In all the de nitions and arguments above, we

- ⋆ change groups into R-modules;
- ⋆ change normal subgroups into submodules — this greatly simpli es the arguments;
- ⋆ the normal series are now replaced by a descending chain $M = M_0 \supset \cdots \supset M_{s+1} = \{0\}$ of submodules, often called a *ltration* of M;
- ⋆ change the product of two subgroups HK into the sum of submodules $M + N$;
- ⋆ the simple modules now replace the rôle of simple groups in the de nition of composition series of an R-module.

The isomorphisms in Lemma 6.2.2 and Theorem 6.2.1 now arise from appropriate isomorphism theorems in module theory. We omit the details.

Lemma 6.3.4. *An R-module $M \neq 0$ admits a composition series if and only if M is both noetherian and artinian.*

Such modules are also said to be of nite length.

Proof. Evidently, any simple module is both noetherian and artinian. Assume that $M = M_0 \supset \cdots \supset M_{s+1} = \{0\}$ is a composition series of M. Arguing recursively on the short exact sequences

$$0 \to M_{i+1} \to M_i \to \overbrace{M_i/M_{i+1}}^{\text{simple}} \to 0$$

we see that each M_i is noetherian and artinian, thus so is $M = M_0$.

Conversely, assume M both noetherian and artinian. Let $\mathcal{S}$ be the set of proper submodules of M. Put $M_0 := M$. Since M_0 is noetherian, there exists a maximal element $M_1 \in \mathcal{S}$ with respect to inclusion; this is equivalent to the simplicity of M_0/M_1. Since M_1 inherits the noetherian property, the same procedure can be iterated whenever $M_1 \neq \{0\}$ and we deduce a descending chain

$$M = M_0 \supsetneq M_1 \supsetneq \cdots$$

of R-modules, in which each M_i/M_{i+1} is simple. Since M is artinian, this procedure must terminate, i.e. eventually $M_{s+1} = \{0\}$ for some $s \geq 0$. Thus we obtain a composition series of M. □

Retain the notation $\mathrm{JH}(M)$ for the set with multiplicities of Jordan-Hölder factors of M.

Exercise 6.3.5. Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence such that M has a composition series. Show that $\mathrm{JH}(M) = \mathrm{JH}(M') \cup \mathrm{JH}(M'')$ (with multiplicities).

It is of utmost importance in algebra to know the manner how a module is assembled from smaller pieces via exact sequences. In view of the preceding result, Jordan-Hölder factors are of very limited use for this purpose!

Exercise 6.3.6. Describe the Jordan-Hölder factors of finite abelian groups in terms of their classification theorem.

Remark 6.3.7. The notions of simple objects, Jordan-Hölder factors, etc. can be formulated in a broader categorical context (eg. for sheaves on suitable spaces).

6.4 Direct sum decompositions

Throughout this section, M stands for a nonzero R-module, so that $\mathrm{End}_R(M)$ is a nonzero ring.

We have discussed the decompositions of an R-module M into the "internal direct sum" $\bigoplus_{i\in I} M_i$ of a family of submodules $(M_i)_{i\in I}$: recall that this means the natural homomorphism

$$\begin{aligned} \bigoplus_{i\in I} M_i &\longrightarrow \sum_{i\in I} M_i \\ (x_i)_{i\in I} &\longmapsto \sum_{i\in I} x_i \end{aligned}$$

is an isomorphism. This admits a ring-theoretic interpretation.

Definition 6.4.1. Let S be a ring. An element $s \in S$ is called an *idempotent* if $s^2 = s$. In this case, $1 - s$ is also an idempotent since $(1-s)^2 = 1 - 2s + s^2 = 1 - s$, and we have $s(1-s) = 0$.

To a decomposition $M = \bigoplus_{i\in I} M_i$ as above, we associate the endomorphism

$$\begin{aligned} e_i : M &\longrightarrow M \\ \sum_{j\in I} x_j &\longmapsto x_i \end{aligned}$$

in $\mathrm{End}_R(M)$, for each $i \in I$. The following conditions are then satis ed:

(i) the sum (possibly in nite) $\sum_{i\in I} e_i$ makes sense in $\mathrm{End}_R(M)$, i.e. for all x we have $e_i(x) = 0$ for all but nitely many $i \in I$;

(ii) furthermore, $\sum_{i\in I} e_i$ equals the identity endomorphism 1 in $\mathrm{End}_R(M)$;

(iii) e_i is an idempotent for each i;

(iv) $e_i e_j = 0$ if $i \neq j$.

Conversely, given a family of idempotents $(e_i)_{i\in I}$ with the conditions above, we set

$$M_i := \mathrm{im}(e_i) \subset M, \quad i \in I.$$

Then $M = \bigoplus_{i\in I} M_i$. Indeed, (i) and (ii) imply $M = \sum_{i\in I} M_i$; if $x = \sum_i x_i$ with $x_i \in M_i$, then (iii) and (iv) imply that x_i is uniquely determined by $x_i = e_i(x)$. The following result is now clear.

Proposition 6.4.2. *Fix a set I of indexes. The recipe above furnishes a bijection between*
- ⋆ *families of submodules $(M_i)_{i\in I}$ with $M = \bigoplus_{i\in I} M_i$, and*
- ⋆ *families of idempotents of $\mathrm{End}_R(M)$ satisfying (i)–(iv) above.*

A direct summand M_i equals M (resp. 0) if and only if $e_i = 1$ (resp. $e_i = 0$).

De nition 6.4.3. An R-module M is called *decomposable* if there exists a decomposition $M = M_1 \oplus M_2$ with M_1, M_2 both nonzero; otherwise we say M is *indecomposable*.

Example 6.4.4. The $\mathbb{Z}$-module $\mathbb{Z}/4\mathbb{Z}$ is indecomposable but not simple.

Proposition 6.4.5. *An R-module M is indecomposable if and only if the only idempotents in $\mathrm{End}_R(M)$ are 0 and 1.*

Proof. Decompositions $M = M_1 \oplus M_2$ correspond to pairs of idempotents of the form $\{e, 1 - e\}$. □

The so-called *Fitting decomposition* below will play a crucial rôle. Recall that an element a in a ring is called *nilpotent* if $a^N = 0$ for some $N \in \mathbb{Z}_{\geq 1}$.

Lemma 6.4.6 (Fitting)**.** *Let M be an R-module, $M \neq 0$, which is both noetherian and artinian. For every $u \in \mathrm{End}_R(M)$, there exists a canonical decomposition*

$$M = \mathrm{im}(u^\infty) \oplus \ker(u^\infty)$$

such that each summand is u-stable, and
- ⋆ *$u|\mathrm{im}(u^\infty)$ is an isomorphism,*
- ⋆ *$u|\ker(u^\infty)$ is nilpotent.*

Proof. Consider the chains

$$\operatorname{im}(u) \supset \operatorname{im}(u^2) \supset \operatorname{im}(u^3) \supset \cdots,$$
$$\ker(u) \subset \ker(u^2) \subset \ker(u^3) \subset \cdots.$$

By our hypothesis, they stabilize to submodules $\operatorname{im}(u^\infty)$ and $\ker(u^\infty)$, respectively.

Let us show $\operatorname{im}(u^\infty) \cap \ker(u^\infty) = 0$. Take $n \gg 0$ so that $\ker(u^n) = \ker(u^\infty)$ and $\operatorname{im}(u^n) = \operatorname{im}(u^\infty)$. Write $x \in \operatorname{im}(u^\infty)$ as $x = u^n(y_n)$ for some $y_n \in M$. If $x \in \ker(u^n) = \ker(u^\infty)$, then $u^n(x) = u^{2n}(y_n) = 0$, so $y_n \in \ker(u^{2n}) = \ker(u^\infty) = \ker(u^n)$, thus $x = 0$.

Next, retain the assumption that $n \gg 0$ so that everything stabilizes at n. Given $x \in M$, choose $y \in M$ with $u^n(x) = u^{2n}(y)$ — this is always possible. Then

$$x = \underbrace{x - u^n(y)}_{\in \ker(u^n)} + u^n(y),$$

from which we conclude $M = \operatorname{im}(u^\infty) + \ker(u^\infty)$. The direct sum decomposition follows.

Since $\operatorname{im}(u^\infty) \cap \ker(u) \subset \operatorname{im}(u^\infty) \cap \ker(u^\infty) = 0$, we have $u|\operatorname{im}(u^\infty)$ injective, whilst $u|\operatorname{im}(u^\infty)$ is surjective by de nition. Hence $u|\operatorname{im}(u^\infty)$ is an isomorphism. The nilpotency of $u|\ker(u^\infty)$ is evident. □

6.5 Krull-Remak-Schmidt theorem

Our objective is to address the uniqueness of the direct sum decompositions into indecomposables, under certain niteness conditions. The history of such results can be traced back to Azumaya (1950), Krull (1925), Schmidt (1913), Remak (1911) and Wedderburn (1909).

De nition 6.5.1. Call a ring S *local* if $S \setminus S^\times$ is a two-sided ideal of S.

Exercise 6.5.2. Show that a commutative ring R is local if and only if there is a unique maximal ideal $\mathfrak{m}$ of R; in this case we have $\mathfrak{m} = R \setminus R^\times$.

Proposition 6.5.3. *Let M be an indecomposable R-module which is artinian and noetherian. Then*

(i) every $f \in \operatorname{End}_R(M)$ is either nilpotent or invertible,

(ii) $\operatorname{End}_R(M)$ is local in the sense above.

Proof. To prove (i), it su ces to apply Lemma 6.4.6 to f. The assertion (ii) amounts to showing that the nilpotent elements form a two-sided ideal of $\operatorname{End}_R(M)$.

Let u be nilpotent, $u \neq 0$ and $v \in \operatorname{End}_R(M)$, we claim that uv and vu are both non-invertible. Choose $n \in \mathbb{Z}_{\geq 0}$ such that $u^n \neq 0$, $u^{n+1} = 0$. The endomorphism uv (resp. vu) cannot be invertible as $u^n(uv) = 0$ (resp. $(vu)u^n = 0$). The claim follows.

It remains to show that $u_1 + u_2$ is non-invertible when u_1, u_2 are both nilpotent. If not, put

$$v_i := u_i(u_1 + u_2)^{-1}, \quad i = 1, 2$$

so that $v_1 + v_2 = 1$. By the previous paragraph v_1 and v_2 are both nilpotent, thus $v_1 = 1 - v_2$ can be inverted via

$$(1 - v_2)^{-1} = 1 + v_2 + v_2^2 + v_2^3 + \cdots \quad (\text{ nite sum!})$$

which contradicts the non-invertibility of v_1. We conclude that the nilpotent elements in $\mathrm{End}_R(M)$ form a two-sided ideal. □

Lemma 6.5.4. *Let M, N be R-modules. Assume $M \neq 0$ and N indecomposable. If $u \in \mathrm{Hom}_R(M,N)$, $v \in \mathrm{Hom}_R(N,M)$ are such that $vu \in \mathrm{End}_R(M)$ is invertible, then u, v are both isomorphisms.*

Proof. Set $e = u(vu)^{-1}v \in \mathrm{End}_R(N)$. We have

$$e^2 = u(vu)^{-1}vu(vu)^{-1}v = u(vu)^{-1}v = e,$$

i.e. e is an idempotent. Since N is indecomposable, either $e = 1$ or $e = 0$. On the other hand,

$$(vu)^{-1}veu = (vu)^{-1}vu(vu)^{-1}vu = 1 \in \mathrm{End}_R(M)$$

thus we must have $e = 1$. Therefore u has a right inverse $(vu)^{-1}v$. Since u also has a left inverse $(vu)^{-1}v$, we conclude that u is an isomorphism. Consequently $v = (vu)u^{-1}$ is an isomorphism as well. □

Theorem 6.5.5 (Krull-Remak-Schmidt)**.** *Let $M \neq 0$ be an R-module that is noetherian and artinian. There exists a decomposition*

$$M = M_1 \oplus \cdots \oplus M_r, \quad r \in \mathbb{Z}_{\geq 1}$$

into indecomposable submodules. Moreover, the integer r is unique and the indecomposable summands M_i are unique up to isomorphisms and permutations.

Proof. Firstly, we let $\ell(M) \in \mathbb{Z}_{\geq 1}$ denote the cardinality of $\mathrm{JH}(M)$, taking multiplicities into account; this is well-de ned by Lemma 6.3.4. If $M = M_1 \oplus M_2$ with $M_1, M_2 \neq 0$, then $\ell(M_1), \ell(M_2) < \ell(M)$. By induction on $\ell(M)$, we derive the existence of a decomposition into indecomposables.

Suppose $M = M_1 \oplus \cdots \oplus M_r$ and $M = N_1 \oplus \cdots \oplus N_s$ are two decompositions into indecomposables. We shall argue by induction on $\max\{r,s\}$. Assume $s \geq r$. Denote the idempotents furnished by Proposition 6.4.2 as

$$e_i : M \twoheadrightarrow M_i \hookrightarrow M,$$
$$u_j : M \twoheadrightarrow N_j \hookrightarrow M,$$

respectively. We contend that upon a permutation of the indexes, we have $M_1 \simeq N_1$.

Set $v_j := e_1 u_j$ and $w_j := u_j e_1$ for $j = 1, \ldots, s$. We have $\mathrm{im}(v_j) \subset M_1$ and $\mathrm{im}(w_j) \subset N_j$. Moreover,

$$\sum_{j=1}^{s} v_j w_j = \sum_{j=1}^{s} e_1 u_j u_j e_1 = e_1 \left(\sum_{j=1}^{s} u_j \right) e_1 = e_1^2 = e_1.$$

Note that $e_1|_{M_1} = \mathrm{id}_{M_1}$. Upon restricting the displayed formula to M_1, Proposition 6.5.3 implies that $(v_j w_j)|_{M_1} \in \mathrm{End}_R(M_1)$ is invertible for some $1 \leq j \leq s$; it may even be arranged that $j = 1$ upon renumbering the indexes. Therefore, Lemma 6.5.4 implies that $v_1|_{N_1} : N_1 \to M_1$ and $w_1|_{M_1} : M_1 \to N_1$ are both isomorphisms.

The next step is to "cancel out" M_1 and N_1. If $M = N_1$, then $r = s = 1$ and we are done. Assume $s > 1$. Notice that $v_1|_{N_1} = e_1|_{N_1} : N_1 \to M_1$ is an isomorphism, which implies that

$$N_1 \cap \sum_{i>1} M_i = N_1 \cap \ker(e_1) = 0,$$

and

$$M = N_1 + \ker(e_1) = N_1 + \sum_{i>1} M_i.$$

Hence $M = N_1 \oplus \bigoplus_{i>1} M_i$, from which we see M/N_1 is isomorphic to both $\bigoplus_{1<i\leq r} M_i$ and $\bigoplus_{1<j\leq s} N_j$, and we can argue by induction. □

We refer to [15, §19] for further rami cations and examples of the Krull-Remak-Schmidt theorem.

LECTURE 7

SEMISIMPLE RINGS

The following convention is particularly useful in the study of modules. Let M, N be left R-modules. We can let the elements of $\mathrm{Hom}(M, N)$ acts on M on the right, that is, $\varphi(m) = m\varphi$ for $m \in M$ and $\varphi \in \mathrm{Hom}(M, N)$. The R-linearity of homomorphisms then takes the elegant form

$$r(m\varphi) = (rm)\varphi,\ r \in R.$$

The same applies, of course, to the endomorphism ring $\mathrm{End}(M)$. In this setting the multiplication in $\mathrm{End}(M)$ satis es $m(\varphi\psi) = (m\varphi)\psi$; it is opposite to the usual composition $\varphi \circ \psi$. Similarly, for a right R-module M the endomorphism ring $\mathrm{End}(M)$ acts on M on the left. In any case, the convention will be clear according to the context.

The ideals in a ring are to be multiplied in the following manner: let $\mathfrak{a}$ and $\mathfrak{b}$ be left ideals, de ne $\mathfrak{ab}$ to be the subset consisting of nite sums $\sum_i x_i y_i$, where $x_i \in \mathfrak{a}$ and $y_i \in \mathfrak{b}$. Then $\mathfrak{ab}$ is still a left ideal and the multiplication so de ned is associative. The same rule applies to right ideals and two-sided ideals as well.

7.1 Wedderburn-Artin theory for semisimple rings

Our main references are [12, 16, 15].

De nition 7.1.1. A ring R is called simple if it has no two-sided ideals except $\{0\}$ and R itself.

For example, division rings are simple. Before discussing the structure theory of simple rings, let us see some examples rst.

Lemma 7.1.2. *Let R be a ring and $n \in \mathbb{Z}_{\geq 1}$. For any two-sided ideal $\mathfrak{a}$ of R, the set $M_n(\mathfrak{a})$ is a two-sided ideal of $M_n(R)$. Moreover, $\mathfrak{a} \mapsto M_n(\mathfrak{a})$ sets up a bijection*

$$\{\textit{two-sided ideals of } R\} \xrightarrow{\sim} \{\textit{two-sided ideals of } M_n(R)\}.$$

Proof. The rst assertion and the injectivity of $\mathfrak{a} \mapsto M_n(\mathfrak{a})$ are evident. As to the surjectivity, let I be a two-sided ideal of $M_n(R)$. Set

$$\mathfrak{a} := \left\{ r \in R : \exists (x_{ij}) \in I,\ r = x_{11} \right\}.$$

One checks that $\mathfrak{a}$ is a two-sided ideal of R. For every $1 \leq i, j \leq n$, let $E_{i,j}$ denote the matrix with 1 at the (i, j)-entry, and zero elsewhere. Hence for every $X = (x_{jk}) \in M_n(R)$, we have

$$E_{i,j}XE_{k,l} = x_{jk}E_{i,l}.$$

It follows that for $X \in I$, we have $x_{jk}E_{11} = E_{1j}XE_{k1} \in I$, thereby $x_{jk} \in \mathfrak{a}$ for every index (j, k). Thus $I \subset M_n(\mathfrak{a})$. Conversely, let $X \in M_n(\mathfrak{a})$ and x an index (il); by assumption there exists $Y \in I$ with $y_{11} = x_{il}$, hence

$$x_{il}E_{il} = y_{11}E_{il} = E_{i1}YE_{1l} \in I.$$

Hence $I = M_n(\mathfrak{a})$, proving the asserted surjectivity. □

Note that the upshot of the proof is to move the matrix entries around by row and column operations.

Corollary 7.1.3. *Let D be a division ring, then $M_n(D)$ is a simple ring.*

De nition 7.1.4. A ring R is called left (resp. right) semisimple if R is semisimple as a left (resp. right) R-module.

This is a temporary notion: the left and right versions will be shown to be equivalent in the Corollary 7.1.13, as a consequence of the Wedderburn-Artin theorem. We shall simply say that R is a *semisimple ring* afterwards.

Remark 7.1.5. Simple rings are not necessarily semisimple. Cf. Proposition 7.2.2.

De nition 7.1.6. A minimal left (resp. right) ideal is a *nonzero* left (resp. right) ideal containing no proper nonzero left (resp. right) ideals.

Lemma 7.1.7. *Let R be a left (resp. right) semisimple ring, then R is a left (resp. right) artinian and noetherian R-module. Equivalently, R has composition series as a left (resp. right) R-module.*

Proof. It su ces to consider the left case. By semisimplicity, write $R = \sum_{i \in I} \mathfrak{a}_i$ as a direct sum of minimal left ideals, where I is some indexing set. There exists a nite subset $I_0 \subset I$ such that $1 \in \bigoplus_{i \in I_0} \mathfrak{a}_i$. Since $R = R \cdot 1$, we conclude that $I = I_0$ is nite. The left R-module R has a composition series, hence is both artinian and noetherian. □

As before, we begin by looking at the case of matrix algebras closely.

Proposition 7.1.8. *Let D be a division ring, $R := M_n(D)$. Then*

1. *R is a simple and left semisimple ring;*
2. *there exists a unique simple left R-module V up to isomorphism; moreover, R acts faithfully on V (that is, $R \hookrightarrow \mathrm{End}_{\mathrm{ab.grp}}(V)$) and $R \simeq V^{\oplus n}$ as left R-modules;*
3. *we have $\mathrm{End}({}_R V) \simeq D$ as rings.*

Needless to say (we do say it anyway), the same holds if "left" is replaced by "right" everywhere.

Proof. We have seen the simplicity of R. Moreover, R is a D-vector space of dimension n^2, hence R is left (resp. right) artinian and noetherian. Now let V be D^n (identified to the column matrices) on which $R = M_n(D)$ acts by matrix multiplication on the left, and D acts on the right by scalar multiplication. Observe that V is a (R, D)-bimodule.

By linear algebra over D, one readily checks that

- ⋆ V is a simple, faithful left R-module;
- ⋆ as a left R-module, we have $R = \bigoplus_{i=1}^{n} V_i \simeq V^{\oplus n}$, where V_i is the R-submodule consisting of the matrices whose entries vanish outside the i-th column.

Every simple left R-module is cyclic, that is, of the form $R/\mathfrak{m}$ with $\mathfrak{m}$ a maximal left ideal of R. Such an R-module must appear in the composition series of ${}_R R$. By the Jordan-Hölder theorem and the preceding results, the only candidate is V. Now we have proved parts (1) and (2) of the proposition.

To prove (3), define the homomorphism of rings

$$\begin{aligned} \Delta : D &\longrightarrow \mathrm{End}({}_R V) \\ d &\longmapsto [v \mapsto vd]. \end{aligned}$$

It remains to show that Δ is an isomorphism. It is clear that V is clear as a right D-module, hence Δ is injective. Let $f \in \mathrm{End}({}_R V)$ and write

$$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} f = \begin{pmatrix} d \\ * \\ \vdots \\ * \end{pmatrix}, \quad d \in D.$$

We leave it to the reader to check that

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} f = \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ \vdots & & \vdots & \\ a_n & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} d \\ \vdots \\ \vdots \end{pmatrix} = \begin{pmatrix} a_1 d \\ \vdots \\ a_n d \end{pmatrix} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \Delta(d)$$

for all $a_1, \ldots a_n \in D$. This amounts to $f = \Delta(d)$, whence the surjectivity of Δ. □

Lemma 7.1.9. *Let $R_1, \ldots, R_m$ be left semisimple rings, then so is $R = R_1 \times \cdots \times R_m$.*

Proof. For every $1 \leq i \leq m$, the left semisimplicity of R_i amounts to a decomposition $R_i = \bigoplus_j \mathfrak{a}_{ij}$ into minimal left ideals; we view each R_i as a two-sided ideal of R. Hence $R = \bigoplus_{i,j} \mathfrak{a}_{i,j}$ is still a decomposition into minimal left ideals (of R), which implies the left semisimplicity of R. □

By Proposition 7.1.8 and this lemma, rings of the form $M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$ are left semisimple, where $D_1, \ldots, D_r$ are division rings. The Wedderburn-Artin theorem asserts that this is the only case.

Figure 7.1: Photos of N. Jacobson (1910-1999) taken from [4].

Theorem 7.1.10 (Wedderburn-Artin [27, 2])**.** *Let R be a left semisimple ring. There exists a direct product decomposition*

$$R = M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$$

for some $n_1, \ldots, n_r \in \mathbb{Z}_{\geq 1}$ and division rings $D_1, \ldots, D_r$, for some r. Such a decomposition is unique up to isomorphism and permutation of the data (n_i, D_i). Conversely, every R of this form is left semisimple.

Furthermore, up to isomorphism there are exactly r left simple modules of R.

Proof. We just observed the converse direction. Assume that R is left semisimple. By Lemma 7.1.7, one can write

$$_RR = \bigoplus_{i=1}^{r} V_i^{\oplus n_i}$$

where $V_1, \ldots, V_r$ are distinct (up to isomorphism) simple left R-modules.

Moreover, the Jordan-Hölder theorem is applicable to $_RR$ and implies

(i) such a decomposition is unique up to isomorphism and permutation,

(ii) every simple left R-module is a quotient of R by a maximal left ideal, hence isomorphic to some V_i.

Set $D_i := \mathrm{End}(V_i)$ for $i = 1, \ldots, r$, which is a division ring by Schur's lemma. We have

$$\mathrm{End}(_RR) = \bigoplus_{i=1}^{r} \mathrm{End}(V_i^{\oplus n_i}) = \bigoplus_{i=1}^{r} M_{n_i}(D_i).$$

Furthermore, we have an isomorphism of rings

$$\begin{aligned} R &\xrightarrow{\sim} \mathrm{End}(_RR) \\ x &\longmapsto [r \mapsto rx] \end{aligned}$$

the inverse being $\varphi \mapsto \varphi(1)$. Consequently, $R \simeq \prod_{i=1}^{r} M_{n_i}(D_i)$.

From Proposition 7.1.8, the simple left R-modules are exactly $V_1, \ldots, V_r$. The uniqueness part follows from Jordan-Hölder theorem. □

Remark 7.1.11. The same arguments yield a variant for right semisimple rings. One may also argue using the concept of opposite rings as follows.

$$\begin{aligned} R \text{ is right semisimple} &\iff R^{\mathrm{op}} \text{ is left semisimple} \\ &\iff R^{\mathrm{op}} \simeq \prod_{i=1}^{r} M_{n_i}(D_i) \\ &\iff R \simeq \prod_{i=1}^{r} M_{n_i}(D_i)^{\mathrm{op}}, \end{aligned}$$

the last decomposition being unique up to permutation and isomorphism. And one observes that taking transpose $A \mapsto {}^tA$ of matrices yields a ring isomorphism

$$M_{n_i}(D_i^{\mathrm{op}}) \xrightarrow{\sim} M_{n_i}(D_i)^{\mathrm{op}}.$$

Also note that D_i is a division ring if and only if D_i^{op} is. This gives the structure theorem for right semisimple rings.

Exercise 7.1.12. Justify the preceding arguments by showing that for any ring S and $n \in \mathbb{Z}_{\geq 1}$, the transpose $A \mapsto {}^tA$ induces a ring isomorphism $M_n(S)^{\mathrm{op}} \simeq M_n(S^{\mathrm{op}})$.

Corollary 7.1.13. *A ring R is left semisimple if and only if it is right semisimple.*

Proof. The structure theorems for left and right semisimple rings take the same form. Done. □

Thus it is legitimate to speak of semisimple rings. The uniquely determined components $M_{n_i}(D_i)$ are two-sided ideals of R, called the *simple components* of R.

Exercise 7.1.14. Let k be a perfect field and W be a finite-dimensional k-vector space. Given a linear transformation $T \in \mathrm{End}_k(W)$, we let $k[T]$ be the k-subalgebra of $\mathrm{End}_k(W)$ generated by T. Show that the $k[T]$-module W is semisimple if and only if T is diagonalizable over an algebraic closure $\bar{k}$ of k.

Proposition 7.1.15. *A ring R is semisimple if and only if every left (or right) R-module M is semisimple.*

Proof. Every left R-module M is is a homomorphic image of a direct sum $({}_RR)^{\oplus X}$ of ${}_RR$, for some indexing set X. Indeed, we may take X to be a set of generators of M (eg. $X = M$) so that the natural homomorphism

$$\begin{aligned} ({}_RR)^{\oplus X} &\longrightarrow M \\ (r_x)_{x\in X} &\longmapsto \sum_{x\in X} r_x \cdot x \end{aligned}$$

is surjective. It follows that M inherits the semisimplicity when R is semisimple. The other direction is trivial. □

7.2 Double centralizer property

Let R be a simple ring and $\mathfrak{a}$ be a nonzero left ideal of R. One can view $\mathfrak{a}$ as a left R-module. De ne the ring

$$D := \mathrm{End}({}_R\mathfrak{a})$$

which acts on $\mathfrak{a}$ on the right, according to our conventions. There is a natural ring homomorphism

$$\begin{aligned} f : R &\longrightarrow \mathrm{End}(\mathfrak{a}_D) \\ r &\longmapsto [a \mapsto ra]. \end{aligned}$$

Theorem 7.2.1 (Rie el)**.** *Suppose that R is a simple ring and $\mathfrak{a}$ is as above, then $f : R \xrightarrow{\sim} \mathrm{End}(\mathfrak{a}_D)$.*

The assertion is sometimes called the *double centralizer property* in the literature.

Proof. Since R is simple, f must be injective. To show the surjectivity, let $r \in \mathfrak{a}$ and $h \in E := \mathrm{End}(\mathfrak{a}_D)$. Unfolding the de nitions, one sees that

$$h \cdot f(r) = f(h(r)) \quad \text{in } E.$$

Indeed, both elements send $a \in \mathfrak{a}$ to $h(ra)$ (note that a can be regarded as an element of D, acting by right multiplication on $\mathfrak{a}$).

Since R is simple and $\mathfrak{a} \neq \{0\}$ we have

$$1 = \sum_{i=1}^{m} r_i t_i$$

for some $r_1, \ldots, r_m \in \mathfrak{a}$ and $t_1, \ldots, t_m \in R$. As f is a ring homomorphism, for every $h \in E$ the preceding discussion yields

$$h = h \cdot f(1) = \sum_{i=1}^{m} h f(r_i) f(t_i) = \sum_{i=1^m} f(h(r_i)) f(t_i) \in \mathrm{im}(f).$$

Hence f is surjective. □

As an application, we deduce an alternative approach to the Wedderburn-Artin theory for simple rings, with some re ned information.

Proposition 7.2.2. *Let R be a simple ring. The following conditions are equivalent.*

1. *${}_R R$ is a left artinian.*
2. *R has a minimal left ideal.*
3. *$R \simeq M_n(D)$ for some $n \in \mathbb{Z}_{\geq 1}$ and some division ring D.*
4. *R is left semisimple.*

Proof. (1) ⇒ (2) is an easy application of the descending chain condition. Let us prove (2) ⇒ (3). Let $\mathfrak{a}$ be a minimal left ideal, then ${}_R\mathfrak{a}$ is a simple R-module. By Theorem 7.2.1, we have $R \simeq \mathrm{End}(\mathfrak{a}_D)$ where $D := \mathrm{End}({}_R\mathfrak{a})$ is a division ring by Schur's lemma. Therefore $\mathfrak{a}_D$ is a right D-vector space and it remains to show that $\dim_D \mathfrak{a}$ is finite. Let I be the subset of D-linear transformations in $\mathrm{End}(\mathfrak{a}_D)$ of finite rank. By linear algebra, I is a nonzero two-sided ideal, hence $I = \mathrm{End}(\mathfrak{a}_D)$ and $\dim_D \mathfrak{a}$ is finite by the simplicity of R.

We have derived that (3) ⇒ (4) in Proposition 7.1.8. Finally, (4) ⇒ (1) by Lemma 7.1.7. □

The same statements hold if "left" is replaced by "right" everywhere.

7.3 Another approach to the Wedderburn-Artin Theorem

We shall present this approach as a series of exercises. Only the "left" case is considered.

Definition 7.3.1. Let R be a ring. Let $\mathfrak{a}$ be a minimal left ideal of R, define

$$B_{\mathfrak{a}} := \sum_{\mathfrak{a}' \simeq \mathfrak{a}} \mathfrak{a}' \subset R$$

where $\mathfrak{a}'$ ranges over the minimal left ideals of R which are isomorphic to $\mathfrak{a}$ as R-modules.

Exercise 7.3.2. Show that

1. $B_{\mathfrak{a}}$ is a two-sided ideal of R;
2. if $\mathfrak{a}, \mathfrak{b}$ are non-isomorphic minimal left ideals of R, then $B_{\mathfrak{a}} \cdot B_{\mathfrak{b}} = \{0\}$.

Hint. For (1), note that for every $r \in R$, there is a natural surjection $\mathfrak{a} \twoheadrightarrow \mathfrak{a}r$ of left R-modules; use this to show $\mathfrak{a}r \subset B_{\mathfrak{a}}$. For (2) it suffices to show $\mathfrak{a}\mathfrak{b} = \{0\}$. If it is not the case, there exists $x \in \mathfrak{b}$ such that $\mathfrak{a}x \neq \{0\}$; deduce that $\mathfrak{a} \simeq \mathfrak{a}x = \mathfrak{b}$ using minimality.

Next, recall that a left semisimple ring R can be written as a direct sum $\bigoplus_{\mathfrak{a}} \mathfrak{a}$ where $\mathfrak{a}$ ranges over the minimal left ideals (that is, simple R-submodules). To each $\mathfrak{a}$ in the sum is associated an idempotent $e \in R$ so that $\mathfrak{a} = Re$.

Exercise 7.3.3. Let R be a left semisimple ring. By the preceding construction we have $R = \bigoplus_{\mathfrak{a}} B_{\mathfrak{a}}$, where $\mathfrak{a}$ ranges over isomorphism classes of minimal left ideals.

1. Show that this is actually a finite direct sum.
2. Show that each $B_{\mathfrak{a}}$ is a simple and left artinian ring.

Hint. For (1), look at the decomposition of $1 \in R$. To show the simplicity of $B_{\mathfrak{a}}$ in (2), let I be a two-sided ideal of $B_{\mathfrak{a}}$, hence of R. Then I contains some minimal left ideal $\mathfrak{a}'$ of R; there exists an isomorphism $\varphi : \mathfrak{a} \xrightarrow{\sim} \mathfrak{a}'$ between left R-modules. Show that $\mathfrak{a}' \subset I$ using $\varphi(\mathfrak{a}) = \varphi(\mathfrak{a}e) = \mathfrak{a}\varphi(e) \subset I$ where $\mathfrak{a} = R \cdot e$ for some idempotent $e \in R$.

Exercise 7.3.4. Deduce the Wedderburn-Artin Theorem 7.1.10 from Proposition 7.2.2 and the $B_{\mathfrak{a}}$-construction above.

Hint. Now we have a finite decomposition $R = \prod_{\mathfrak{a}} B_{\mathfrak{a}}$ into simple, left artinian rings.

7.4 Jacobson radicals

Jacobson introduced the radical $\mathrm{rad}(R)$ of a ring in order to extend the Wedderburn-Artin structure theory to rings without minimum conditions.

De nition 7.4.1. Let R be a ring, we write

$$\mathrm{rad}(R) := \bigcap_{\mathfrak{m}:\text{maximal left ideals}} \mathfrak{m}$$

and call it the left Jacobson radical of R. Similarly we may de ne the right Jacobson radical of R.

As in the case of semisimplicity, the left and right Jacobson radicals will turn out to be the same (Proposition 7.4.5). In what follows we will only discuss the left Jacobson radical.

Lemma 7.4.2. *Let $y \in R$, the following statements are equivalent:*

1. $y \in \mathrm{rad}(R)$;
2. $1 - xy$ *admits a left inverse for every* $x \in R$;
3. $yM = \{0\}$ *for every simple left* R*-module* M.

Proof. (1) $\Rightarrow$ (2). If there exists $x \in R$ such that $1 - xy$ is not left-invertible, then Zorn's lemma implies that there exists a maximal left ideal $\mathfrak{m}$ such that $R(1 - xy) \subset \mathfrak{m}$. Since $y \in \mathrm{rad}(R) \subset \mathfrak{m}$, we will have $1 \in \mathfrak{m}$ which is absurd.

(2) $\Rightarrow$ (3). Let M be a simple left R-module. If $m \in M$ satis es $ym \neq 0$, then $Rym = M$ by the simplicity of M, hence there exists $x \in R$ such that $xym = m$. Equivalently, $(1 - xy)m = 0$. This contradicts the left invertibility of $1 - xy$.

(3) $\Rightarrow$ (1). For every maximal left ideal $\mathfrak{m}$, we have $y(R/\mathfrak{m}) = \{0\}$ by assumption, hence $y \in \mathfrak{m}$. Varying $\mathfrak{m}$ gives the assertion. □

Before stating the next result, recall that for a left R-module M, we denote its annihilator as

$$\mathrm{ann}(M) := \{r \in R : rM = 0\},$$

which is a two-sided ideal.

Corollary 7.4.3. *We have* $\mathrm{rad}(R) = \bigcap_M \mathrm{ann}(M)$*, where M ranges over the simple left R-modules. In particular,* $\mathrm{rad}(R)$ *is a two-sided ideal of R.*

As an aside, note that for the simple module $M := R/\mathfrak{m}$ in the proof above, $\mathrm{ann}(M)$ is a proper subset of $\mathfrak{m}$ in general, when R is noncommutative.

Lemma 7.4.4. *Let $y \in R$, then $y \in \mathrm{rad}(R)$ if and only if for every $x, z \in R$, we have $1 - xyz \in R^\times$.*

Proof. If $1 - xyz$ is invertible for all x, z, then $1 - xy$ is left invertible for all x, hence $y \in \mathrm{rad}(R)$ by the previous lemma. Conversely, let $y \in \mathrm{rad}(R)$. For all $z \in R$, we have $yz \in \mathrm{rad}(R)$ since $\mathrm{rad}(R)$ is a two-sided ideal. Therefore $1 - xyz$ is left invertible for all $x \in R$, that is,

$$\exists u \in R,\ u(1 - xyz) = 1.$$

The element u is right invertible. However, $xyz \in \mathrm{rad}(R)$; as before, $u = 1 + uxyz$ is left invertible. Consequently $u \in R^\times$ and thus $1 - xyz \in R^\times$. □

Proposition 7.4.5. *The left and right Jacobson radicals coincide.*

Proof. Note the left/right symmetry of the characterization of $\mathrm{rad}(R)$ in the previous lemma. □

Exercise 7.4.6. Show that $\mathrm{rad}(R)$ is the largest two-sided ideal $\mathfrak{a}$ of R satisfying $1 + \mathfrak{a} \in R^\times$. This characterization is extensively used in commutative algebra.

De nition 7.4.7. A ring R is called *semiprimitive* (or: Jacobson semisimple) if $\mathrm{rad}(R) = \{0\}$.

An extrinsic characterization of semiprimitivity in terms of R-modules will be given later. The relation between semiprimitivity and semisimplicity will be deferred to the next lecture.

Proposition 7.4.8. *For every two-sided ideal $\mathfrak{a}$ of R contained in $\mathrm{rad}(R)$, we have*

$$\mathrm{rad}(R/\mathfrak{a}) = \mathrm{rad}(R)/\mathfrak{a}.$$

In particular, $R/\mathrm{rad}(R)$ is semi-primitive.

Proof. Immediate from the de nition, since any maximal left ideal of R must contain $\mathfrak{a}$. □

Proposition 7.4.9. *Let $\bar{R} := R/\mathrm{rad}(R)$. The natural map*

$$\left\{\textit{simple left } \bar{R}\textit{-modules}\right\} / \simeq \longrightarrow \{\textit{simple left } R\textit{-modules}\} / \simeq$$

is bijective.

Proof. Recall that $\mathrm{rad}(R)$ annihilates every simple left R-module. □

Next, we shall discuss the relation between the Jacobson radical and nilpotence in R.

De nition 7.4.10. Let $\mathfrak{a}$ be a left (resp. right) ideal of R. We say

- ⋆ $\mathfrak{a}$ is nil, if every $x \in \mathfrak{a}$ is nilpotent, that is, $x^{n(x)} = 0$ for some $n(x) \in \mathbb{Z}_{\geq 1}$;
- ⋆ $\mathfrak{a}$ is nilpotent, if $\mathfrak{a}^n = \{0\}$ for some $n \in \mathbb{Z}_{\geq 1}$.

"Nilpotent" implies "nil", but the converse is not always true. See Corollary 7.4.14, however.

Exercise 7.4.11. Show that a finite sum of nilpotent left (resp. right) ideals of R is still nilpotent.

Lemma 7.4.12. *Let $\mathfrak{a}$ be a left (resp. right) ideal of R. If $\mathfrak{a}$ is nil, then $\mathfrak{a} \subset \mathrm{rad}(R)$.*

Proof. The proof is well-known. It suffices to consider the left case. Let $y \in \mathfrak{a}$ and $x \in R$. Then

$$(1 - xy)^{-1} = \sum_{i=0}^{\infty} (xy)^i.$$

Indeed, this can be verified by elementary algebra; the sum is finite since $xy \in \mathfrak{a}$ is nilpotent. □

Theorem 7.4.13. *Let R be a left artinian ring, then $\mathrm{rad}(R)$ is the largest nilpotent left ideal; it is also the largest nilpotent right ideal.*

Proof. Set $J := \mathrm{rad}(R)$. In view of the preceding lemma, it suffices to show that J is nilpotent.

We have a descending chain $J \supset J^2 \supset \cdots$, which must stabilize, say $J^k = I$ for some left ideal I whenever $k \gg 0$. Suppose that $I \neq \{0\}$. Again, the descending chain condition yields a minimal element $\mathfrak{a}_0$ in

$$\{\mathfrak{a} : \text{left ideal such that } I\mathfrak{a} \neq 0\}.$$

Choose $a \in \mathfrak{a}_0$ such that $Ia \neq \{0\}$. Since $I^2 = I$ by the construction of I, we have $I(Ia) = I^2 a = Ia \neq \{0\}$, thus $Ia = \mathfrak{a}_0$ by minimality.

All in all, there exists $y \in I \subset J$ such that $a = ya$, that is, $(1 - y)a = 0$. However $1 - y \in R^\times$, thus $a = 0$, a contradiction. □

Corollary 7.4.14. *Let R be a left artinian ring, then every left or right nil ideal $\mathfrak{a}$ is nilpotent.*

Proof. The Theorem asserts that $\mathrm{rad}(R)$ is nilpotent, hence so is the smaller ideal $\mathfrak{a}$ (Lemma 7.4.12). □

LECTURE 8

SEMIPRIMITIVE RINGS

8.1 Semiprimitivity versus semisimplicity

We keep the conventions of the previous lecture and follow Lam's book [15] closely in what follows.

Recall that we have de ned semisimple rings and semiprimitive rings in the previous lecture, the latter also known as *Jacobson semisimple* or *J-semisimple* rings in the literature. The following result shows that "semisimple" is equivalent to "semiprimitive + left artinian".

A left (resp. right) ideal $\mathfrak{a}$ of R is called *principal* if there exists $x \in R$ such that $\mathfrak{a} = Rx$ (resp. xR).

Proposition 8.1.1. *Let R be a ring. The following statements are equivalent.*

1. *R is semisimple.*
2. *R is semi-primitive and left artinian.*
3. *R is semi-primitive and satis es descending chain condition on principal left ideals.*

Proof. (1) $\Rightarrow$ (2). We have seen that semisimple rings are left artinian. On the other hand, there exists a left ideal $\mathfrak{a}$ such that $R = \mathrm{rad}(R) \oplus \mathfrak{a}$. If $\mathrm{rad}(R) \neq \{0\}$, then $\mathfrak{a} \neq R$ and there exists a maximal left ideal $\mathfrak{m} \supset \mathfrak{a}$. But we also have $\mathfrak{m} \supset \mathrm{rad}(R)$, hence $\mathfrak{m} = R$ which is absurd.

(2) $\Rightarrow$ (3). Trivial.

(3) $\Rightarrow$ (1). Our assumption has two consequences:

(i) Every left ideal contains a minimal ideal — this follows from the DCC on principal left ideals. Note that minimal ideals must be principal.

(ii) Every minimal left ideal I is a direct summand. Indeed, there exists a maximal left ideal $\mathfrak{m} \not\supset I$ since $\mathrm{rad}(R) = \{0\}$, hence $I + \mathfrak{m} = R$ and $I \cap \mathfrak{m} = \{0\}$ (by minimality), i.e. $R = I \oplus \mathfrak{m}$.

Now take a minimal left ideal $\mathfrak{a}_1 \subset R$ and write $R = \mathfrak{a}_1 \oplus \mathfrak{b}_1$. If $\mathfrak{b}_1 = \{0\}$ then R is semisimple as a left R-module and the proof terminates. Otherwise, there exists a minimal left ideal

$$\mathfrak{a}_2 \subset \mathfrak{b}_1$$

together with a direct sum decomposition $R = \mathfrak{a}_2 \oplus \mathfrak{c}_2$; let $\mathrm{pr}_2 : R \twoheadrightarrow \mathfrak{a}_2$ be the corresponding projection homomorphism. Set

$$\mathfrak{b}_2 := \mathfrak{c}_2 \cap \mathfrak{b}_1 = \ker[\mathrm{pr}_2 : \mathfrak{b}_1 \twoheadrightarrow \mathfrak{a}_2].$$

One checks that $\mathfrak{b}_1 = \mathfrak{a}_2 \oplus \mathfrak{b}_2$, thus $R = \mathfrak{a}_1 \oplus \mathfrak{a}_2 \oplus \mathfrak{b}_2$. If $\mathfrak{b}_2 = \{0\}$ then R is semisimple, otherwise we can take a minimal $\mathfrak{a}_3 \subset \mathfrak{b}_2$, and so forth. Assuming that R is not semisimple, we would get

- ⋆ a descending chain of left ideals $R =: \mathfrak{b}_0 \supset \mathfrak{b}_1 \supset \mathfrak{b}_2 \supset \cdots$;
- ⋆ a family of minimal left ideals $\mathfrak{a}_1, \mathfrak{a}_2, \ldots$, such that

$$\mathfrak{a}_i \oplus \mathfrak{b}_i = \mathfrak{b}_{i-1}, \quad i \geq 1.$$

Note that if an R-module is generated by a single element, then so are its homomorphic images (the direct summands included). In particular, this applies to left ideals and we deduce that $\mathfrak{b}_i$ is principal for each $i \geq 0$. All in all, we obtain a strictly descending chain condition of left ideals. Contradiction. □

Originally, Wedderburn de nes the radical for nite-dimensional algebras over a eld as the largest nilpotent ideal and uses it to characterize semisimplicity. His approach is easily recovered as follows.

Corollary 8.1.2. *Let R be a left artinian ring. There is a largest nilpotent left (resp. right) ideal* $\mathrm{nil}(R)$ *and R is semisimple if and only if* $\mathrm{nil}(R) = \{0\}$.

Proof. We have seen in the previous lecture that $\mathrm{nil}(R)$ is nothing but $\mathrm{rad}(R)$. Now apply the previous result. □

Exercise 8.1.3. Check that $\mathbb{Z}$ is semiprimitive but not semisimple.

Exercise 8.1.4. The *socle* of a left R-module M, denoted by $\mathrm{soc}(M)$, is de ned as its maximal semisimple submodule, i.e. the sum of the simple R-submodules of M. Show that

1. $\mathrm{soc}(M) \subset \{m \in M : \mathrm{rad}(R)m = 0\}$;
2. if $\bar{R} := R/\mathrm{rad}(R)$ is left artinian, then $\mathrm{soc}(M) = \{m \in M : \mathrm{rad}(R)m = 0\}$.

To elucidate the relation between artinian and noetherian conditions, we record the following result without proof. The reader may consult [15, (4.15)] for details.

Theorem 8.1.5 (Hopkins-Levitzki)**.** *Let R be a ring such that $\mathrm{rad}(R)$ is a nilpotent ideal and that $R/\mathrm{rad}(R)$ is semisimple. For every left R-module M, we have*

$$M \text{ is noetherian} \iff M \text{ is artinian}.$$

8.2 Intermezzo: der Nullstellensatz

We will need some dose of commutative algebra.

Let k be a field and R be a quotient k-algebra $k[X_1, \dots, X_n]/\mathfrak{a}$ of the polynomial algebra $k[X_1, \dots, X_n]$ over k with n variables. It is essentially a consequence of Hilbert's *Nullstellensatz* that

$$\mathrm{rad}(R) = \mathrm{nil}(R) = \sqrt{\mathfrak{a}}/\mathfrak{a}$$

where $\sqrt{\mathfrak{a}} := \{f \in k[X_1, \dots, X_n] : \exists m,\ f^m \in \mathfrak{a}\}$.

For a *commutative ring* R, we define its nilradical as the ideal

$$\mathrm{nil}(R) := \sqrt{(0)_R} = \{x \in R : x \text{ is nilpotent}\}.$$

It is well-known result in commutative algebra that $\mathrm{nil}(R)$ is the intersection of all *prime ideals* of R, therefore $\mathrm{nil}(R) \subset \mathrm{rad}(R)$. The Nullstellensatz amounts to the assertion

$$\mathfrak{p} = \bigcap_{\mathfrak{m}:\text{maximal ideal} \supset \mathfrak{p}} \mathfrak{m}, \quad \forall \mathfrak{p} : \text{prime ideal of } R, \tag{8.1}$$

whenever $R = k[X_1, \dots, X_n]/\mathfrak{a}$ as above. This result is one of the cornerstones of algebraic geometry. Let us deduce a generalization thereof from the theory developed so far.

Theorem 8.2.1 (E. Snapper)**.** *Let R be a commutative ring. Then the polynomial ring $R[X]$ over R in one variable satisfies* $\mathrm{rad}(R[X]) = \mathrm{nil}(R[X])$.

Proof. To show that $\mathrm{nil}(R[X]) \supset \mathrm{rad}(R[X])$, let $f(X) = \sum_i a_i X^i \in \mathrm{rad}(R[X])$, then $1 + Xf(X) = 1 + \sum_i a_i X^{i+1} \in R[X]^\times$. By looking at the reduction modulo $\mathfrak{p}$ of $f(X)$ for every prime ideal $\mathfrak{p}$ of R, we see that $a_i \in \bigcap \mathfrak{p} = \mathrm{nil}(R)$ for all i. It remains to show that an element of $R[X]$ is nilpotent if its coefficients are all nilpotent, which we leave to the reader. □

Lemma 8.2.2. *Let $R \subset A$ be commutative domains such that A is finitely generated over R as an R-algebra. If* $\mathrm{rad}(R) = \{0\}$, *then* $\mathrm{rad}(A) = \{0\}$.

Proof. We may assume that A is generated by a single element $a \in A$ over R. If a is transcendental over the field of fractions $K := \mathrm{Frac}(R)$, the Theorem above can be applied. Let us assume that a satisfies $f(a) = 0$ for some $f(X) = \sum_{i=0}^n r_i X^i \in R[X]$ with the smallest possible degree n. Let $b \in \mathrm{rad}(A)$. If $b \neq 0$, it satisfies $g(b) = 0$ for some $g(X) = \sum_{i=0}^m s_i X^i \in R[X]$ with the smallest possible degree m. Since A is a domain, we must have $s_0 \neq 0$.

Using $\mathrm{rad}(R) = \{0\}$, there exists a maximal ideal $\mathfrak{m}$ of R such that $r_n s_0 \notin \mathfrak{m}$. After localization at $\mathfrak{m}$, we see $A' := A \otimes_R R_\mathfrak{m}$ becomes a finite $R_\mathfrak{m}$-module. Nakayama's Lemma implies that $\mathrm{rad}(R_\mathfrak{m})A' \subsetneq A'$, thus $\mathfrak{m}A \subsetneq A$. Now choose a maximal ideal $\mathfrak{m}_A$ of A containing $\mathfrak{m}$. We must have $\mathfrak{m}_A \cap R = \mathfrak{m}$, which entails $s_0 \notin \mathfrak{m}_A$. This is a contradiction since $s_0 = -\sum_{i=1}^m s_i b^i \in \mathrm{rad}(A)$. □

Theorem 8.2.3. *Let $R \subset A$ be commutative rings such that A is finitely generated over R as an R-algebra. Assume that R satisfies (8.1). The following statements hold.*

1. *The ring A satisfies (8.1) as well.*
2. *Let $\mathfrak{m}$ be a maximal ideal of A, then $R \cap \mathfrak{m}$ is a maximal ideal of R.*
3. *If A is a field then so is R, and A is a finite field extension over R.*

Proof. Note that (8.1) (for A) is equivalent to $\mathrm{rad}(A/\mathfrak{p}) = 0$ for every prime ideal $\mathfrak{p}$ of A. Apply the previous Lemma to the commutative domains $R/R \cap \mathfrak{p} \subset A/\mathfrak{p}$ to prove (1).

Let us prove (3). Using (1) and induction, one reduces to the case $A = R[a]$ for some $a \in A$. Since A is a field, a satisfies $\sum_{i=0}^{n} c_i a^i = 0$ for some $c_0, \ldots, c_n \in R$ with $c_n \neq 0$ (otherwise $A \simeq R[X]$). Let $\mathfrak{m}$ be any maximal ideal of R not containing c_n, which exists since $\mathrm{rad}(R) = 0$. By the proof of the previous Lemma, $\mathfrak{m}A \subsetneq A$, hence $\mathfrak{m} = 0$. This implies that R is a field and A is finite over R.

As for (2), replace A (resp. R) by $A/\mathfrak{m}$ (resp. $R/R \cap \mathfrak{m}$) to reduce to the assertion (3). □

Commutative rings satisfying (8.1) are called Jacobson rings or Hilbert rings in the literature.

8.3 Primitive rings and primitive ideals

Recall that an R-module M is called faithful if the scalar multiplication induces an injection $R \to \mathrm{End}_{\mathrm{ab.grp}}(M)$.

Proposition 8.3.1. *A ring R is semiprimitive if and only if there exists a faithful semisimple left R-module.*

Proof. If there exists a faithful semisimple left R-module M, then $\mathrm{rad}(R) \subset \mathrm{ann}(M) = \{0\}$. Conversely, assume $\mathrm{rad}(R) = \{0\}$ and set

$$M := \bigoplus_{N:\mathrm{simple}} N.$$

Then M is semisimple and $\mathrm{ann}(M) = \bigcap_N \mathrm{ann}(N) = \mathrm{rad}(R)$ is zero, hence M is faithful. □

This extrinsic characterization (i.e. in terms of the R-modules) motivates the following definition.

Definition 8.3.2. A ring R is called left (resp. right) *primitive* if there exists a faithful simple left (resp. right) R-module.

Remark 8.3.3. Simple modules are nonzero by definition, hence left or right primitive rings R must be nonzero as well.

Remark 8.3.4. The notion of primitivity is NOT left-right symmetric. Counterexamples are not so easy to construct, however; see [5].

Definition 8.3.5. A two-sided ideal $\mathfrak{a}$ of R is called left (resp. right) primitive if $R/\mathfrak{a}$ is a primitive ring, or equivalently, if $\mathfrak{a} = \mathrm{ann}(M)$ for a simple left (resp. right) R-module.

Proposition 8.3.6. *We have* $\mathrm{rad}(R) = \bigcap \mathfrak{a}$ *where* $\mathfrak{a}$ *ranges over left (resp. right) primitive ideals.*

Proof. Recall the left-right symmetry of $\mathrm{rad}(R)$ and use the property $\mathrm{rad}(R) = \bigcap \mathrm{ann}(M)$ where M ranges over the simple left (resp. right) R-modules. □

Example 8.3.7. Take V to be a right vector space over a division ring D. Assume $V \neq \{0\}$ and set $R := \mathrm{End}(V_D)$ so that V is a simple faithful left R-module, which can be easily checked by linear algebra over D. Therefore R is a left primitive ring.

- ⋆ If $n := \dim_D V$ is nite, then $R \simeq M_n(D)$ is a left artinian simple ring which arises in the Wedderburn-Artin theorem.
- ⋆ When $\dim_D V$ is in nite we get something much larger. This turns out to be the typical case, cf. Theorem 8.5.2.

Proposition 8.3.8. *Simple rings are left and right primitive.*

Proof. A simple ring R (i.e. nonzero and without nontrivial two-sided ideals) must act faithfully on every nonzero left R-module M since $\mathrm{ann}(M)$ is a two-sided ideal. It remains to note that simple R-modules exist: take a maximal left ideal $\mathfrak{m}$ and form $R/\mathfrak{m}$. □

Proposition 8.3.9. *Let R be a left artinian ring. Then*

1. *R is semisimple if and only if R is semiprimitive;*

2. *R is simple if and only if R is left primitive.*

Proof. We have proved (1). As for (2), we have just shown one direction: simplicity implies primitivity.

Conversely, assume that R is left primitive. Then R is semiprimitive since $\mathrm{rad}(R) = \bigcap \mathrm{ann}(M)$ with M ranging over simple left R-modules, and $\mathrm{ann}(M) = 0$ for some simple M. By (1) it follows that R is semisimple. Now invoke the Wedderburn-Artin theorem and check that if there are more than one simple components of R, then R cannot be left primitive. □

Exercise 8.3.10. Show that a commutative primitive ring is a eld. Hint: $\mathrm{ann}(R/\mathfrak{m}) = \mathfrak{m}$ for commutative R.

8.4 Density theorems

De nition 8.4.1. Let R and k be rings. Let $V = {}_R V_k$ be an (R, k)-bimodule. Then $E := \mathrm{End}(V_k)$ acts on V on the left and there is a natural homomorphism $R \to E$, given by the left R-module structure of V.

We say that R *acts densely* on V_k if for every $f \in E$, $n \in \mathbb{Z}_{\geq 1}$ and $v_1, \ldots, v_n \in V$, there exists $r \in R$ such that

$$rv_i = f(v_i), \quad i = 1, \ldots, n.$$

Remark 8.4.2. The etymology of "density" is as follows. We equip V with the discrete topology and E with the coarsest topology such that for every $v \in V$, the homomorphism $f \mapsto f(v) \in V$ is continuous. Then R acts densely on V_k if and only if the natural homomorphism

$$R \to E$$

has dense image.

Lemma 8.4.3. *Let V be a semisimple left R-module and $k := \mathrm{End}({}_R V)$. Set $E := \mathrm{End}(V_k)$. Every R-submodule $W \subset V$ is an E-submodule.*

Proof. Use semisimplicity to write $V = W \oplus W'$ as R-modules, for some $W' \subset V$, and let $e : V \twoheadrightarrow W$ be the projection homomorphism. Note that $e \in k$. For every $f \in E$, we have

$$f(W) = f(We) = (fW)e \subset W,$$

as required. □

Theorem 8.4.4 (Jacobson, Chevalley; rst appeared in [10])**.** *Let R be a ring, V be a semisimple left R-module and $k := \mathrm{End}({}_R V)$, so that V becomes an (R, k)-bimodule. Then R acts densely on V_k.*

Proof. Put $E := \mathrm{End}(V_k)$ as before. Given $f \in E$ and $v_1, \ldots, v_n \in V$, we set

- ⋆ $\tilde{V} := V^{\oplus n}$ which is still a left R-module;
- ⋆ $\tilde{k} := \mathrm{End}({}_R \tilde{V}) = M_n(\mathrm{End}({}_R V)) = M_n(k)$;
- ⋆ $\tilde{f} := (f, \ldots, f)$, the diagonal action of f on $V^{\oplus n}$;
- ⋆ $\tilde{W} := R(v_1, \ldots, v_n) \subset \tilde{V}$.

Let us check that $\tilde{f} \in \mathrm{End}(\tilde{V}_{\tilde{k}})$. Consider $\tilde{u} = (u_1, \ldots, u_n) \in \tilde{V}$ and a matrix $A = (a_{ij})_{1 \le i,j \le n} \in M_n(k)$, viewed as an element of $\tilde{k}$. Then $\tilde{f}(\tilde{u}A)$ is obtained by rst forming the product

$$\tilde{u}A$$

using matrix multiplication (formally), then multiplying each entry of $\tilde{u}A$ by f from the left. Since V is an (E, k)-bimodule, this equals $(\tilde{f}\tilde{u})A = (fu_1, \ldots, fu_n)A$.

The previous Lemma can thus be applied. It asserts that $\tilde{W}$ is stable under $\tilde{f} \in \mathrm{End}(\tilde{V}_{\tilde{k}})$, that is,

$$\exists r \in R,\ \tilde{f}(v_1, \ldots, v_n) = r(v_1, \ldots, v_n).$$

Thus $f(v_i) = rv_i$ for $i = 1, \ldots, n$. □

The proof above is usually attributed to N. Bourbaki.

8.5 Structure theory for primitive rings

Lemma 8.5.1. *Let R, V, k, E be as in the Density Theorem 8.4.4. If the right k-module V is nitely generated, then the natural homomorphism $\rho : R \to E$ is surjective.*

Proof. Choose a set of generators $v_1, \ldots, v_n$ of V_k. Let $f \in E$, there exists $r \in R$ such that $rv_i = f(v_i)$ for all i by the Density Theorem 8.4.4. Hence $\rho(r) = f$. □

Theorem 8.5.2. *Let R be a left primitive ring, V be a faithful simple left R-module. Set $k := \mathrm{End}({}_R V)$, which is a division ring by Schur's Lemma. Then R is isomorphic to a dense subring of $\mathrm{End}(V_k)$ in the sense of Remark 8.4.2. Moreover,*

1. *if R is left artinian, then $n := \dim_k V$ is nite and $R \simeq M_n(k)$;*
2. *if R is not left artinian, then $\dim_k V$ is in nite and for every $n \in \mathbb{Z}_{\geq 1}$ there exists a subring R_n of R together with a surjective ring homomorphism $R_n \twoheadrightarrow M_n(k)$.*

Proof. We have the natural homomorphism $\rho : R \to E := \mathrm{End}(V_k)$. Note that ρ is injective by the faithfulness of V. The density of $\rho(R)$ in E is just a paraphrase of Theorem 8.4.4 and Remark 8.4.2. Hence the rst assertion.

Assume that $n := \dim_k V$ is nite. By Lemma 8.5.1, ρ is surjective, thus $R \simeq M_n(k)$; in particular R is left artinian.

Assume that $\dim_k V$ is in nite. There exists a family $\{v_i\}_{i \in \mathbb{Z}_{\geq 1}}$ of k-linear independent vectors in V. For every $n \in \mathbb{Z}_{\geq 1}$, let V_n be the k-linear span of $v_1, \ldots, v_n$ and put

$$\begin{aligned} R_n &:= \{r \in R : r(V_n) \subset V_n\} \quad \rightsquigarrow \text{subring of } R, \\ \mathfrak{a}_n &:= \{r \in R : r(V_n) = 0\} \quad \rightsquigarrow \text{two-sided ideal of } R_n. \end{aligned}$$

We have the natural ring homomorphism $\rho_n : R_n/\mathfrak{a}_n \hookrightarrow \mathrm{End}(V_{n,k})$. Furthermore, the Density Theorem implies that ρ_n is actually surjective, hence $R_n \twoheadrightarrow R_n/\mathfrak{a}_n \simeq M_n(k)$.

Note that $\mathfrak{a}_n$ is a left ideal of R, and $\mathfrak{a}_{n+1} \subsetneq \mathfrak{a}_n$ for all n. Thus R is not left artinian when $\dim_k V$ is in nite. This completes the proof. □

Remark 8.5.3. The density theorem gives another proof of the Wedderburn-Artin theorem for left artinian simple rings.

As for the semiprimitive rings, there is technique called *subdirect products* that allows us to reduce some ring-theoretic questions about semiprimitive rings to the left primitive case. For details see [15, §12]. An impressive application of this procedure is the celebrated Jacobson-Herstein Theorem [15, (12.9)]. It asserts that a ring R is commutative if and only if

$$\forall x \text{ of the form } ab - ba,\ a, b \in R,\ \exists n(x) \in \mathbb{Z}_{>1} \text{ such that } x^{n(x)} = x. \tag{8.2}$$

In the following exercises, we ASSUME the validity of the Jacobson-Herstein Theorem for division rings (see [15, (13.9)]) and derive the case for general rings.

Exercise 8.5.4. Prove the Jacobson-Herstein Theorem for left primitive rings. **Hint**: show that (8.2) is satis ed by $R = M_n(k)$ for some division ring k if and only if $n = 1$ and k is a eld, by considering the element $x = E_{12} = E_{11}E_{12} - E_{12}E_{11}$ when $n > 1$. Now apply the Theorem 8.5.2 to show that a left primitive ring R satisfying (8.2) must be a eld.

Exercise 8.5.5. For a semiprimitive ring R, show the injectivity of the natural ring homomorphism

$$R \to \prod_{\substack{\mathfrak{a} \\ \text{left primitive ideals}}} R/\mathfrak{a}.$$

Deduce the Jacobson-Herstein Theorem for R from the case for the left primitive rings $R/\mathfrak{a}$.

Exercise 8.5.6. Deduce the Jacobson-Herstein Theorem in full generality. **Hint**: for $x = ab - ba \in R$ we have $x(1 - x^{n(x)-1}) = 0$ for some $n(x) > 1$; on the other hand, the case for $\bar{R} := R/\mathrm{rad}(R)$ implies that $x \in \mathrm{rad}(R)$, hence $1 - x^{n(x)-1} \in R^\times$.

The weaker assertion that $x^3 = x$ for all $x \in R$ implies commutativity is sometimes posed as a challenge to undergraduates by cruel professors.

8.6 The primitive spectrum

Let R be a nonzero ring with unit. De ne

$$\mathrm{Prim}(R) := \{\text{left primitive ideals of } R\}.$$

For every two-sided ideal I of R, set

$$V(I) := \{\mathfrak{a} \in \mathrm{Prim}(R) : \mathfrak{a} \supset I\}.$$

Adopt the following notation: given an R-module M and a left ideal $\mathfrak{a}$ of R, de ne $\mathfrak{a}M$ to be the submodule consisting of linear combinations of elements of the form xm where $x \in \mathfrak{a}$ and $m \in M$.

Lemma 8.6.1. *Given two-sided ideals I, J, we have $V(I) \cup V(J) = V(I \cap J)$.*

Proof. The inclusion $V(I) \cup V(J) \subset V(I \cap J)$ is evident. Let $\mathfrak{a} \in \mathrm{Prim}(R)$ such that $\mathfrak{a} \supset I \cap J$. Take a simple left R-module M with $\mathrm{ann}(M) = \mathfrak{a}$. If I is not contained in $\mathfrak{a}$, then $IM = M$ by the simplicity of M. Similarly, $JM = M$ if J is not contained in $\mathfrak{a}$. This would imply $IJ \cdot M = M$, which is impossible since $IJ \subset I \cap J \subset \mathfrak{a}$. □

Exercise 8.6.2. Show that there exists a unique topological structure on $\mathrm{Prim}(R)$ such that the closed subsets are precisely those $V(I)$.

Exercise 8.6.3. For every subset S of $\mathrm{Prim}(R)$, show that the closure of S is given by $V(\bigcap_{\mathfrak{a} \in S} \mathfrak{a})$. Note that this property characterizes the topology on $\mathrm{Prim}(R)$ by Kuratowski's axioms.

Exercise 8.6.4. Show that $\mathrm{Prim}(R)$ is a T_0 space, that is, for every $\mathfrak{a} \neq \mathfrak{b} \in \mathrm{Prim}(R)$, there exists an open subset U such that $\mathfrak{a} \in U$, $\mathfrak{b} \notin U$.

This topology is called the *Jacobson topology* or the *hull-kernel topology* that plays a prominent role in the study of C^*-algebras. It can be regarded as a noncommutative analogue of the Zariski topology.

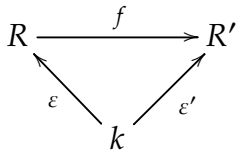
The case of right primitive ideals is similar.

8.7 Finite-dimensional algebras: Burnside's Theorem

Let k be a commutative ring. Recall that a k-algebra R is a ring homomorphism

$$\varepsilon : k \to R$$

such that $\varepsilon(k)$ lies in the center of R. Thus the multiplication $R \times R \to R$ is k-bilinear, inducing a k-linear homomorphism $R \otimes_k R \to R$. Note that our algebras are all associative and unital by convention. A homomorphism between k-algebras R, R' is a ring homomorphism $f : R \to R'$ such that the diagram



commutes. Equivalently, f is a k-linear ring homomorphism.

De nition 8.7.1. A k-algebra is called a *division algebra* if it is a division ring.

In what follows, we only consider the case where k is a eld and regard k as a subset of R. A k-algebra R is called nite-dimensional if $\dim_k R$ is nite. Finite-dimensional k-algebras are automatically left (resp. right) artinian and noetherian as rings.

Lemma 8.7.2. *Let R be a nite-dimensional k-algebra and M be a simple left R-module. Let $D := \mathrm{End}({}_R M)$ which acts on M on the right, then the natural map $R \to \mathrm{End}(M_D)$ is surjective.*

Proof. Firstly, observe that M must be nite-dimensional over k. Indeed, $M \simeq R/\mathfrak{m}$ for some maximal left ideal $\mathfrak{m}$, and $\mathfrak{m}$ is certainly a k-vector subspace. We may embed k into D via scalar multiplication. Therefore M is nitely generated over $k \subset D$. The required surjectivity then follows from Lemma 8.5.1. □

Thus we recover the following classical result of Burnside. It will be used in the representation theory of nite groups.

Theorem 8.7.3. *Consider the situation*
- ⋆ *k: an algebraically closed eld,*
- ⋆ *V: a nite-dimensional k-vector space,*
- ⋆ *R: a subalgebra of $\mathrm{End}_k(V)$ such that the only R-stable subspaces of V are $\{0\}$ and V.*

Then we have $R = \mathrm{End}_k(V)$ over k.

Proof. Note that V is a simple left R-module. By Schur's Lemma, $D := \mathrm{End}({}_R V)$ is a division k-algebra that is nite-dimensional since V is. Every $x \in D$ must satisfy some polynomial equation over k: indeed, the elements

$$1, x, x^2, \ldots$$

in D are linearly dependent over k. Hence $D = k$ since $D^\times = D \setminus \{0\}$ and k is algebraically closed. We conclude by the previous Lemma that $R \xrightarrow{\sim} \mathrm{End}(V_D) = \mathrm{End}_k(V)$. □

The module/representation theory of nite-dimensional associative algebras is a highly active area of current research, interweaving ideas from algebra, topology, algebraic geometry and combinatorics, etc. One may take a glimpse of [3] to get some taste of this subject.

Have a nice vacation!

LECTURE 9

CENTRAL SIMPLE ALGEBRAS

Our main references are [12, §4.6] and [23, Chapter 8]. Substantial use of field theory will be made. Be prepared!

9.1 Basic properties of central simple algebras

Let k be a field and A, B be k-algebras. We have defined the tensor product k-algebra $A \otimes_k B$. Recall that

$$(a \otimes b)(a' \otimes b') = aa' \otimes bb', \qquad a, a' \in A,\ b, b' \in B$$

by stipulation. We have inclusions of k-algebras

$$A = A \otimes 1 \subset A \otimes_k B,$$
$$B = 1 \otimes B \subset A \otimes_k B.$$

Therefore A and B commute with each other when regarded as subalgebras of $A \otimes_k B$. Denote the category of k-algebras by k-**Alg** and that of sets by **Sets**. The tensor product can be characterized by an universal property: there is an isomorphism between functors from k-**Alg** to **Sets**

$$\begin{array}{c} \{(f, g) \in \mathrm{Hom}(A, -) \times \mathrm{Hom}(B, -) : \mathrm{Im}(f), \mathrm{Im}(g) \text{ commute } \} \\ \uparrow \simeq \\ \mathrm{Hom}(A \otimes_k B, -) \end{array}$$

where the $\mathrm{Hom}(\cdots)$ are taken in the category k-**Alg**: for any k-algebra C and $h \in \mathrm{Hom}(A \otimes_k B, C) \times \mathrm{Hom}(B, C)$, we associate $(f, g) \in \mathrm{Hom}(A, C) \times \mathrm{Hom}(B, C)$ using the two inclusions above.

Exercise 9.1.1. Verify the aforementioned universal property for tensor products.

Definition 9.1.2. Let A be a k-algebra, the center of A is denoted by $Z(A)$. More generally, for any subset $S \subset A$, we denote by $Z_A(S) = \{z \in A : \forall s \in S,\ zs = sz\}$ the centralizer of S in A. We say that A is *central* if $Z(A) = k$.

Convention 9.1.3. Unless otherwise specified, the k-algebras under consideration are assumed to be finite-dimensional over k.

Definition 9.1.4. Let A be a k-algebra. We say that A is *central simple* if
- ⋆ A is a simple ring,
- ⋆ A is a central k-algebra.

Central simple algebras are left (and also right) noetherian and artinian, hence they are of the form $M_n(D)$ where D is a central division k-algebra. Recall (Wedderburn-Artin Theorem) that D and n can be recovered by the decomposition ${}_AA \simeq M^{\oplus n}$ where M is the unique simple left A-module, and $D \simeq \mathrm{End}({}_AM)$.

Our main concern is the tensor products of central simple algebras.

Example 9.1.5. We have $M_n(k) \otimes_k M_m(k) \simeq M_{nm}(k)$ as k-algebras. Indeed, let V and W be k-vector spaces of dimension n and m, respectively. There is a canonical homomorphism

$$\begin{aligned} \mathrm{End}_k(V) \otimes_k \mathrm{End}_k(W) &\xrightarrow{\sim} \mathrm{End}_k(V \otimes_k W), \\ \varphi \otimes \psi &\longmapsto [v \otimes w \mapsto \varphi(v) \otimes \psi(w)] \end{aligned}$$

which turns out to be an isomorphism by counting dimensions. More generally, we have $M_n(D) \otimes_k M_m(k) \simeq M_{nm}(D)$ for any division k-algebras D.

The opposite k-algebra $(A^{\mathrm{op}}, +, \star)$ of $(A, +, \cdot)$ is defined by $x \star y = y \cdot x$.

Lemma 9.1.6. *Let A be a central k-algebra. The homomorphism of k-algebras*

$$\begin{aligned} F : A \otimes_k A^{\mathrm{op}} &\longrightarrow \mathrm{End}_k(A) \\ a \otimes b &\longmapsto [x \mapsto axb] \end{aligned}$$

is an isomorphism if and only if A is central simple.

Proof. Suppose A is not simple. Let I be a proper, nonzero two-sided ideal of A. The image of F must stabilize I, therefore F cannot be surjective.

Now assume that A is simple. Write $E := A \otimes_k A^{\mathrm{op}}$ and regard A as a left E-module using F. Then A is a simple E-module since A is a simple ring. We have an identification $\mathrm{End}({}_EA) \xrightarrow{\sim} Z(A) = k$. Indeed, for $\varphi \in \mathrm{End}_k(A)$, we have $\varphi \in \mathrm{End}({}_EA)$ if and only if $\varphi(xay) = x\varphi(a)y$ for all $a, x, y \in A$, in which case we have

$$x\varphi(1) = \varphi(x) = \varphi(1)x, \quad x \in A$$

hence $\varphi(1) \in Z(A)$; conversely $x \mapsto zx$ defines an element of $\mathrm{End}({}_EA)$ if $z \in Z(A)$.

Apply the Density Theorem to ${}_EA$. It follows that F is surjective, thus is bijective by dimension counting. □

Lemma 9.1.7. *Let A be a k-algebra and K/k be a field extension, then A is central simple over k if and only if $A_K := A \otimes_k K$ is central simple over K.*

Proof. The upshot is that being central simple is a property de ned in terms of linear algebra. Indeed, A is central if and only if $\dim_k Z(A) = 1$, whilst $Z(A)$ is de ned by the k-linear equations $xa - ax = 0$ in x, where a ranges over a basis of A. The dimension of $Z(A)$ does not change after base change to K. Thus A is central if and only if A_K is central over K. Similarly, Lemma 9.1.6 asserts that a central k-algebra A is simple if and only if the k-linear map F is surjective. □

Theorem 9.1.8. *Let B be a k-algebra, not necessarily of nite dimension over k, and A be a k-subalgebra which is central simple. Set $C := Z_B(A)$, then*

1. *the natural homomorphism $A \otimes_k C \to B$ given by $a \otimes c \mapsto ac$ between k-algebras is an isomorphism;*
2. *there is a bijection*

$$\{\text{two-sided ideals of } C\} \longrightarrow \{\text{two-sided ideals of } B\}$$
$$I \longmapsto AI = A \otimes_k I,$$

   whose inverse is given by $I = AI \cap C$.
3. $Z(B) = Z(C)$.

We need a few easy properties of tensor products in the proof.

(i) For k-module W and any family of k-modules $(X_i)_{i\in I}$, there is a canonical isomorphism $\bigoplus_{i\in I}(W \otimes_k X_i) \xrightarrow{\sim} W \otimes_k \bigoplus_{i\in I} X_i$.

(ii) Let A be a k-module and $E := \mathrm{End}_k(A)$. For any k-module X, the left E-submodules Y' of $A \otimes_k X$ (with E acting on the rst slot) are in bijection with the k-submodules Y of X: set $Y' \leftrightarrow Y$ if $Y' = A \otimes_k Y$.

(iii) Let ${}_EA$ be a module and $k := \mathrm{End}({}_EA)$ so that A becomes an (E, k)-bimodule. For any ${}_EB$, the additive group $\mathrm{Hom}({}_EA, {}_EB)$ is a left k-module: for any $f \in \mathrm{Hom}({}_EA, {}_EB)$ and $\kappa \in k$, let κf be the homomorphism $A \ni a \mapsto (a\kappa)f$ (recall that homomorphisms of left E-modules act on the right). The universal property of $\otimes$ yields a homomorphism of E-modules

$$\Theta : A \otimes_k \mathrm{Hom}({}_EA, {}_EB) \longrightarrow {}_EB$$
$$a \otimes f \longmapsto af$$

where E acts on the rst slot of the left-hand side.

Exercise 9.1.9. Justify these properties.

Proof. As before, we regard B as a left E-module, where $E := A \otimes_k A^{\mathrm{op}}$ acting on B by left and right multiplication. By the previous Lemma, $E \xrightarrow{\sim} \mathrm{End}_k(A)$ is semisimple and simple as a ring, thus every E-module is a direct sum of copies of ${}_EA$. Since $\mathrm{End}({}_EA) = Z(A) = k$, the property (iii) gives a homomorphism of left E-modules

$$\Theta : A \otimes_k \mathrm{Hom}({}_EA, {}_EB) \longrightarrow B.$$

We contend that Θ is an isomorphism. For injectivity, note that $\ker(\Theta) = A \otimes_k Y$ for some k-subspace $Y \subset \mathrm{Hom}({}_EA, {}_EB)$, by the property (ii) above. If $\iota \in Y$ is nonzero, there would exist $a \in A$ with $\Theta(a \otimes \iota) = \iota(a) \neq 0$; hence $\ker(\Theta) = 0$. Now assume ${}_EB = ({}_EA)^{\oplus I}$ for some set I; every $b \in B$ has the form $b = \sum_{i \in I_0} \iota_i(a_i)$ where $I_0 \subset I$ is nite and $\iota_i : A \to B$ is the inclusion into the i-th component. The surjectivity follows as $b = \sum_{i \in I_0} \Theta(a_i \otimes \iota_i)$.

Let us derive (1). Pick a k-basis $\mathcal{B}$ of A. By the foregoing discussions, every $b \in B$ admits a unique expression

$$b = \sum_{\iota \in \mathcal{B}} \iota(a_\iota) = \Theta\left(\sum_{\iota \in \mathcal{B}} a_\iota \otimes \iota \right), \quad a_\iota \in A.$$

In view of the E-module structure on B, we have $b \in Z_B(A)$ if and only if $(a \otimes 1)b = (1 \otimes a)b$ holds true for all $a \in A$; as Θ is E-linear, this amounts to

$$(a \otimes 1)a_\iota = (1 \otimes a)a_\iota, \quad a \in A,\ \iota \in \mathcal{B}.$$

But this is equivalent to $aa_\iota = a_\iota a$, i.e. $a_\iota \in Z(A) = k$. All in all, we have identi ed $C = Z_B(A)$ with the image of $1 \otimes \mathrm{Hom}({}_EA, {}_EB)$ under Θ. The homomorphism Θ is then identi ed with the canonical homomorphism $A \otimes_k C \to B$ given by $a \otimes c \mapsto ac$.

To derive (2), we use the isomorphism Θ and the property (ii) above to show that the E-submodules of B are in bijection with k-subspaces of C: to $I \subset C$ we attach $AI \subset B$. It remains to show that AI is a two-sided ideal of B if and only if I is a two-sided ideal of C: this follows from (1).

The assertion (3) is now clear. □

Let A be a central simple k-algebra and C be any k-algebra. Set $B := A \otimes_k C$. One may check that $C = Z_B(A)$ by choosing a k-basis of C, as in the proof of (1) above. Hence the earlier Theorem is applicable to A, B and C.

Corollary 9.1.10. *Let A be a central simple algebra. For every k-algebra B, the k-algebra $A \otimes_k B$ is simple (resp. central) if and only if B is.*

Theorem 9.1.11. *Let B be a central simple k-algebra and A be a simple subalgebra of B. Every homomorphism $\varphi : A \hookrightarrow B$ of k-algebras can be extended to an automorphism of B which is inner, that is, of the form $x \mapsto y^{-1}xy$ for some $y \in B^\times$.*

Proof. Set $C := A \otimes_k B^{\mathrm{op}}$. It is a nite-dimensional simple k-algebra by the previous Theorem. The Wedderburn-Artin Theorem implies that the left C-modules are classi ed by their dimensions over k.

There are two left C-modules structures on B. One is de ned using the usual left and right multiplications by A and B, respectively. To de ne the other one, let $a \in A$ acts by left multiplication by $\varphi(a)$ and leave the B-action intact. These two C-module structures must be intertwined by some $\ell \in \mathrm{Aut}_k(B)$, namely

$$\ell(x)b = \ell(xb), \quad x, b \in B,$$
$$a\ell(x) = \ell(\varphi(a)x), \quad a \in A,\ x \in B.$$

The rst formula implies that $\ell(x) = yx$ for all x, where $y := \ell(1) \in B^\times$. The second one implies $ay = y\varphi(a)$, or equivalently: $\varphi(a) = y^{-1}ay$. □

Corollary 9.1.12 (Skolem-Noether). *Automorphisms of central simple k-algebras are inner.*

Proof. Take $A = B$ in the previous Theorem. □

Theorem 9.1.13. *Let B be a central simple k-algebra.*

1. *For every semisimple k-subalgebra A of B, we have $Z_B(Z_B(A)) = A$.*
2. *If A is simple, then $Z_B(A)$ is simple. Furthermore, $\dim_k B = \dim_k A \cdot \dim_k Z_B(A)$.*

Proof. The idea is to realize $Z_B(A)$ as an endomorphism algebra and apply the existing results on double centralizers, such as the Density Theorem. Set

$$E_0 := A \otimes_k B^{\mathrm{op}}.$$

This is a semisimple k-algebra. To see this, it su ces to decompose A into simple factors (Wedderburn-Artin theory) and apply Corollary 9.1.10. As before, B can be regarded as a E_0-module using bilateral multiplication; it is semisimple since E_0 is. Set

$$E' := \mathrm{End}({}_{E_0}B).$$

We may identify E' with $Z_B(A)$ which acts on B by left multiplication. Indeed, let $f \in E'$:

- ⋆ commutation with the action of $1 \otimes B^{\mathrm{op}}$ forces f to be $x \mapsto bx$ for some $b \in B$, whilst
- ⋆ commutation with $A \otimes 1$ forces $b \in Z_B(A)$.

The density theorem implies that the natural homomorphism $E_0 \to \mathrm{End}(B_{E'})$ is surjective; it is injective as well by Lemma 9.1.6 applied to B.

Given $x \in Z_B(Z_B(A))$, the endomorphism $b \mapsto xb$ of B commutes with the action of E', hence comes from E_0. The injectivity of $B \otimes_k B^{\mathrm{op}} \to \mathrm{End}_k(B)$ implies that

$$x \otimes 1 \in (B \otimes 1) \cap (A \otimes B^{\mathrm{op}}) = A \otimes 1,$$

proving the inclusion $Z_B(Z_B(A)) \subset A$. The other direction is trivial. This proves (1).

To prove (2), assume the simplicity of A. Then E_0 is simple by Corollary 9.1.10. Let M be the unique simple E_0-module, $D := \mathrm{End}({}_{E_0}M)$, and write ${}_{E_0}B = M^{\oplus r}$, $M = D^{\oplus s}$. It follows that

$$Z_B(A) \simeq E' = \mathrm{End}({}_{E_0}B) \simeq M_r(D)$$

is simple, thereby proving the rst assertion of (2). The dimension equality follows by sorting out the following equations (abbreviation: $\dim = \dim_k$)

$$\begin{aligned} \dim B &= r \cdot \dim M, \\ \dim E_0 &= \dim A \cdot \dim B, \\ \dim M &= s \cdot \dim D, \\ \dim E_0 &= s^2 \dim D, \quad (\text{recall} : E_0 \simeq M_s(D)), \\ \dim Z_B(A) &= r^2 \cdot \dim D. \end{aligned}$$

Thus (2) is proved. □

Exercise 9.1.14. Fill out the details of the last step.

9.2 Splitting elds

Lemma 9.2.1. *For any k-algebra A, there is an isomorphism $A \otimes_k M_n(k) \xrightarrow{\sim} M_n(A)$ between k-algebras.*

Proof. To $a \in A$ and $(\alpha_{ij})_{1\leq i,j\leq n} \in M_n(k)$ we associate $(a\alpha_{ij})_{1\leq i,j\leq n} \in M_n(A)$. □

De nition 9.2.2. Let A be a central simple k-algebra and K be a eld extension of k. We call K a *splitting eld* of A if $A_K := A \otimes_k K \simeq M_n(K)$ as K-algebras. We call A *split* if $A \simeq M_n(k)$ for some n.

By writing $A \simeq M_n(D)$, one sees that splitting elds exist; for example, we may take K to be an algebraic closure of k in order to split D. We will prove much stronger results on splitting elds.

In what follows, a "sub eld" in a k-algebra A will always mean a k-subalgebra of A which is a eld.

Lemma 9.2.3. *Let A be a central simple k-algebra and L be a sub eld of A. Set $A_L := A \otimes_k L$ and $C := Z_A(L)$, there exist m, n such that $M_m(A_L) \simeq M_n(C)$ as L-algebras.*

Note that C is a central simple L-algebra. Indeed, the simplicity of C follows from Theorem 9.1.13; furthermore, it implies that

$$L \subset Z(C) \subset Z_A(C) = Z_A(Z_A(L)) = L.$$

It is probably better to write $A_L \sim C$ using the notion of similarity between central simple L-algebras; cf. De nition 9.3.1.

Proof. Make A into a left $A_L = A \otimes_k L$-module by bilateral multiplication as usual (note that $L = L^{\mathrm{op}}$). As observed in the proof of Theorem 9.1.13, $\mathrm{End}({}_{A_L}A) \simeq C$ (acting by right multiplication).

Lemma 9.1.7 asserts that A_L is a central simple L-algebra. The unique simple A_L-module is nite-dimensional over L (it is a quotient of A_L — choose a generator!); let D be its endomorphism algebra, which is also nite-dimensional. For every A_L-module M of nite dimension over L, there exists d such that $\mathrm{End}({}_{A_L}M) \simeq M_d(D)$. Applying this to the left A_L-modules A and A_L yields the required result. □

Proposition 9.2.4. *Let D be a central division k-algebra, then every maximal sub eld L of D is a splitting eld of D. Furthermore, $[L : k]^2 = \dim_k D$.*

Proof. Note that $Z_D(L) = L$ by the maximality of L. The previous Lemma implies that $M_m(D_L) \simeq M_n(L)$ for some m, n. By the uniqueness part in the Wedderburn-Artin theory for semisimple simple L-algebras, we see that $D_L \simeq M_d(L)$ for some d. The second assertion follows from the dimension equality in Theorem 9.1.13. □

Remark 9.2.5. Maximal sub elds of D are NOT unique in general. Counterexamples appear naturally in the case of quaternion algebras, cf. De nition 9.6.1.

The next result is crucial. It will allow us to apply the technique of Galois descent to study central simple algebras.

Figure 9.1: Richard D. Brauer (1901-1977) together with Barthel L. van der Waerden (left). Source: Oberwolfach Photo Collection.

Theorem 9.2.6. *Let A be a central simple k-algebra, then A splits over a separable finite extension of k. More precisely, every central division k-algebra D contains a maximal subfield which is separable.*

Proof. The second assertion implies the first one by Proposition 9.2.4. Let D be a central division k-algebra and L be a maximal separable subfield of D. We have to show that L is actually a maximal field.

Let $C := Z_D(L)$ so that C is a division L-algebra; it is central by Theorem 9.1.13. If L is not a maximal subfield, then $C \supsetneq L$ and the following Lemma 9.2.7 would exhibit a separable extension $L' \supsetneq L$ in C, contradicting the maximality of L. □

Lemma 9.2.7. *Let k be a field and let D be a central division k-algebra. If $D \neq k$, then D contains a separable extension $L \supsetneq k$.*

Proof. The following proof is due to Artin. Let $N := \dim_k D$, $N > 1$. Every $\xi \in D$ generates a field extension $k(\xi)$ of k with $[k(\xi) : k] | N$. The extension can be decomposed into $k(\xi) \supset k(\xi)_s \supset k$ with $k(\xi)/k(\xi)_s$ *purely inseparable* and $k(\xi)_s/k$ separable. If D contains no separable extension other than k itself, then

- ⋆ k has characteristic $p > 0$;
- ⋆ for every $\xi \in D$, we would have $k(\xi)_s = k$, thus $\xi^{p^d} \in k$ for some $d \in \mathbb{Z}_{\geq 1}$;
- ⋆ k is infinite (otherwise $k^p = k$, forcing $D = k$ by the previous condition).

Let q be the highest power of p divides N. As the inseparable degree $[k(\xi) : k]_i$ divided N, we have $\xi^q \in k$ for every $\xi \in D$. The next step is to write

$$D = E \oplus k \cdot 1, \quad \text{for some } E \subset D$$

as k-vector spaces. Let $\mathrm{pr} : D \twoheadrightarrow E$ be the corresponding k-linear projection. Note that we may identify $D \simeq k^N$, $E \simeq k^{N-1}$ upon choosing bases, and regard them as affine k-spaces. Then $\mathrm{pr} : D \to E$ is a polynomial map. On the other hand, the q-th power map

$\xi \mapsto \xi^q$ from D to itself is also a polynomial map. All in all, $\xi \mapsto \mathrm{pr}(\xi^q)$ is polynomial map, denoted as $Q : D \to E$. We have $\xi^q \in L \iff Q(\xi) = 0$, thus

$$Q(\xi) = 0, \quad \forall \xi \in D. \tag{9.1}$$

Write $Q = (f_1, \ldots, f_{N-1})$ in coordinates, where $f_i \in k[X_1, \cdots, X_n]$. The upshot is that (9.1) implies that the polynomials $f_1, \ldots, f_{N-1}$ are identically zero, since k is an in - nite eld [1]. But now we can change the base eld k to a splitting eld L of D, obtaining the polynomial map $Q_L : D_L \to E_L$ in the same manner. More precisely, we have $Q_L = (f_1, \ldots, f_{N-1})$ in coordinates where those f_i are now viewed as elements of $L[X_1, \ldots, X_N]$. Hence we still have

$$Q_L(\xi) = \mathrm{pr}(\xi^q) = 0, \quad \forall \xi \in D_L = M_n(L).$$

Therefore $\xi^q \in L \cdot 1$ for all $\xi \in M_n(L)$. This is impossible when $n = \sqrt{N} > 1$: take ξ to be the diagonal matrix with entries $(1, 0, \ldots, 0)$, for instance. □

Another proof using derivations, due to I. N. Herstein, can be found in [12, §8.8].

9.3 Brauer groups

De nition 9.3.1. Let A and B be central simple k-algebras. We say that A is similar to B, written as $A \sim B$, if there exist $n, m \in \mathbb{Z}_{\geq 1}$ such that $M_n(A) \simeq M_m(A)$.

This de nes an equivalence relation. If A and B are central division k-algebras, then $A \sim B$ if and only if $A \simeq B$ by our earlier discussion on the Wedderburn-Artin theory. Also note that Lemma 9.2.1 implies

$$A \sim A' \quad \Rightarrow A \otimes_k B \sim A' \otimes_k B.$$

De nition-Proposition 9.3.2. Let $\mathrm{Br}(k)$ be the monoid formed by the similarity classes central simple k-algebras, the multiplication being given by $\otimes$-products and the units being the class of k. Then $\mathrm{Br}(k)$ is a commutative group, called the *Brauer group* of k.

In view of Lemma 9.2.1, this amounts to inverting the $M_n(k)$'s in the monoid (under $\otimes$) of isomorphism classes of central simple k-algebras.

Proof. The commutativity follows from the isomorphism between k-algebras

$$\begin{aligned} A \otimes_k B &\longrightarrow B \otimes_k A \\ a \otimes b &\longmapsto b \otimes a. \end{aligned}$$

To show that $\mathrm{Br}(k)$ is a group, it remains to exhibit the inverses. Indeed we may de ne the inverse $[A]^{-1}$ of the class $[A]$ as A^{op}; we have $A \otimes_k A^{\mathrm{op}} \sim k$ by Lemma 9.1.6. □

Exercise 9.3.3. Justify the following statements.

[1] In the parlance of algebraic geometry, we used the fact that the k-points in a ne k-spaces are Zariski dense.

1. $\mathrm{Br}(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$, the nontrivial element being represented by Hamilton's quaternion algebra. **Hint**: use Frobenius' theorem for real division algebras.

2. If k is a finite field, then $\mathrm{Br}(k)$ is trivial. **Hint**: by a celebrated theorem of Wedderburn, finite division rings are just fields.

3. If k is separably closed, then $\mathrm{Br}(k)$ is trivial.

Remark 9.3.4. The vanishing of $\mathrm{Br}(k)$ holds for an important class of fields called C_1 fields, such as the function fields of algebraic curves over an algebraically closed field (Tsen-Lang theorem). We recommend [7] for a very readable account on central simple algebras, C_1 fields and the life of its creator Zeng Jiongzhi (1898-1940).

For any field extension K of k, the map $A \mapsto A_K := A \otimes_k K$ induces a group homomorphism

$$\mathrm{Br}(k) \to \mathrm{Br}(K).$$

Denote its kernel by $\mathrm{Br}(K/k)$. It is the subgroup of $\mathrm{Br}(k)$ of elements which split over K. By Theorem 9.2.6 we deduce

$$\mathrm{Br}(k) = \bigcup_{K/k:\ \text{finite Galois}} \mathrm{Br}(K/k).$$

Exercise 9.3.5. Show that $(A \otimes_k B)_K \simeq A_K \otimes_K B_K$ for all central simple k-algebras A, B. Thus $[A] \mapsto [A_K]$ is indeed a well-defined group homomorphism.

Let K be a finite Galois extension of k. Let $n \in \mathbb{Z}_{\geq 1}$ and denote by $\mathrm{CSA}_n(K/k)$ the isomorphism classes of central simple k-algebras of dimension n^2 that split over K. We shall describe $\mathrm{CSA}_n(K/k)$ using the technique of *Galois descent*. Let $A \in \mathrm{CSA}_n(K/k)$, the idea is to compare A with its split avatar $M_n(k) \in \mathrm{CSA}_n(K/k)$.

Choose an isomorphism $f : A_K \xrightarrow{\sim} M_n(K)$ over K and recall that $\mathrm{Gal}(K/k)$ acts on A_K and $M_n(K)$ through its action on K. For every $\sigma \in \mathrm{Gal}(K/k)$, set

$${}^{\sigma}f := \sigma \circ f \circ \sigma^{-1}.$$

Define $\mathrm{GL}_n(K)$ as the group of invertible elements in $M_n(K)$ and define $\mathrm{PGL}_n(K) := \mathrm{GL}_n(K)/K^{\times}$. The group $\mathrm{PGL}_n(K)$ acts faithfully on $M_n(K)$ by the adjoint action $\mathrm{Ad}(g) : X \mapsto gXg^{-1}$.

Exercise 9.3.6. Use Skolem-Noether Theorem (Corollary 9.1.12) to show that there exists a unique map $\sigma \mapsto c_\sigma \in \mathrm{PGL}_n(K)$, for $\sigma \in \mathrm{Gal}(K/k)$, such that

$${}^{\sigma}f = \mathrm{Ad}(c_\sigma) \circ f.$$

Show that

$$c_{\sigma\tau} = \sigma(c_\tau)c_\sigma, \quad \sigma, \tau \in \mathrm{Gal}(K/k). \tag{9.2}$$

The functions $c : \mathrm{Gal}(K/k) \to \mathrm{PGL}_n(K)$ satisfying (9.2) are called 1-cocylces with values in $\mathrm{PGL}_n(K)$.

Exercise 9.3.7. Call two 1-cocycles c, c' with values in $\mathrm{PGL}_n(K)$ equivalent if there exists $b \in \mathrm{PGL}_n(K)$ such that

$$c'_\sigma = \sigma(b) c_\sigma b^{-1}, \quad \sigma \in \mathrm{Gal}(K/k).$$

Denote by $H^1(K/k, \mathrm{PGL}_n)$ the set of equivalence classes of 1-cocycles with values in $\mathrm{PGL}_n(K)$. Show that the class $[c]$ of the 1-cocycle constructed above is independent of the choice of f.

Exercise 9.3.8. Deduce a canonical bijection from $\mathrm{CSA}_n(K/k)$ onto $H^1(K/k, \mathrm{PGL}_n)$, under which $M_n(k)$ is mapped to the distinguished element represented by the constant function . Use Theorem 9.4.1 if need be.

Remark 9.3.9. To obtain a cohomological description of the group $\mathrm{Br}(K/k)$, we have to pass to another object $H^2(K/k, \mathbb{G}_\mathrm{m})$ and play with 2-cocycles. Moreover, the Brauer group $\mathrm{Br}(k)$ can be shown to be isomorphic to $H^2(k, \mathbb{G}_\mathrm{m}) = \varinjlim_{K/k} H^2(K/k, \mathbb{G}_\mathrm{m})$. This approach requires either more involved cohomological machineries, or a complicated construction of cross-products. We will not go into the details.

Remark 9.3.10. There is an important generalization of central simple algebras called *Azumaya algebras*, by allowing k to be a commutative local ring. Likewise the Brauer group can be de ned in this context. This makes it possible to de ne the Brauer group in algebraic geometry, namely a group $\mathrm{Br}(X)$ of a *scheme* X in terms of Azumaya $\mathcal{O}_X$-algebras. It has an interpretation via étale cohomology, and becomes a useful vehicle for studying the rational points on algebraic varieties in the hands of Yu I. Manin.

9.4 Rational structure on vector spaces

This section serves as a preparation for the study of reduced norms and traces of central simple algebras.

Let k be a eld and K be a Galois extension of k, possibly of in nite degree. Write $\Gamma := \mathrm{Gal}(K/k)$. The category of K-vector spaces is denoted by $\mathbf{Vect}_K$.

Given a K-vector space W, a Galois action on W is an action of Γ on W such that

- ⋆ for every $\sigma \in \Gamma$ and $t \in K$, $w \in W$, we have $\sigma(tw) = \sigma(t)\sigma(w)$;
- ⋆ $W = \bigcup_{\Gamma'} W^{\Gamma'}$ where Γ' ranges over the subgroups of Γ of nite index, and $W^{\Gamma'}$ is the k-subspace of Γ'- xed elements.

For a K-linear homomorphism $f : W \to W'$ between K-vector spaces endowed with Galois actions, we set

$${}^\sigma f := \sigma \circ f \circ \sigma^{-1}$$

which is still K-linear. We say f is Γ-equivariant if ${}^\sigma f = f$ for every $\sigma \in \Gamma$. The K-vector spaces together with the Γ-equivariant homomorphisms form a category $\mathbf{Vect}_{K,\Gamma}$.

If V is a k-vector space, then $V_K := V \otimes_k K$ is equipped with the obvious Galois action, say by letting Γ act on K. We can recover V since $(V_K)^\Gamma = V \otimes_k 1 = V$.

Theorem 9.4.1. *The functor*

$$\begin{aligned} \mathbf{Vect}_k &\longrightarrow \mathbf{Vect}_{K,\Gamma} \\ V &\longmapsto V \otimes_k K \end{aligned}$$

is an equivalence; a quasi-inverse is given by $W \mapsto W^\Gamma$.

Proof. Given an object W of $\mathbf{Vect}_{K,\Gamma}$, we set $V := W^\Gamma$. There is a natural homomorphism $V \otimes_k K \to W$ in $\mathbf{Vect}_{K,\Gamma}$. We shall prove its injectivity first.

The kernel W' of $V \otimes_k K \to W$ is a Γ-stable subspace of $V \otimes_k K$ whose intersection with $V \otimes 1$ is zero. Claim: such a subspace W' must be zero. Indeed, choose a k-basis $\{e_i\}_{i\in I}$ for V. Choose a nonzero element $w \in W'$ whose expression $w = \sum_i a_i e_i$ is as short as possible. To simplify the notations, let us assume $I = \mathbb{Z}_{\geq 1}$. We may arrange that $w = e_1 + a_2 e_2 + \cdots$ and $a_2 \notin k$. By choosing $\sigma \in \Gamma$ such that $\sigma(a_2) \neq a_2$, we get $w - \sigma(w) \in W' \smallsetminus \{0\}$ with a shorter expression in $e_1, e_2, \ldots$. Contradiction.

As for the surjectivity, let $w \in W^{\Gamma'}$ for $\Gamma' = \mathrm{Gal}(K/k')$ where k'/k is a finite extension. Upon enlarging k' we may assume k'/k Galois of degree n. Let $a_1, \ldots, a_n$ be a k-basis of k' and enumerate the elements of $\mathrm{Gal}(k'/k)$ as $1 = \sigma_1, \sigma_2, \ldots, \sigma_n$. From the linear independence of characters [16, p.284], $(\sigma_j(a_i))_{i,j}$ is an invertible $n \times n$-matrix over k' whose inverse we denote by $(b_{ij})_{i,j}$. Now:

$$w = 1 \cdot w = \sum_{j=1}^{n} \delta_{j,1}\sigma_j(w) = \sum_{i,j=1}^{n} \sigma_j(a_i) b_{i,1} \sigma_j(w) = \sum_{i=1}^{n} b_{i,1} \underbrace{\left(\sum_{j=1}^{n} \sigma_j(a_i)\sigma_j(w) \right)}_{\in (W^{\Gamma'})^{\mathrm{Gal}(k'/k)} = W^\Gamma = V}$$

where $\delta_{j,1}$ is Kronecker's δ. Thus $W = V \otimes_k K$. To establish the equivalence between categories, it remains to show the bijectivity of

$$\mathrm{Hom}_k(V_1, V_2) \to \mathrm{Hom}_K(V_1 \otimes_k K, V_2 \otimes_k K)^{\Gamma-\text{equivariant}}$$

for $V_1, V_2 \in \mathbf{Vect}_k$, by categorical nonsense. This can be readily checked, for example by expressing the linear maps in terms of k-bases. □

9.5 Reduced norms and reduced traces

Proposition 9.5.1. *Let A be a central simple k-algebra of dimension n^2. There are canonical polynomial maps over k*

$$\mathrm{Trd} : A \to k,$$
$$\mathrm{Nrd} : A \to k$$

such that

1. Trd *is k-linear and* $\mathrm{Trd}(xy - yx) = 0$ *for every $x, y \in A$;*
2. Nrd *is multiplicative, homogeneous of degree n, sending* 1 *to* 1*;*
3. *for every splitting field K of A and $F_K : A_K \xrightarrow{\sim} M_n(K)$, we have* $\mathrm{Trd} = \mathrm{Tr} \circ F_L|_A$ *and* $\mathrm{Nrd} = \det \circ F_L|_A$*, where* Tr *and* det *are the usual trace and determinant maps of $M_n(K)$.*

These maps are certainly uniquely determined, called the *reduced trace* and the *reduced norm* of A, respectively.

Proof. In view of Theorem 9.2.6, we may start from the case in which K is a separable closure of k. De ne $T := \mathrm{Tr} \circ F_K$ and $N := \det \circ F_K$ as in the statement 3. They are polynomial maps over K from A_K to K; we want to show that T and N descend to k, that is, there exist polynomial maps over k from A to k, which give rise to T and N after a change of base eld K/k. The idea is to apply Theorem 9.4.1 to the vector spaces of such polynomial functions.

By Corollary 9.1.12, for every $\sigma \in \mathrm{Gal}(K/k)$ we have

$$ {}^{\sigma}F_K := \sigma \circ F_K \circ \sigma^{-1} = \mathrm{Ad}(c_\sigma) \circ F_K $$

for some $c_\sigma \in \mathrm{PGL}_n(K)$, where

- ⋆ σ is taken relative to the k-structure $M_n(k)$ for $M_n(K)$,
- ⋆ σ^{-1} is taken relative to the k-structure A for A_K, and
- ⋆ $\mathrm{Ad}(c_\sigma) : X \mapsto c_\sigma X c_\sigma^{-1}$ is the adjoint action.

Since Tr and det are de ned over k and invariant under conjugation, we see ${}^{\sigma}T = T$ and ${}^{\sigma}N = N$. Hence T and N are de ned over k. The required properties in statements 1 and 2 follow immediately.

The same holds when K contains a separable closure of k. Now let K be any splitting eld of A. By adjoining the roots of separable polynomials into K, we may pass to a eld $K' \supset K$ that contains a separable closure of k. We have

$$\begin{array}{ccc} A_{K'} & \xrightarrow{F_{K'}} & M_n(K') \\ \uparrow & & \uparrow \text{extension of scalars} \\ A_K & \xrightarrow[F_K]{} & M_n(K) \end{array}$$

and the required properties follow from the previous case. □

The adjective "reduced" is explained by the following.

Corollary 9.5.2. *Keep the notations above. Let $a \in A$ and de ne endomorphisms of the k-vector space A as follows*

$$ L_a : x \mapsto ax, $$
$$ R_a : x \mapsto xa. $$

Then we have

$$ \mathrm{Tr}(R_a) = \mathrm{Tr}(L_a) = n\mathrm{Trd}(a) $$
$$ \det(R_a) = \det(L_a) = \mathrm{Nrd}(a)^n. $$

Proof. It su ces to check this on a splitting eld, thus we may assume $A = M_n(k)$. The remaining arguments are straightforward. □

We also write Trd_A, Nrd_A to emphasize the reference to A, if need be.

Exercise 9.5.3. Show that $a \in A^\times$ if and only if $\mathrm{Nrd}_A(a) \neq 0$.

Exercise 9.5.4. Let D be a central division k-algebra and $A = M_n(D)$.

1. For an upper-triangular matrix $X = (x_{ij}) \in A$, show that $\mathrm{Trd}_A(X) = \sum_{i=1}^{n} \mathrm{Trd}_D(x_{ii})$ and $\mathrm{Nrd}_A(X) = \prod_{i=1}^{n} \mathrm{Nrd}_D(x_{ii})$.

2. For a permutation matrix X, show that $\mathrm{Nrd}(X) = \pm 1$.

3. Show that $\mathrm{Nrd}_A(A^\times) = \mathrm{Nrd}_D(D^\times)$.

9.6 Example: quaternion algebras

You are probably familiar with Hamilton's quaternion algebra. It is the central division $\mathbb{R}$-algebra $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$, subject to the multiplication law

$$\begin{aligned} i^2 = j^2 = k^2 &= -1, \\ ij = -ji &= k, \\ jk = -kj &= i, \\ ki = -ik &= j. \end{aligned}$$

Up to isomorphism, this is the only finite-dimensional division $\mathbb{R}$-algebra besides $\mathbb{C}$ and $\mathbb{R}$ (Frobenius' theorem). Let us generalize this construction over any field F of characteristic $\neq 2$.

Definition 9.6.1. Let F be a field of characteristic $\neq 2$. Let $a, b \in F^\times$, the corresponding *quaternion algebra*, denoted by $\left(\frac{a,b}{F}\right)$, is the F-algebra $F \oplus Fi \oplus Fj \oplus Fk$ whose multiplication table is determined by

$$\begin{aligned} i^2 = a,\ j^2 &= b, \\ ij = -ji &= k. \end{aligned}$$

Proposition 9.6.2. *Let $a, b \in F^\times$. Then $\left(\frac{a,b}{F}\right)$ is a central simple F-algebra, and the following statements are equivalent.*

1. *The equation $x^2 - ay^2 - bz^2 + abw^2 = 0$ has a solution in $F^4 \smallsetminus \{(0,0,0,0)\}$.*

2. *The F-algebra $\left(\frac{a,b}{F}\right)$ is not a division algebra.*

3. $\left(\frac{a,b}{F}\right) \simeq M_2(F)$.

Proof. Observe that for every $r, s \in F^\times$ we have $\left(\frac{a,b}{F}\right) \xrightarrow{\sim} \left(\frac{ar^2,bs^2}{F}\right)$: simply use the homomorphism $1 \mapsto 1$, $i \mapsto ri$, $j \mapsto sj$ and $k \mapsto rsk$. Next, we have $\left(\frac{1,-1}{F}\right) \simeq M_2(F)$ by sending

$$\begin{aligned} i &\mapsto E_{01} + E_{10}, \\ j &\mapsto E_{01} - E_{10}, \\ k &\mapsto E_{11} - E_{00}, \end{aligned}$$

in our notation for matrices in Lecture 7. Recall that an F-algebra A is central simple if and only if $A_E := A \otimes_F E$ is central simple over E, for any field extension E (Lemma

9.1.7). We may pass to a nite extension E/F in which $a, -b \in E^{\times 2}$, so that $\left(\frac{a\ b}{F}\right) \otimes_F E = \left(\frac{a\ b}{E}\right) \simeq M_2(E)$, hence $\left(\frac{a\ b}{F}\right)$ is central simple over F.

(1) $\Rightarrow$ (2). Set $\tau(x + yi + zj + wk) := x - yi - zj - wk$. We leave it to the reader to check that τ is an F-linear anti-automorphism of $\left(\frac{a\ b}{F}\right)$, i.e. $\tau : \left(\frac{a\ b}{F}\right) \xrightarrow{\sim} \left(\frac{a\ b}{F}\right)^{\mathrm{op}}$. Now put

$$N(\alpha) := \alpha\tau(\alpha), \quad x + yi + zj + wk \mapsto x^2 - ay^2 - bz^2 + abw^2 \in F.$$

One readily checks that N de nes a multiplicative map $\left(\frac{a\ b}{F}\right) \to F$ such that $N(1) = 1$, $N(0) = 0$. If $x^2 - ay^2 - bz^2 + abw^2 = 0$ with $(x, y, z, w) \neq (0, 0, 0, 0)$, then $\alpha := x + yi + zj + wk$ is nonzero and satis es $N(\alpha) = 0$, hence is not invertible in $\left(\frac{a\ b}{F}\right)$.

(2) $\Rightarrow$ (3). Since $\left(\frac{a\ b}{F}\right)$ is 4-dimensional, this is an immediate consequence of the structure theory of central simple algebras.

(3) $\Rightarrow$ (1). Suppose that the only solution of $x^2 - ay^2 - bz^2 + abw^2 = 0$ in F^4 is $(0, 0, 0, 0)$. Every $\alpha = x + yi + zj + wk \neq 0$ is then invertible with $\alpha^{-1} = N(\alpha)^{-1}\tau(\alpha)$ since $N(\alpha) \neq 0$. □

Remark 9.6.3. One may check that the map N is exactly the reduced norm of $\left(\frac{a\ b}{F}\right)$.

Conversely, the quaternion algebras exhaust all 4-dimensional central simple F-algebras.

Theorem 9.6.4 (Wedderburn)**.** *Every 4-dimensional central simple F-algebra A is isomorphic to $\left(\frac{a\ b}{F}\right)$ for some $a, b \in F^\times$.*

Proof. We may assume that A is a central division algebra since $M_2(F) \simeq \left(\frac{1\ -1}{F}\right)$. Let E be a maximal sub eld of A; we have $E = F[i] \subset A$ for some element i satisfying $i^2 = a \in F^\times$. Therefore the inner automorphism $\sigma : x \mapsto ixi^{-1}$ of A is an involution (i.e. $\sigma^2 = \mathrm{id}$). Furthermore $\sigma \neq \mathrm{id}$, otherwise we would have $i \in Z(A) = F$. Thus the (-1)-eigenspace of σ is nontrivial, say $\sigma(j) = -j$ for some $j \in A \smallsetminus F$. Let $K = F[j] \subset A$. Note that E and K are quadratic extensions of F.

Consequently, $\sigma(K) = K$ but $\sigma|_K \neq \mathrm{id}$. It follows that $j^2 = b$ for some $b \in F^\times$. Finally put $k := ij \in A$. All the relations de ning $\left(\frac{a\ b}{F}\right)$ are veri ed and it remains to show that $1, i, j, k$ are linearly independent over F. It is left to the reader to show that, if $x + yi + zj + wk = 0$, conjugation by i, j and k yields the extra relations

$$\begin{aligned} x + yi - zj - wk &= 0 \\ x - yi + zj - wk &= 0 \\ x - yi - zj + wk &= 0. \end{aligned}$$

The required linear independence follows at once. □

Remark 9.6.5. For $a, b \in F^\times$, let $(a, b)_F \in \mathrm{Br}(F)$ be the class of $\left(\frac{a\ b}{F}\right)$. In view of the preceding results, the classi cation of 4-dimensional central simple F-algebras boils down to describe all the relations among the classes $(a, b)_F$ in $\mathrm{Br}(F)$. For general F, the map $(a, b) \mapsto (a, b)_F$ factors through a bi-additive map

$$(F^\times/F^{\times 2}) \times (F^\times/F^{\times 2}) \to \mathrm{Br}(F)$$

and satis es $(x, y)_F = 1$ if $x + y = 1$ – this immediately suggests some relationship to algebraic K-theory. When F is a local eld, $(a, b)_F$ can be identi ed with the quadratic *Hilbert symbol* of F.

The theory of central simple algebras have intimate connections with quadratic and hermitian forms. For example, the double centralizer theorems re ect analogous classical construction for quadratic forms. Due to time constraints, we will not dive into the details. The interested reader may consult [23] for details.

LECTURE 10

MORITA THEORY

10.1 Review of categorical nonsense

The category of abelian groups is denoted by **Ab**.

Let R be a ring, the category of left (resp. right) R-modules is denoted by R-**Mod** (resp. **Mod**-R). Similarly, given a pair of rings (R, S), we may de ne the category of (R, S)-bimodules (R, S)-**Mod**: it is equivalent to the category $R \underset{\mathbb{Z}}{\otimes} S^{\mathrm{op}}$-**Mod**.

We shall work exclusively with the category R-**Mod**; the other cases can be deduced by considering the opposite rings. Unless otherwise speci ed, R-modules will always mean left R-modules.

The category R-**Mod** is an *abelian category*, meaning that it is an *additive category* in which every morphism is *strict* and admits kernels and cokernels. These wordings should not bother us here: it su ces to notice that it makes sense to talk about short exact sequences

$$0 \to M' \to M \xrightarrow{f} M'' \to 0$$

in an abelian category; here $M' = \ker(f)$ and $M'' = \mathrm{im}(f)$. All these are already familiar in the case of R-**Mod**.

De nition 10.1.1. In an abelian category C, an object P is called *projective* if the functor $\mathrm{Hom}(P, -) : C \to \mathbf{Ab}$ is exact. That is, for every short exact sequence

$$0 \to M' \to M \to M'' \to 0$$

in C, the sequence

$$0 \to \mathrm{Hom}(P, M') \to \mathrm{Hom}(P, M) \to \mathrm{Hom}(P, M'') \to 0$$

is exact in **Ab**. Note that $\mathrm{Hom}(P, -)$ is only *left exact* for general P: we only have the exactness of $0 \to \mathrm{Hom}(P, M') \to \mathrm{Hom}(P, M) \to \mathrm{Hom}(P, M'')$ in **Ab**.

An R-module M is called *free* if $M \simeq {}_R R^{\oplus I}$ for some indexing set I. Free modules are projective.

Proposition 10.1.2. *For an object P of R-**Mod**, the following statements are equivalent.*

1. *P is projective;*
2. *Every short exact sequence $0 \to M' \to M \xrightarrow{f} P \to 0$ in R-**Mod** splits, that is, there exists $s : P \to M$ such that $f \circ s = \mathrm{id}$;*
3. *P is a direct summand of some free R-module.*

Proof. (1) $\Rightarrow$ (2). Take s to be an inverse image of id under the surjection $\mathrm{Hom}(P, M) \to \mathrm{Hom}(P, P)$.

(2) $\Rightarrow$ (3). There exists a surjection $f : R^{\oplus I} \twoheadrightarrow P$ for some indexing set I. Now apply (1) to get $(f, 1 - s \circ f) : R^{\oplus I} \xrightarrow{\sim} P \oplus \ker(f)$.

(3) $\Rightarrow$ (1). We may assume that $R^{\oplus I} = P \oplus M$, then

$$\mathrm{Hom}(R^{\oplus I}, -) = \mathrm{Hom}(P, -) \oplus \mathrm{Hom}(M, -).$$

The functor on the left-hand side is known to be exact, hence $\mathrm{Hom}(P, -)$ and $\mathrm{Hom}(M, -)$ are both exact. □

We remark that when P is a projective and finitely generated left R-module, P can actually be realized as a direct summand of ${}_R R^{\oplus n}$ for some $n \in \mathbb{Z}_{\geq 1}$; this is clear from the proof above.

Exercise 10.1.3 (Eilenberg's trick)**.** Show that, in the statement 3 above, we may actually take a free R-module F such that $F \simeq P \oplus F$. **Hint**: suppose that $P \oplus M$ is free for some M; take the countable direct sum $F := (M \oplus P) \oplus (M \oplus P) \oplus \cdots$.

Definition 10.1.4. In an abelian category C admitting inductive limits[1] (eg. R-**Mod**, the uninterested reader may skip the extra generality here), there are two generalizations of *finite generation* of an object M:

(i) For any family of subobjects $\{M_i : i \in I\}$ of M such that $\sum_{i \in I} M_i = M$, we have $\sum_{i \in I_0} M_i = M$ for some finite subset I_0 of I.

(ii) For any chain of subobjects $\{M_i : i \in I\}$ of M (i.e. totally ordered by inclusion), we have $\sum_{i \in I} M_i \neq M$ if $M_i \neq M$ for any $i \in I$.

Here I denotes an indexing set. We may call (i) as "compactness" (topological notion) whereas (ii) as "finite type" (algebraic notion).

Theorem 10.1.5. *The conditions (i) and (ii) are equivalent. In the category R-**Mod** they are both equivalent to the finite generation of an R-module.*

Proof. The equivalence of (i) and finite generation in R-**Mod** is easy. (i) $\Longrightarrow$ (ii): Assume $\sum_{i \in I} M_i = M$ holds for the chain $(M_i)_{i \in I}$. Let I_0 be given by (i), we have $M_{\max(I_0)} = M$.

(ii) $\Longrightarrow$ (i): Consider a set J of subobjects of M such that J is closed under $\sum$ and $M \in J$. Let $J' := J \setminus \{M\}$. These sets are partially ordered by inclusion. Condition (ii) entails that every chain in $(J', \leq)$ has its sum in J'. It suffices to show that for every subset $\varnothing \neq I \subset J'$ we have $\sum_{i \in I} M_i \notin J \implies \sum_{i \in I_0} M_i \notin J$ for some finite subset $I_0 \subset I$. This is a set-theoretic property: see [21, §4.7, Lemma 1] for a proof. □

[1] The standard practice seems to be working with Grothendieck categories, and we have to choose an "universe" as well. The inductive limits are then assumed to be *small*. Let us forget about these technical details

De nition 10.1.6. Let P be an object in an abelian category C.

- ⋆ P is called a *generator* if $\mathrm{Hom}(P, -)$ is a faithful functor from C to **Ab**, i.e. it is injective on the Hom-sets. Explicitly, we require that for given objects M, M' and every nonzero $f \in \mathrm{Hom}(M, M')$, there exists $g \in \mathrm{Hom}(P, M)$ such that $\mathrm{Hom}(P, f)(g) = f \circ g \in \mathrm{Hom}(P, N)$ is nonzero.
- ⋆ P is called a *progenerator* if P is projective, nitely generated (in the sense of De nition 10.1.4) and is a generator.

Example 10.1.7. The free R-modules are progenerators in R-**Mod**. It su ces to check this for the free R-module ${}_RR$. Note that $\mathrm{Hom}({}_RR, M) = M$ for every M.

Remark 10.1.8. By the Freyd-Mitchell Theorem, any small abelian category C is equivalent to a full abelian subcategory of R-**Mod**, for some ring R. It is perhaps worth mentioning that the proof of the Freyd-Mitchell theorem relies on taking appropriate generators.

Let us take a closer look at the case the category of R-modules.

De nition 10.1.9. Let M be an R-module. The *trace ideal* of M is de ned as

$$\mathrm{Tr}(M) := \sum_{f \in \mathrm{Hom}(M, {}_RR)} \mathrm{im}(f) \quad \subset R.$$

This is a two-sided ideal of R. Indeed, suppose that $r = \sum_{i=1}^n f_i(m_i)$ for some $f_i : M \to {}_RR$ and $m_i \in M$, $i = 1, \ldots, n$. For any $s \in R$, we have

$$sr = \sum_{i=1}^n f_i(sm_i) \in \mathrm{Tr}(M),$$
$$rs = \sum_{i=1}^n (f_i s)(m_i) \in \mathrm{Tr}(M),$$

where $f_i s \in \mathrm{Hom}(M, {}_RR)$ means f_i followed by the right multiplication by s.

Proposition 10.1.10. *Let P be an R-module. The following statements are equivalent.*

1. *P is a generator in R-**Mod**.*
2. *$\mathrm{Tr}(P) = R$.*
3. *${}_RR$ is a quotient of $P^{\oplus I}$ for some nite indexing set I.*
4. *${}_RR$ is a quotient of $P^{\oplus I}$ for some indexing set I.*
5. *Every R-module M is a quotient of $P^{\oplus I}$, for some indexing set I depending on M.*

Proof. (1) ⇒ (2). Let $\mathfrak{a} := \mathrm{Tr}(P)$. If $\mathfrak{a} \neq R$, then $R \to R/\mathfrak{a}$ is a nonzero morphism in R-**Mod**. By the de nition of generators, there must exist $g \in \mathrm{Hom}(P, {}_RR)$ such that the composition $P \xrightarrow{g} R \to R/\mathfrak{a}$ is nonzero. This would imply that $\mathrm{im}(g) \not\subset \mathfrak{a}$, which is absurd.

(2) ⇒ (3). By assumption, there exists $g_1, \ldots, g_n \in \mathrm{Hom}(P, {}_RR)$ such that

$$\sum_{i=1}^n \mathrm{im}(g_i) = R;$$

indeed it su ces that the sum of images contains $1 \in R$. Hence we obtain an epimorphism $P^{\oplus n} \twoheadrightarrow {}_R R$.

(3) $\Rightarrow$ (4). Trivial.

(4) $\Rightarrow$ (5). Every M is a quotient of some free R-module.

(5) $\Rightarrow$ (1). Let $f : M \to N$ be some nonzero morphism in R-**Mod**. There exists an epimorphism $\psi = (\psi_i)_{i\in I} : P^{\oplus I} \twoheadrightarrow M$ for some I, where $\psi_i \in \mathrm{Hom}(P, M)$. The composition $(f \circ \psi_i)_{i\in I} : P^{\oplus I} \to M \to N$ is nonzero, hence $f \circ \psi_i \neq 0$ for some $i \in I$, as required. □

10.2 Morita contexts

The main results are due to Kiiti Morita (1915-1995) [18]; see [1] for a description of his works in algebra and topology. We will follow the standard treatment of Morita theory, eg. that of [14, §18]. Nonetheless, we will work with left R-modules rather than the right ones.

De nition 10.2.1. Two rings R and S are called Morita equivalent if the categories R-**Mod** and S-**Mod** are equivalent.

Likewise one can de ne Morita equivalences using right modules. However, it turns out that the notion of Morita equivalence is left-right symmetric (Proposition 10.5.1). This is somehow surprising since R-**Mod** and **Mod**-R are not equivalent in general. For example, a ring R being left primitive is a property of the category R-**Mod** [14, p.482], whereas we have remarked that the notion of primitivity is not left-right symmetric.

Two rings R and S are Morita equivalent if and only if there exists a pair of functors

$$R - \mathbf{Mod} \underset{G}{\overset{F}{\rightleftarrows}} S - \mathbf{Mod}$$

which are mutually inverse equivalences of categories (see Convention 10.4.1). Set $Q := F({}_R R)$ and $P := G({}_S S)$. We will de ne the *Morita contexts* by extracting the properties of such pairs (P, Q) using the notion of progenerators introduced before. Then we will prove

Morita I . Morita contexts $\rightsquigarrow$ Morita equivalences.

Morita II . Morita equivalences $\rightsquigarrow$ Morita contexts.

Morita III . Composition of equivalences $\leftrightarrow$ tensor products of progenerators.

Fix a ring R and let P be an object of R-**Mod**. De ne

$$\begin{aligned} Q &:= \mathrm{Hom}(P, {}_R R), \\ S &:= \mathrm{End}({}_R P). \end{aligned}$$

Claim: there are canonical bimodule structures

$${}_R P_S, \quad {}_S Q_R, \quad {}_R R_R, \quad {}_S S_S,$$

together with

$$\begin{aligned} \beta : Q \otimes_R P &\longrightarrow S \\ q \otimes p &\longmapsto qp, \\ \alpha : P \otimes_S Q &\longrightarrow R \\ p \otimes q &\longmapsto pq \end{aligned}$$

which are homomorphisms of (S,S)- and (R,R)-bimodules, respectively. Explanations are given below.

1. Recall that according to our conventions, given left module M and N, the elements of $\mathrm{Hom}(M,N)$ operate *on the right* of M. Hence P becomes an (R,S)-bimodule; the R-linearity of homomorphisms are interpreted as an associativity law $(rp)s = r(ps)$ for all $p \in P$, $r \in R$, $s \in S = \mathrm{End}({}_RP)$.
2. The bimodule structure of Q is given by $qr : p \mapsto (pq)r$; $sq : p \mapsto (ps)q$ for all $q \in Q = \mathrm{Hom}(P, {}_RR)$, $s \in S = \mathrm{End}(P)$ and $r \in R$, according to the rule above.
3. The bimodule structures of R and S come from their ring structures.
4. For given $p \in P$ and $q \in Q$, the rules above gives $pq \in R$ (it is simply the image of p under q).
5. On the other hand, qp is the endomorphism of P given by $p'(qp) = \underbrace{(p'q)}_{\in R} p$ for every $p' \in P$; it is routine to check that qp is left R-linear.

We have observed that these bimodule structures and the homomorphisms α, β satisfy various compatibility conditions. These conditions are encoded in the single assertion that we may de ne the *Morita ring* formally as

$$\mathcal{M} := \begin{pmatrix} R & P \\ Q & S \end{pmatrix}$$

under the usual matrix multiplication and the operations above, which makes $\mathcal{M}$ into an *associative ring*. The compatibilities are thus expressed in terms of various "associativity laws". For instance, we have the equality in ${}_SQ_R$:

$$\underbrace{(q'p)}_{\in S} q = q' \underbrace{(pq)}_{\in R}, \quad q, q' \in Q,\ p \in P. \tag{10.1}$$

To check such relations, one can unfold all the de nitions in terms of elements of P and various homomorphisms, which is not di cult (see [14]). Alternatively, one can realize everything as arrows, eg. $P = \mathrm{Hom}({}_RR, P)$, $R = \mathrm{Hom}({}_RR, {}_RR)$, and reduce to the associativity of the composition of morphisms in R-**Mod**. Take (10.1) for example:

$$\begin{aligned} \text{Left hand side} &= \underbrace{\left(P \xrightarrow{q'} R \xrightarrow{p} P \right)}_{\in S} \xrightarrow{q} R \\ &= P \xrightarrow{q'} \underbrace{\left(R \xrightarrow{p} P \xrightarrow{q} R \right)}_{\in R} \\ &= \text{right hand side}. \end{aligned}$$

Exercise 10.2.2. Find out the other compatibility relations and verify them.

De nition 10.2.3. The 6-tuple $(R, P, Q, S; \alpha, \beta)$ is called the *Morita context* attached to the left R-module P.

If we work with the categories of right modules as in [12, 14], say starting from an object P_R of **Mod**-R, then $Q := \mathrm{Hom}(P, R_R)$ will be an (R, S)-bimodule where $S := \mathrm{End}(P_R)$ and P is an (S, R)-bimodule. The Morita ring $\mathcal{M}_{\mathrm{right}}$ in this setup di ers from $\mathcal{M}$ by a matrix transpose, namely

$$\mathcal{M}_{\mathrm{right}} := \begin{pmatrix} R & Q \\ P & S \end{pmatrix}.$$

10.3 Progenerators

Fix a ring R.

Proposition 10.3.1. *Let P be a left R-module and construct the 6-tuple $(R, P, Q, S; \alpha, \beta)$ as in the previous section.*

1. *P is a generator in R-**Mod** if and only if $\alpha : P \otimes_S Q \to R$ is surjective.*
2. *If P is a generator in R-**Mod**, then*
   - *(a) α is an isomorphisms between (R, R)-modules;*
   - *(b) $Q \simeq \mathrm{Hom}(P_S, S_S)$ as (S, R)-bimodules;*
   - *(c) $P \simeq \mathrm{Hom}({}_SQ, {}_SS)$ as (R, S)-bimodules;*
   - *(d) $R \simeq \mathrm{End}(P_S) \simeq \mathrm{End}({}_SQ)$ as rings.*

The isomorphisms above are all canonical.

Before beginning the proof, recall that according to our earlier conventions, $\mathrm{Hom}(P_S, S_S)$ operates *on the left* of P since we are considering right S-modules here. The (S, R)-bimodule structure on $\mathrm{Hom}(P_S, S_S)$ is

$$s f r : p \mapsto s \underbrace{f(rp)}_{\in S}, \quad p \in P, s \in S, r \in R, f \in \mathrm{Hom}(P_S, S_S).$$

Likewise $\mathrm{Hom}({}_SQ, {}_SS)$ operates *on the right* of Q and is equipped with a natural (R, S)-bimodule structure.

Proof. Recall the notion of the trace ideal $\mathrm{Tr}({}_RP)$ of P (De nition 10.1.9). By Proposition 10.1.10, ${}_RP$ is a generator if and only if $\mathrm{Tr}({}_RP) = R$. By the very de nition of α, it amounts to the surjectivity of α. Hence the rst assertion follows.

The "associativity laws" will be extensively used in the following arguments. Assume that ${}_RP$ is a generator. We have shown that there is an equation

$$\sum_i p_i q_i = 1 \in R, \quad p_i \in P, q_i \in Q.$$

Let us begin with the assertion (a). The surjectivity of α is known. If $0 = \sum_j p'_j q'_j$ for some $p'_j \in P$, $q'_j \in Q$, then we have

$$\begin{aligned}\sum_j p'_j \otimes q'_j &= \sum_{i,j} p'_j \otimes q'_j(p_i q_i) \\ &= \sum_{i,j} p'_j \otimes \underbrace{(q'_j p_i)}_{\in S} q_i = \sum_{i,j} p'_j (q'_j p_i) \otimes q_i \\ &= \sum_i \left(\sum_j p'_j q'_j \right) p_i \otimes q_i = 0\end{aligned}$$

in $P \otimes_S Q$. This proves the injectivity of α. The compatibility with (R, R)-bimodule structures is easy to check.

As for the assertion (b), de ne $\lambda : Q \to \mathrm{Hom}(P_S, S_S)$ by the "left multiplication action", that is:

$$\lambda(q)p = qp \in S, \quad q \in Q, p \in P.$$

The S-linearity of $\lambda(q)$ follows from various "associativity laws" mentioned before. Claim: λ is an isomorphism between (S, R)-modules.

- ⋆ Injectivity of λ. If $qp = 0$ for all $p \in P$, then

$$q = q \cdot 1_R = \sum_i q(p_i q_i) = \sum_i (qp_i) q_i = 0$$

  by associativity laws.
- ⋆ Surjectivity of λ. Let $f \in \mathrm{Hom}(P_S, S_S)$, we have

$$\begin{aligned}fp = f\left(\left(\sum_i \underbrace{p_i q_i}_{\in R} \right) p \right) &= \sum_i f((p_i q_i)p) = \sum_i f(p_i(\underbrace{q_i p}_{\in S})) \\ &= \sum_i (\underbrace{fp_i}_{\in S})(q_i p) = \sum_i ((fp_i)q_i)p = \left(\sum_i (fp_i) q_i \right) p\end{aligned}$$

  for all $p \in P$. Hence $f = \lambda(\sum_i (fp_i)q_i)$.

The compatibility of (S, R)-bimodule structures is straightforward and is left to the reader. This proves (b) and the proof of (c) is similar.

Let us prove (d). De ne $\sigma : R \to \mathrm{End}(P_S)$ and $\tau : R \to \mathrm{End}({}_S Q)$ by left and right multiplication, respectively. This makes sense since P (resp. Q) is an (R, S)-bimodule (resp. (S, R)-bimodule). They are evidently ring homomorphisms. We set out to show that σ is an isomorphism.

- ⋆ Injectivity of σ. Let $r \in R$ be such that $rp = 0$ for all $p \in P$, i.e. $\sigma(r) = 0$. Then $r = r \cdot 1 = \sum_i r(p_i q_i) = \sum_i (rp_i) q_i = 0$.

⋆ Surjectivity of σ. Let $f \in \mathrm{End}(P_S)$. For every $p \in P$ we have

$$fp = f\left(\left(\sum_i p_i q_i\right)p\right) = \sum_i f(p_i(\underbrace{q_i p}_{\in S})) = \left(\underbrace{\sum_i (fp_i)q_i}_{\in R}\right)p$$

for all $p \in P$. Hence $f = \sigma(\sum_i (fp_i)q_i)$.
The case of τ is similar. □

Proposition 10.3.2. *Let $(R, P, Q, S; \alpha, \beta)$ be as before.*

1. *P is projective and nitely generated in R-**Mod** if and only if β is surjective.*
2. *If P is projective and nitely generated in R-**Mod**, then*
   (a) *$\beta : Q \otimes_R P \to S$ is an isomorphism of (S, S)-bimodules;*
   (b) *$Q \simeq \mathrm{Hom}({}_R P, {}_R R)$ as (S, R)-bimodules;*
   (c) *$P \simeq \mathrm{Hom}(Q_R, R_R)$ as (R, S)-bimodules;*
   (d) *$S \simeq \mathrm{End}({}_R P) \simeq \mathrm{End}(Q_R)$ as rings.*

The isomorphisms above are all canonical.

The bimodule structures of $\mathrm{Hom}({}_R P, {}_R R)$ and $\mathrm{Hom}(Q_R, R_R)$ are de ned in the standard manner, as in the previous proposition.

Proof. We shall only give the proof for statement 1. The arguments for statement 2 are parallel to those in the previous proposition and will be omitted.

The surjectivity of β is equivalent to an equation in S of the form

$$1 = \sum_{i=1}^{n} q_i p_i, \quad q_i \in Q, p_i \in P.$$

This amounts to the existence of $q_i \in \mathrm{Hom}({}_R P, {}_R R)$ such that $p = \sum_i (\underbrace{pq_i}_{\in R})p_i$ for all $p \in P$. Equivalently, we have a homomorphism

$$\begin{aligned} {}_R R^{\oplus n} = \bigoplus_{i=1}^{n} Re_i &\xrightarrow{f} {}_R P \\ e_i &\longmapsto p_i, \end{aligned}$$

together with a homomorphism $s : P \to \bigoplus_{i=1}^n Re_i$ given by $p \mapsto \sum_{i=1}^n (pq_i)e_i$ satisfying

$$f \circ s = \mathrm{id}.$$

By Proposition 10.1.2, this amounts to the assertion that ${}_R P$ is nitely generated and projective. □

The aforementioned results concerning left R-modules apply to the setup of right R-modules as well – simply replace R by R^{op}.

Proposition 10.3.3. *If P is a progenerator in R-**Mod**, then ${}_SQ$, P_S and Q_R are all progenerators in suitable categories and α, β are isomorphisms.*

Proof. The assertions concerning α and β are already proved. Let us show that ${}_SQ$ is a progenerator. We recall from Proposition 10.3.2 the following "re exivity"

$$\mathrm{Hom}({}_SQ, {}_SS) \simeq P,$$
$$\mathrm{End}({}_SQ) \simeq R.$$

Both isomorphisms are canonical. From the left S-module Q we associate a Morita context, in which the objects derived from ${}_SQ$ are decorated with quotation marks:

$$(S, Q, "Q", "S"; "\alpha", "\beta").$$

From re exivity, one gets canonical identi cations "S"=R and "Q"=P, under which the "β" becomes

$$\alpha : P \otimes_S Q \to R,$$

an isomorphism of (R, R)-bimodules. Hence Q is a progenerator in S-**Mod**. The remaining cases are similar: one constructs suitable Morita contexts and concludes from the bijectivity of α and β. Cf. the next Corollary and Remark. □

In the preceding proof we have observed that the "α" and "β" for ${}_SQ$ are identi ed with the β and α for ${}_RP$, respectively. The cases for P_S and Q_R are similar. Let us summarize these re exivities below.

Corollary 10.3.4. *Assume that P is a progenerator in R-**Mod** and let $(R, P, Q, S; \alpha, \beta)$ be the corresponding Morita context. Then α, β are isomorphisms and*

$$(S, {}_SQ, P, R; \beta, \alpha)$$
$$(S, P_S, Q, R; \beta, \alpha)$$
$$(R, Q_R, P, S; \alpha, \beta)$$

are Morita contexts corresponding to the progenerators ${}_SQ$, P_S, Q_R respectively.

Remark 10.3.5. We leave it to the reader to de ne the Morita contexts for right modules which appear above. See also [14, §18C] or [12].

10.4 Main theorems

Warning: the proofs below will be sketchy.

Convention 10.4.1. In what follows, a category equivalence between additive categories C and C' is a functor $F : C \to C'$ such that there exists a functor $G : C' \to C$ satisfying $F \circ G \simeq \mathrm{id}_{C'}$, $G \circ F \simeq \mathrm{id}_C$. Such (F, G) is called a pair of mutually inverse category equivalences. By isomorphism of equivalences we mean isomorphism in the sense of functors. The author apologizes for these nonstandard terminologies.

Theorem 10.4.2 (Morita I)**.** *Let P be a progenerator in R-**Mod** and $(R, P, Q, S; \alpha, \beta)$ be the corresponding Morita context. Then there are mutually inverse category equivalences*

$$R - \textbf{Mod} \underset{P\otimes_S -}{\overset{Q\otimes_R -}{\rightleftarrows}} S - \textbf{Mod},$$

$$\textbf{Mod} - R \underset{-\otimes_S Q}{\overset{-\otimes_R P}{\rightleftarrows}} \textbf{Mod} - S$$

Proof. We have isomorphisms of functors from R-**Mod** to itself

$$P \otimes_S (Q \otimes_R -) \simeq (P \otimes_S Q) \otimes_R - \xrightarrow{\alpha\otimes\mathrm{id}} R \otimes_R - = \mathrm{id}_{R-\mathbf{mod}}(-).$$

Similarly we have isomorphisms of functors from S-**Mod** to itself

$$Q \otimes_R (P \otimes_S -) \simeq (Q \otimes_R P) \otimes_S - \xrightarrow{\beta\otimes\mathrm{id}} S \otimes_S - = \mathrm{id}_{S-\mathbf{mod}}(-).$$

Thus the first equivalence is established. The proof for the other one is similar. □

Remark 10.4.3. Let P be a progenerator of R-**Mod** and define Q, S accordingly. We have an isomorphism of functors

$$\begin{aligned} Q \otimes_R - &\longrightarrow \mathrm{Hom}({}_RP, -) \\ q \otimes \clubsuit &\longmapsto [p \mapsto \underbrace{pq}_{\in R} \clubsuit] \end{aligned}$$

from R-**Mod** to S-**Mod**. Indeed, the isomorphism is evident for ${}_RP = {}_RR$; the general case follows by realizing ${}_RP$ as a direct summand of some ${}_RR^{\oplus I}$ by Proposition 10.1.2. Likewise, we deduce

$$\begin{aligned} P \otimes_S - &\xrightarrow{\sim} \mathrm{Hom}({}_SQ, -), \\ - \otimes_R P &\xrightarrow{\sim} \mathrm{Hom}(Q_R, -), \\ - \otimes_S Q &\xrightarrow{\sim} \mathrm{Hom}(P_S, -) \end{aligned}$$

by applying Proposition 10.3.3.

Theorem 10.4.4 (Morita II)**.** *Let R, S be rings. Given a pair of mutually inverse equivalences*

$$R - \textbf{Mod} \underset{G}{\overset{F}{\rightleftarrows}} S - \textbf{Mod}$$

we put $Q := F({}_RR)$ and $P := G({}_SS)$. There exist canonical bimodule structures ${}_RP_S$, ${}_SQ_R$ and isomorphisms of functors

$$\begin{aligned} F(-) &\simeq Q \otimes_R -, \\ G(-) &\simeq P \otimes_S -. \end{aligned}$$

Moreover, the Morita context associated to ${}_RP$ can be identified with $(R, P, Q, S; \alpha, \beta)$ for appropriate α,β.

Proof. We have $\mathrm{End}({}_RP) \simeq \mathrm{End}({}_SS) = S$ and $\mathrm{End}({}_SQ) = \mathrm{End}({}_RR) = R$ (right multiplications) given by the functors F and G, which yield the required bimodule structures. Being a progenerator is a categorical property, hence P and Q are progenerators (cf. Example 10.1.7).

There are isomorphisms $\mathrm{Hom}({}_RP, {}_RR) \xrightarrow{\sim} \mathrm{Hom}({}_SS, {}_SQ) \simeq Q$ given by the functor F; it is routine to check that they respect the relevant (S, R)-bimodule structures. This proves the assertion on the identi cation of Morita contexts. Moreover, by Remark 10.4.3 we get isomorphism of functors

$$F \simeq \mathrm{Hom}({}_SS, F(-)) \simeq \mathrm{Hom}({}_RP, -) \simeq Q \otimes_R -.$$

Similarly, $G \simeq P \otimes_S -$. □

De nition 10.4.5. Let A, B be rings. An (A, B)-bimodule ${}_AC_B$ is called *faithfully balanced* if the multiplications maps $A \to \mathrm{End}(C_B)$ and $B \to \mathrm{End}({}_AC)$ are both ring isomorphisms. It is called an (A, B)-progenerator if ${}_AC_B$ is faithfully balanced and ${}_AC$ is a progenerator.

Note a hidden left-right symmetry in the de nition: if ${}_AC_B$ is an (A, B)-progenerator, then C_B is also a progenerator in **Mod**-B (i.e. B^{op}-**Mod**) by Proposition 10.3.3, since B may be identi ed with $\mathrm{End}({}_AC)$.

Corollary 10.4.6. *If P is a progenerator in R-**Mod**, then ${}_RP_S$ (resp. ${}_SQ_R$) is an (R, S)-progenerator (resp. (S, R)-progenerator).*

Proof. Combine the Propositions 10.3.1, 10.3.2 and 10.3.3. □

Theorem 10.4.7 (Morita III)**.** *Let R, S be rings. Then the isomorphism classes of equivalences $F : R - \boldsymbol{Mod} \to S - \boldsymbol{Mod}$ form a set, which is in canonical bijection with the (R, S)-progenerators. Furthermore, composition of functors corresponds to $\otimes$-product of bimodules: given rings R, S and T,*

$$R - \boldsymbol{Mod} \xrightarrow{{}_RP'_S} S - \boldsymbol{Mod} \xrightarrow{{}_SP''_T} T - \boldsymbol{Mod} \qquad (10.2)$$

$$\text{with } {}_RP_T := P' \otimes_S P'' \text{ over the composite}$$

commutes up to isomorphism.

Proof. By the Theorems 10.4.2 and 10.4.4, up to isomorphisms, the (R, S)-progenerators ${}_RP_S$ are in bijection with the equivalences $G : S - \mathbf{Mod} \to R - \mathbf{Mod}$. More precisely, $G = P \otimes_S -$. Hence the isomorphism classes of such equivalences form a set. The compatibility between composition and $\otimes$-product in the sense of (10.2) is now clear. □

Now take $R = S$. It follows immediately that the isomorphisms classes of (R, R)-progenerators form a set, which is a monoid with identity element ${}_RR_R$. It is actually a group by Proposition 10.3.2. Thus the following corollary is immediate.

Corollary 10.4.8. *The isomorphism classes of self-equivalences of R-**Mod** form a group, which is isomorphic to the group of isomorphisms classes of (R, R)-progenerators under $\otimes$-product.*

10.5 Applications

Recall the notion of Morita equivalence in De nition 10.2.1.

Proposition 10.5.1. *The notion of Morita equivalence for rings is left-right symmetric.*

Proof. Two rings R and S are Morita equivalent (in the sense of left modules) if and only if there exists an (R, S)-progenerator ${}_RP_S$, by Theorems 10.4.4 and 10.4.7. Alternatively, we may view P as a $(S^{\mathrm{op}}, R^{\mathrm{op}})$-progenerator, hence R^{op} and S^{op} are Morita equivalent. □

As another application, let us deduce the Wedderburn-Artin structure Theorem from Morita theory. Such is the approach adopted in [12].

Theorem 10.5.2. *Let R be a left semisimple ring. There exist $n \in \mathbb{Z}_{\geq 1}$, division rings D_i and $n_i \in \mathbb{Z}_{\geq 1}$ for $i = 1, \ldots, n$ such that*

$$R \simeq \prod_{i=1}^{n} M_{n_i}(D_i).$$

Moreover, the datum $(D_i, n_i)_{1 \leq i \leq n}$ is unique up to permutation and isomorphisms.

Proof. We will omit the uniqueness part. Let R be a left semisimple ring. There is a decomposition

$${}_RR = \bigoplus_{i=1}^{n} \mathfrak{a}_i^{\oplus m_i}$$

into simple submodules (i.e. minimal left ideals), such that $\mathfrak{a}_i \simeq \mathfrak{a}_j \iff i = j$; as in the previous approaches, the niteness follows by looking at $1 \in R$. By Proposition 10.1.10, $P := \bigoplus_{i=1}^{n} \mathfrak{a}_i$ is a generator. It is a progenerator as ${}_RP$ is clearly a direct summand of ${}_RR$.

Let $(R, P, Q, S; \alpha, \beta)$ be the attached Morita context, with

$$S = \mathrm{End}({}_RP) = \prod_{i=1}^{n} D_i, \quad D_i := \mathrm{End}({}_R\mathfrak{a}_i) \quad \text{(division ring)}.$$

Set $n_i := \dim_{D_i}(\mathfrak{a}_i)$ for each $1 \leq i \leq n$. Since P_S is a progenerator by Proposition 10.3.3, hence nitely generated over S, we deduce $n_i < \infty$ for all i. Proposition 10.3.1 implies

$$R \simeq \mathrm{End}(P_S) = \prod_{i=1}^{n} \mathrm{End}_{D_i}(\mathfrak{a}_i) \simeq \prod_{i=1}^{n} M_{n_i}(D_i)$$

as rings. □

Exercise 10.5.3. How many proofs have we given for the Wedderburn-Artin theorem?

Exercise 10.5.4. Let C be an additive category. De ne its *center* as

$$Z(C) := \mathrm{End}(\mathrm{id}_C)$$

which is a ring. More precisely, an element of $Z(C)$ is a family $(\varphi_M \in \mathrm{Hom}(M, M))_M$, where M ranges over the objects of C, such that for every morphism $f : M \to N$ in C the following diagram commutes.

$$\begin{array}{ccc} M & \xrightarrow{\varphi_M} & M \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ N & \xrightarrow[\varphi_N]{} & N \end{array}$$

1. For $C = R - \mathbf{Mod}$, show that $Z(C) \simeq Z(R)$ canonically, where $Z(R)$ stands for the center of R. **Hint**: describe φ_{RR} and show that it determines the other endomorphisms φ_M in a given element of $Z(C)$.

2. Show that if two rings R and S are Morita equivalent, their centers must be isomorphic.

3. Let R, S be rings and let ${}_RM_S$ be a faithfully balanced (R, S)-bimodule (De nition 10.4.5). Show that the action by left R-multiplication induces an isomorphism $Z(R) \xrightarrow{\sim} \mathrm{End}({}_RM_S)$. Similarly, $Z(S) \xrightarrow{\sim} \mathrm{End}({}_RM_S)$ via right S-multiplication. Now deduce part 2 from Morita theory.

LECTURE 11

REPRESENTATIONS OF FINITE GROUPS

In this lecture we will proceed into the realm of representation theory of nite groups. For a historical account, we recommend the excellent book [6] by Curtis.

11.1 Representation of algebras

Fix a eld F. We begin by summarizing the representation theory of nite-dimensional F-algebras, i.e. the study of their left modules. Some results hold for left artinian rings as well, but the author is too lazy to single them out.

Let A be a nite-dimensional F-algebra. By the theory of Jacobson radical, $\bar{A} := A/\mathrm{rad}(A)$ is a semisimple F-algebra. From the Wedderburn-Artin Theorem, we have a ring isomorphism

$$\bar{A} = \prod_{i=1}^{r} \underbrace{\mathrm{End}((\mathfrak{a}_i)_{D_i})}_{:=B_i} \tag{11.1}$$

where $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ are representatives of isomorphism classes of the simple left A-submodules (i.e. the minimal left ideals) of $\bar{A}$, and

$$D_i := \mathrm{End}({}_A\mathfrak{a}_i) = \mathrm{End}({}_{B_i}\mathfrak{a}_i), \quad \text{(division } F\text{-algebra)}$$

acts on the right of $\mathfrak{a}_i$ by our convention.

Upon inspecting our proof of the Wedderburn-Artin Theorem, the isomorphism (11.1) is given by sending $a \in A$ to the family $L_i(a) : \mathfrak{a}_i \to \mathfrak{a}_i$, where $L_i(a) : x \mapsto ax$, for $i = 1, \ldots, r$. It is convenient to treat each component B_i separately. For a xed index i, we shall temporarily drop the index and write $\mathfrak{a}$, D, B to alleviate notations. Put

$$\mathfrak{a}' := \mathrm{Hom}(\mathfrak{a}_D, D_D).$$

Note that $\mathfrak{a}$ (resp. $\mathfrak{a}'$) is a (B, D)-bimodule (resp. (D, B)-bimodule). Moreover, in the last part of the previous lecture we have seen that ${}_B\mathfrak{a}$ is a progenerator, hence

$$\mathfrak{a}' \simeq \mathrm{Hom}({}_B\mathfrak{a}, {}_BB).$$

The natural homomorphism

$$\begin{aligned} \mathfrak{a} \underset{D}{\otimes} \mathfrak{a}' &\xrightarrow{\sim} B = \mathrm{End}(\mathfrak{a}_D) \\ v \otimes \check{v} &\mapsto [x \mapsto v \underbrace{(\check{v}x)}_{\in D}] \end{aligned}$$

of (B, B)-bimodules turns out to be an isomorphism. Indeed, this can be seen by the identi cations $B = M_n(D)$ and $\mathfrak{a}_D = (D_D)^{\oplus n}$, for some n.

Variation of the index i yields the following bimodule version of Wedderburn-Artin Theorem.

Proposition 11.1.1. *We have isomorphisms of (A, A)-bimodules*

$${}_A\bar{A}_A \xrightarrow{\sim} \bigoplus_{i=1}^{r} \mathrm{End}((\mathfrak{a}_i)_{D_i}) \xleftarrow{\sim} \bigoplus_{i=1}^{r} \mathfrak{a}_i \otimes_{D_i} \mathfrak{a}_i'$$

in which $a \mapsto (L_i(a))_{i=1}^r$ and $v_i \otimes \check{v}_i \mapsto v_i(\check{v}_i(\cdot))$.

Proposition 11.1.2. *The left ideals $\mathfrak{a}_1, \ldots \mathfrak{a}_r$ form a complete set of representatives of the simple left A-modules. Each simple left A-module is nite-dimensional over F.*

Proof. The simple A-modules are just simple $\bar{A}$-modules. Thus we may assume $A = \bar{A}$. Since a simple left A-module is necessarily a quotient of ${}_AA$, which is nite-dimensional over F, we conclude by the Wedderburn-Artin Theorem. □

Consider an arbitrary eld extension $E \supset F$. Write $A_E := A \underset{F}{\otimes} E \simeq E \underset{F}{\otimes} A$. The assignment $M \mapsto M_E$ ts in to a functor from A-**Mod** to A_E-**Mod**.

De nition 11.1.3. Let M be a simple left A-module. We say that M is *absolutely simple* if M_E is simple for every eld extension E.

De nition 11.1.4. A eld extension $E \supset F$ is called a *splitting eld* of A if every simple left A_E-module is absolutely simple. In this case we also say that E splits A.

Theorem 11.1.5. *Let M be a simple left A-module. The following statements are equivalent:*

1. *M is absolutely simple;*
2. *M_E is simple for every nite extension E of F;*
3. *$\mathrm{End}({}_AM) = F$;*
4. *the homomorphism $A \to \mathrm{End}_F(M)$ given by the left A-module structure is surjective.*

In particular, for algebraically closed F the notion of absolute simplicity is redundant.

Proof. (1) $\Rightarrow$ (2) is trivial.

(2) $\Rightarrow$ (3). Let $\varphi \in \mathrm{End}({}_AM)$. Let λ be an eigenvalue of φ as an element of $\mathrm{End}_F(M)$ and take $E \ni \lambda$. Set $\varphi_E := E \underset{F}{\otimes} \varphi \in \mathrm{End}_E(M_E)$. Then $\varphi_E - \lambda$ is non-invertible in $\mathrm{End}({}_{A_E}M_E)$, which is a division ring. Hence $\varphi_E = \lambda$ is a scalar operator, and so is φ.

(3) $\Rightarrow$ (4). Apply the Density Theorem.

(4) $\Rightarrow$ (1). For every field extension E, the homomorphism $A_E \to \mathrm{End}_E(M_E)$ is still surjective. Thus the simplicity of M_E follows from linear algebra. □

Corollary 11.1.6. *A field E is a splitting field of A if and only if $\overline{A_E}$ is a direct product of matrix algebras over E. Thus this definition is compatible with the one for central simple algebras.*

Proof. Use (3) of the preceding theorem and apply Proposition 11.1.1 to $\overline{A_E}$. □

Exercise 11.1.7. Let M, N be simple left A-modules. Show that $\mathrm{Hom}(M_E, N_E) \neq \{0\}$ if and only if $M \simeq N$. **Hint**: $\mathrm{Hom}(M_E, N_E) = \mathrm{Hom}(M, N) \underset{F}{\otimes} E$.

Proposition 11.1.8. *Let E/F be a field extension. For every simple left A_E-module N, there exists a simple left A-module M such that N is a Jordon-Hölder factor of M_E i.e. N is a subquotient (= quotient of a submodule) thereof.*

Proof. We know that N must be a Jordon-Hölder factor of the left A_E-module A_E, which is obtained from ${}_AA$ by applying $E \otimes_F -$. Let

$$\{0\} = F_0 \subset F_1 \subset \cdots \subset F_n = {}_AA$$

be a composition series of ${}_AA$, i.e. with simple successive quotients $M_i := F_i/F_{i-1}$. Then $(F_i)_E$ form an ascending chain of left A_E-submodules of A_E, with successive quotients $(M_i)_E$. Indeed, $E \otimes_F -$ is an *exact functor* in the sense that given a short exact sequence

$$0 \to M' \to M \to M'' \to 0$$

in A-**Mod**, one can check that

$$0 \to M'_E \to M_E \to M''_E \to 0$$

is exact in A_E-**Mod**, say by choosing an F-basis of E.

By Schreier's refinement theorem, we may refine $((F_i)_E)_{i=0}^n$ to get a composition series of A_E. Hence N must appear as a Jordan-Hölder factor of some $(M_i)_E$. □

Corollary 11.1.9. *If E is a splitting field for A, then so is every extension L of E.*

Proof. Let Q be a simple left A_L-module. By the preceding Proposition, Q is a subquotient of N_L for some simple left A_E-module N. But N_L is simple since E is a splitting field, hence $Q = N_L$. Now for every extension L'/L we have $Q_{L'} = N_{L'}$ which is again simple in $A_{L'}$-**Mod**. □

Corollary 11.1.10. *There exists a finite extension E of F that splits A.*

Proof. Pick an algebraic closure $\bar{F}$ of F. By Corollary 11.1.6, $\bar{F}$ is a splitting field of A. Let $M_1', \ldots . M_n'$ be a complete set of representatives of simple left $A_{\bar{F}}$-modules. For each $1 \leq i \leq n$, we may choose an $\bar{F}$-basis of M_i' and by inspecting the actions of an F-basis of A on M_i', we see that there exist a finite extension E_i/F, a left A_{E_i}-module M_i such that $M_i' = \bar{F} \underset{E}{\otimes} M_i$. Take E to be the compositum of $E_1, \ldots, E_n$ in $\bar{F}$, we obtain left A_E-modules $M_1, \ldots, M_n$.

By Theorem 11.1.5, $M_1, \ldots, M_n$ are absolutely simple left A_E-modules. If M is a simple left A_E-module, then there exists $1 \leq i \leq n$ such that

$$\{0\} \neq \underbrace{\mathrm{Hom}_{\bar{F}-\mathbf{Mod}}(M_{\bar{F}}, M_i') = \mathrm{Hom}_{E-\mathbf{Mod}}(M, M_i) \underset{E}{\otimes} \bar{F}}_{\text{by linear algebra}}.$$

Hence $M = M_i$. It follows that E is a splitting field for A. □

Exercise 11.1.11. Let $f(X)$ be a polynomial over F and set $A := F[X]/(f(X))$. Describe the splitting fields of A and reconcile the notions of "splitting field" in representation theory and field theory.

11.2 Characters

Fix a field F. For every F-algebra A and a left A-module M which is finite-dimensional over F, we define

$$\chi_M : A \to F$$

by setting $\chi_M(a) = \mathrm{Tr}(a|M)$; the notation means that we calculate the trace by regarding a as an element of $\mathrm{End}_F(M)$. It depends only on the isomorphism class of M.

We call χ_M the *character* of M. Let $[A, A]$ be the additive subgroup of A generated by elements of the form $xy - yx$, $x, y \in A$. Then χ_M induces an F-linear map $A/[A, A] \to F$ since $\mathrm{Tr}(xy - yx|M) = 0$. In fact χ_M vanishes on $[A, A] + \mathrm{rad}(A)$.

Lemma 11.2.1. *If $0 \to M' \to M \to M'' \to 0$ is a short exact sequence in A-**Mod**, then*

$$\chi_M = \chi_{M'} + \chi_{M''}.$$

Proof. Linear algebra. □

Hereafter, we revert to the assumption that $\dim_F A < +\infty$.

From the previous Lemma we learn that χ_M only "sees" the Jordan-Hölder factors of M. In favorable circumstances, however, it will determine the modules.

Theorem 11.2.2. *The characters of absolutely simple left A-modules are linearly independent as elements of* $\mathrm{Hom}_F(A/[A, A], F)$.

Proof. Enumerate the isomorphism classes of absolutely simple left A-modules by $M_1, \ldots, M_s$. By Proposition 11.1.1, for every $1 \leq i \leq s$ there exists $a_i \in A$ such that

$$\mathrm{Tr}(a_i|M_j) = \begin{cases} 1, & i = j, \\ 0, & i \neq j. \end{cases}$$

In any linear combination $\sum_{j=1}^{s} c_j \chi_{M_j}$, the coefficient c_i can be read off by evaluation at a_i, hence the linear independence. □

We do not attempt to record all the generalizations or improvements of this theorem. Below is an easy variant.

Theorem 11.2.3. *Suppose that F is of characteristic zero. The characters of simple left A-modules are linearly independent over F. Consequently, χ_M determines the Jordan-Hölder factors of M, for any left A-module that is nitely-dimensional over F.*

The second assertion does not hold in general when $\mathrm{char}(F) = p > 0$. Indeed, choose non-isomorphic simple modules M_1, M_2, then $M_1^{\oplus p}$ and $M_2^{\oplus p}$ have the same character, say zero, but they are not isomorphic

Proof. Enumerate the isomorphism classes of simple left A-modules by $M_1, \ldots, M_r$ and copy the previous proof. This time we can only assume that a_i acts on M_i as id, which is certainly linear over $D_i := \mathrm{End}({}_AM_i)$, and a_i acts on M_j as zero if $i \neq j$. Thus $\mathrm{Tr}(a_i|M_i) = \dim_F M_i$. Now we can apply the assumption $\mathrm{char}(F) = 0$ to determine the coe cients c_i in any linear combination $\sum_{j=1}^r c_j \chi_{M_j}$. □

When A is not semisimple, the study of simple A-modules only reveals a very small portion of information on the algebra A. It turns out that the *indecomposable* A-modules have much richer (and harder!) structure. Unfortunately, we are unable to address these questions in this course.

11.3 The group algebra

Let $\Bbbk$ be a commutative ring and G be any group. The group $\Bbbk$-algebra $\Bbbk G$ is the free $\Bbbk$-module generated by the symbols $g \in G$, that is, the elements in $\Bbbk G$ are formal $\Bbbk$-linear combinations

$$\sum_{g \in G} a_g g, \quad \forall g, a_g \in \Bbbk,\ a_g = 0 \text{ for all but nitely many } g,$$

and the multiplication in $\Bbbk G$ is de ned on the generators by

$$g \cdot h = gh \quad \text{(multiplication in } G\text{)}, \quad g, h \in G,$$

then extended linearly to $\Bbbk G$. The identity element of $\Bbbk G$ is $1 \in G$. We may regard G as a distinguished basis of the $\Bbbk$-vector space $\Bbbk G$.

There is a universal property characterizing $\Bbbk G$. Let $U : \Bbbk - \mathbf{Alg} \to \mathbf{Grp}$ be the functor which maps a $\Bbbk$-algebra R to its group of units $R^\times$. Then the natural inclusion $G \hookrightarrow \Bbbk G$ induces an isomorphism

$$\mathrm{Hom}_{\Bbbk - \mathbf{Alg}}(\Bbbk G, -) \simeq \mathrm{Hom}_{\mathbf{Grp}}(G, U(-))$$

of functors from $\Bbbk$-**Alg** to **Sets**. In fact it is also functorial in G.

In what follows, we will specialize to the case where $\Bbbk = F$ is a chosen eld, and speak of FG as the group algebra associated to G.

De nition 11.3.1. A representation of G over F is a pair (V, ρ) where V is an F-vector space and $\rho : G \to \mathrm{Aut}_F(V)$ is a group homomorphism. A morphism (also known as *intertwining operator*) between two representations (V_1, ρ_1) and (V_2, ρ_2) is an F-linear map $f : V_1 \to V_2$ such that the diagram

$$\begin{array}{ccc} V_1 & \xrightarrow{f} & V_2 \\ {\scriptstyle \rho_1(g)}\downarrow & & \downarrow{\scriptstyle \rho_2(g)} \\ V_1 & \xrightarrow[f]{} & V_2 \end{array}$$

commutes for every $g \in G$.

In practice we will often drop V or ρ from the datum (G, ρ). The F-vector space of morphisms from (V_1, ρ_1) to (V_2, ρ_2) is denoted as $\mathrm{Hom}_G(V_1, V_2)$.

Thus one can talk about the category $\mathbf{Rep}_F(G)$ of representations of G over F, and de ne subrepresentations, quotient representations, etc., in the obvious manner. It is sometimes more convenient, however, to pass to the category FG-**Mod**.

Proposition 11.3.2. *There is an equivalence between the categories $\boldsymbol{Rep}_F(G)$ and FG-**Mod**, given as follows. Let (ρ, V) be a representations of G over F, we make V into an FG-module by letting $\sum_g a_g g$ act as $\sum_g a_g \rho(g)$. The morphisms are left untouched.*

Proof. Quite trivial. Use the fact

$$\begin{aligned} \{FG - \text{module structures on } V\} &= \mathrm{Hom}_{F-\mathbf{Alg}}(FG, \mathrm{End}_F(V)) \\ &= \mathrm{Hom}_{\mathbf{Grp}}(G, \mathrm{Aut}_F(V)) \end{aligned}$$

from the universal property of FG. □

For example, a subrepresentation is just an FG-submodule, and we may talk about quotient representations as well. A nonzero representation of G over F is called *irreducible* if there is no subrepresentation besides $\{0\}$ and itself, i.e. the corresponding FG-module is simple. The group algebra FG has some extra structures, however. For example we have

$$\begin{aligned} FG &\xrightarrow{\sim} (FG)^{\mathrm{op}}, \qquad g \mapsto g^{-1}, \\ FG \otimes_F FH &\xrightarrow{\sim} F(G \times H), \qquad g \otimes h \mapsto gh, \quad g \in G, h \in H. \end{aligned}$$

Let us consider some elementary operations on representations.

Change of elds Let (V, ρ) be a representation of G over F and E/F be a eld extension. Then $(E \underset{F}{\otimes} V, 1 \otimes \rho)$ is a representation of G over E. This corresponds to the functor $V \mapsto V_E$ from FG-**Mod** to EG-**Mod** studied before.

Direct sum The same as the $\oplus$ in FG-**Mod**.

Tensor product Let $(V_1, \rho_1), (V_2, \rho_2)$ be representations, then $V_1 \otimes_F V_2$ becomes a representation by letting $g \in G$ act by $(\rho_1 \otimes \rho_2)(g) = \rho_1(g) \otimes \rho_2(g)$. In module-theoretic terms, it corresponds to the homomorphism of F-algebras $FG \to FG \underset{F}{\otimes} FG = F(G \times G)$ determined by $g \mapsto g \otimes g$.

External tensor product Let (V_i, ρ_i) be a representation of G_i over F, for $i = 1, 2$. Then $V_1 \otimes_F V_2$ becomes a representation of $G_1 \times G_2$ over F by letting $(g_1, g_2) \in G_1 \times G_2$ act by $(\rho_1 \boxtimes \rho_2)(g_1, g_2) = \rho_1(g_1) \otimes \rho_2(g_2)$. The module-theoretic interpretation is similar to $\otimes$.

Trivial representation The trivial representation of G over F is the 1-dimensional representation $(F, \mathbb{1})$ such that each $g \in G$ acts as id. It corresponds to the homomorphism $FG \to F$ given by $\sum_g c_g g \mapsto \sum_g c_g$.

Hom-spaces Let $(V_1, \rho_1), (V_2, \rho_2)$ be representations of G over F. The space $\mathrm{Hom}_F(V_1, V_2)$ is equipped with a representation of G: we let $g \in G$ act by

$$[f \in \mathrm{Hom}_F(V_1, V_2)] \longmapsto \left[\rho_2(g) \circ f \circ \rho_1(g)^{-1} \in \mathrm{Hom}_F(V_1, V_2)\right].$$

One readily checks that the space of intertwining operators $\mathrm{Hom}_G(V_1, V_2)$ gets identi ed with the space $\mathrm{Hom}_F(V_1, V_2)^G$ of G- xed elements.

Contragredient representation Let (V, ρ) be a representation of G over F. The contragredient $\check{V}$ is the representation $\mathrm{Hom}_F(V, F)$ above, where F denotes the trivial representation of G over F. To get a module-theoretic interpretation, we note that $\check{V} = \mathrm{Hom}_F(V, F) = \mathrm{Hom}(V_F, F_F)$ is a right FG-module by regarding V as an (FG, F)-bimodule in the usual way. More precisely, we have

$$\lambda a : v \mapsto \lambda(av), \quad a \in FG, \lambda \in \mathrm{Hom}(V_F, F_F).$$

Right FG-modules are just left $(FG)^{\mathrm{op}}$-modules. To obtain a left FG-module structure, we apply $FG \xrightarrow{\sim} (FG)^{\mathrm{op}}$, $g \mapsto g^{-1}$.

Pull-back/restriction/in ation Let $\varphi : H \to G$ be a group homomorphism. Then we may deduce a representation of H from a representation of G. In fact, φ induces an F-algebra homomorphism $FH \to FG$, hence a functor from FG-**Mod** to FH-**Mod**. When $H \to G$ is an inclusion (resp. quotient), the pull-back is called the *restriction* (resp. *in ation*) from G to H.

Reduction Let N be a normal subgroup of G and (V, ρ) be a representation of G over F. Set $V^N := \{v \in V : \forall \nu \in N,\ \rho(\nu)v = v\}$. Then V^N becomes a representation of G/N.

Exercise 11.3.3. Let $(V_1, \rho_1), (V_2, \rho_2)$ be representations of G over F

1. Show that $V_1 \otimes V_2$ is equal to the restriction of the $G \times G$-representation $V_1 \boxtimes V_2$ to G via the diagonal embedding $G \hookrightarrow G \times G$, i.e. $g \mapsto (g, g)$.

2. Assume V_1 is nite-dimensional over F. Show that the standard isomorphism $\check{V}_1 \otimes_F V_2 \xrightarrow{\sim} \mathrm{Hom}_F(V_1, V_2)$ intertwines the G-representation structures de ned via $\otimes$-product and Hom-sets, respectively.

From now on, we make the assumption

$$\boxed{G \text{ is nite.}}$$

So FG is a nite-dimensional F-algebra and the results in §11.1 are applicable. In what follows an FG-module will always mean a left FG-module, unless otherwise speci ed.

De nition 11.3.4. De ne the absolutely irreducible representations of G over F as the absolutely simple FG-modules, by the dictionary Proposition 11.3.2. A eld F is called a splitting eld of G, if FG splits over F; in this case we also say that G splits over F.

In particular, G splits over every algebraically closed eld, and for every F there exists a nite extension E/F that splits G. Likewise, a representation is called faithful if the corresponding FG-module is.

Theorem 11.3.5 (Maschke)**.** *The group algebra FG is semisimple if and only if $\mathrm{char}(F) \nmid |G|$.*

Proof. Assume $\mathrm{char}(F) \nmid |G|$. Let V be an FG-module and W be a submodule. Take an F-vector subspace W' such that $V = W \oplus W'$ and let $\pi : V \twoheadrightarrow W$ be the corresponding projection map. Set

$$\pi' := |G|^{-1} \sum_{g \in G} g \circ \pi \circ g^{-1}.$$

It is obvious that $\pi' \in \mathrm{Hom}_G(V, W)$. Moreover, $\pi'|_W = \pi|_W = \mathrm{id}$. It follows that $\pi' : V \twoheadrightarrow W$ is a projection operator in the sense of FG-modules, thus

$$V = W \oplus \ker(\pi').$$

To show the "only if" part, put $z := \sum_{g \in G} g$. We have $xz = zx = z$ for all $x \in G$, thus $z \in Z(FG)$ and

$$z^2 = \sum_{x \in G} xz = |G|z = 0.$$

It follows that Fz is a two-sided nilpotent ideal of FG, thus $\mathrm{rad}(FG) \supset Fz \neq \{0\}$. □

Thus the study of group representations can be divided into two avors:
- ⋆ *Ordinary representation theory*, if $\mathrm{char}(F) \nmid |G|$;
- ⋆ *Modular representation theory* (after L. E. Dickson), if $\mathrm{char}(F) || G|$.

We will mainly concentrate on the ordinary case.

De nition 11.3.6. Assume $\mathrm{char}(F) \nmid |G|$ and let W be a (left) FG-module. By Theorem 11.3.5, we may write $W \simeq \bigoplus_V V^{\oplus n_V}$ where V ranges over the isomorphism classes of simple FG-modules. The cardinal number n_V here is called the *multiplicity* of V in W. It is uniquely determined. Indeed, put $D := \mathrm{End}_{FG}(V)$ so that V becomes an (FG, D)-bimodule and $\mathrm{Hom}_{FG}(V, W)$ becomes a left D-vector space, then the so-called V-isotyic part $V^{\oplus n_V}$ in W is canonically isomorphic to the left FG-module

$$V \underset{D}{\otimes} \mathrm{Hom}_{FG}(V, W)$$

via $v \otimes \varphi \mapsto v\varphi \in W$. (Reminder: this technique has appeared in the lecture on central simple algebras.) Hence $n_V = \dim_D \mathrm{Hom}_{FG}(V, W)$.

11.4 Representations and characters of nite groups

As before, let F be a eld and G be a nite group. The representations below are assumed to be nite-dimensional. A representation (V, ρ) of G over F can be regarded as a left FG-module. The character $\chi_V : FG/[FG, FG] \to F$ can be regarded as a function on G via the standard inclusion $G \hookrightarrow FG$. The character χ_V is a *class function* on G, namely

$$\chi_V(x^{-1}yx) = \chi_V(y), \quad x, y \in G.$$

Indeed, $x^{-1}yx - y = x^{-1}yx - yxx^{-1} \in [FG, FG]$ and these elements generate $[FG, FG]$. One readily veri es the equalities

$$\begin{aligned}
\chi_V(1) &= \dim_F V, \\
\chi_{V\oplus W}(g) &= \chi_V(g) + \chi_W(g), \\
\chi_{V\otimes W}(g) &= \chi_V(g)\chi_W(g), \\
\chi_{\check{V}}(g) &= \chi_V(g^{-1}),
\end{aligned}$$

for all representations V, W of G over F and all $g \in G$ (for the last one, recall the classical fact that a matrix and its transpose have the same trace). Characters arising from irreducible representations are called *irreducible characters*.

Exercise 11.4.1. Give complete proofs of these equalities.

Proposition 11.4.2 (Orthogonality relations for matrix coe cients)**.** *Let (V, ρ), (W, σ) be irreducible representations of G over F. For $\check{v} \otimes v \in \check{V} \otimes V$ and $\check{w} \otimes w \in \check{W} \otimes W$, we have*

$$\sum_{g\in G} \langle \check{v}, \rho(g)v\rangle\langle \check{\sigma}(g)\check{w}, w\rangle = 0.$$

if the representations V and W are not isomorphic. If $(V, \rho) = (W, \sigma)$ is absolutely irreducible, we have

$$\dim_F V \cdot \sum_{g\in G} \langle \check{v}, \rho(g)v\rangle\langle \check{\sigma}(g)\check{w}, w\rangle = |G|\langle \check{v}, w\rangle\langle \check{w}, v\rangle.$$

Here we write $\langle \check{v}, v\rangle$ to denote the evaluation of $\check{v} : V \to F$ at v.

Proof. Consider the element $\mathrm{Hom}_F(V, W)$ given by

$$v \mapsto \langle \check{v}, v\rangle w.$$

We can make it into an intertwining operator by *averaging* over G. More precisely, we create the element

$$f : v \mapsto \sum_{g\in G} \langle \check{v}, \rho(g)(v)\rangle\sigma(g^{-1})w \quad \in W$$

in $\mathrm{Hom}_G(V, W)$. Then $\langle \check{w}, f(v)\rangle$ is equal to

$$\sum_{g\in G} \langle \check{v}, \rho(g)v\rangle\langle \check{\sigma}(g)\check{w}, w\rangle.$$

However $\mathrm{Hom}_G(V,W) = \{0\}$ when V and W are not isomorphic as representations over F. This proves the first assertion.

Assume now $(V,\rho) = (W,\sigma)$ is absolutely irreducible. The element $f \in \mathrm{End}_G(V)$ must be a scalar operator $\lambda \cdot \mathrm{id}$ since V is absolutely irreducible, by Theorem 11.1.5. Taking traces yields

$$\mathrm{Tr}(f) = \dim_F V \cdot \lambda = |G| \cdot \mathrm{Tr}\,[v \mapsto \langle \check{v}, -\rangle w] = |G|\langle \check{v}, w\rangle.$$

This determines the endomorphism $\dim_F V \cdot f$. Evaluation of $\dim_F V \cdot \langle \check{w}, f(v)\rangle$ gives the second assertion. □

In order to simply the exposition, henceforth we work in the framework of *ordinary* representation theory by assuming

$$\boxed{\mathrm{char}(F) \nmid |G|.}$$

Lemma 11.4.3. *Let $G\times G$ act on FG by setting $R(g,h) : a \mapsto gah^{-1}$, so that (FG,R) becomes a representation of $G \times G$. Assume F is a splitting field of G. There is a canonical isomorphism of representations of $G \times G$*

$$(FG,R) \simeq \bigoplus_{V:\text{irred.}} V \boxtimes \check{V}.$$

Furthermore, we have

$$\mathrm{Tr}(R(x,y)) = \sum_C |Z_G(x)|\mathbb{1}_C(x)\mathbb{1}_C(y) = \sum_V \chi_V(x)\chi_{\check{V}}(y)$$

where, $Z_G(x) := \{g \in G : gxg^{-1} = x\}$, C ranges over the conjugacy classes in G, and $\mathbb{1}_C : G \to \{0,1\}$ is its characteristic function.

Proof. In Proposition 11.1.1 we deduced a similar decomposition of the (FG,FG)-bimodule FG. The isomorphism of F-algebras $FG \xrightarrow{\sim} (FG)^{\mathrm{op}}$ induced by $g \mapsto g^{-1}$ transforms the bimodule into that left $FG \times FG = F(G\times G)$-module (FG,R). The division rings D_i in Proposition 11.1.1 reduce to F by our splitting assumption. The first assertion follows.

Observe that $R(x,y)$ permutes the basis G of FG, the fixed point set being $\{\gamma \in G : x\gamma = \gamma y\}$. The fixed-point set is nonempty only when x and y are conjugate, in which case it has the same cardinality as $Z_G(x)$. The second assertion follows at once. □

The trace formula above can be used to deduce many basic results on the representation theory of finite groups: see [26].

Lemma 11.4.4. *Let (V,ρ) be an irreducible representation of G and $e_V \in FG$ be the corresponding idempotent element (cf. the decomposition of FG in Proposition 11.1.1), i.e. left/right multiplication by e_V gives the projection ${}_{FG}FG \twoheadrightarrow \mathrm{End}_F(V)$. Then*

$$e_V = |G|^{-1} n_V \cdot \sum_{g\in G} \chi_V(g^{-1})g$$

where n_V denotes the multiplicity of V in ${}_{FG}FG$. In particular, we have $n_V \neq 0$ in F.

Note that $n_V = \dim_F V$ when V is absolutely irreducible, by Proposition 11.1.1.

Proof. Denote by χ the character of FG as a left FG-module. We immediately see that $\chi(g) = 0$ if $g \neq 1$, and $\chi(1) = |G|$. Write $e_V = \sum_{x \in G} a_x x$. Therefore

$$\chi(e_V g^{-1}) = \sum_{x \in G} a_x \chi(x g^{-1}) = a_g |G|, \quad \forall g \in G.$$

On the other hand, the presence of e_V in $\chi(e_V g^{-1})$ cuts o the contributions outside $V^{\oplus n_V}$ in the decomposition of ${}_{FG}FG$, thus

$$\chi(e_V g^{-1}) = n_V \cdot \chi_V(g^{-1}), \quad \forall g \in G.$$

Hence $a_g |G| = n_V \chi_V(g^{-1})$, as required. □

Theorem 11.4.5 (Orthogonality relations for characters)**.** *Let V and W be irreducible representations of G over F. We have*

$$\sum_{g \in G} \chi_V(g) \chi_W(g^{-1}) = \begin{cases} |G| \dim_F \mathrm{End}_G(V), & V \simeq W; \\ 0, & \textit{otherwise}. \end{cases}$$

Suppose that G splits over F. For $x, y \in G$, we have

$$\sum_{V:\text{irred.}} \chi_V(x) \chi_V(y^{-1}) = \begin{cases} |Z_G(x)|, & \textit{if } x, y \textit{ are conjugate}, \\ 0, & \textit{otherwise}. \end{cases}$$

Proof. For the rst assertion, we calculate $\chi_W(e_V)$ using Lemma 11.4.4. If $V \not\simeq W$, then $e_V \in FG$ acts trivially on W and we get $\sum_{g \in G} \chi_V(g) \chi_W(g^{-1}) = 0$. If $V \simeq W$, then e_V acts as id on W, thereby $\chi_W(e_V) = \chi_V(1) = \dim_F V$. A comparison gives

$$\sum_{g \in G} \chi_V(g) \chi_V(g^{-1}) = |G| n_V^{-1} \dim_F V.$$

Set $D := \mathrm{End}_G(V)$. It remains to show

$$\dim_F V = n_V \dim_F D.$$

Indeed, we have $n_V = \dim_D \mathrm{Hom}(V_D, D_D) = \dim_D V$ by Proposition 11.1.1. The second assertion is even easier: use the Lemma 11.4.3. □

Theorem 11.4.6. *Suppose that G splits over F. The F-vector space of class functions $G \to F$ admits two bases: the irreducible characters χ_V and the characteristic functions $\mathbb{1}_C$ of the conjugacy classes $C \subset G$.*

Proof. Evidently the $\mathbb{1}_C$'s form a basis. On the other hand, by Theorem 11.2.2 the irreducible characters χ_V are linearly independent. It su ces to show that every $\mathbb{1}_C$ can be written as a linear combination of irreducible characters.

Let C be a conjugacy class of G and x an element $y \in C$. Since $gxg^{-1} = y \implies Z_G(x) = gZ_G(y)g^{-1}$ and di erent conjugacy classes are disjoint, Lemma 11.4.3 can be written in the form

$$|Z_G(y)|\mathbb{1}_C(\cdot) = \sum_{V:\text{irreducible}/\simeq} \chi_V(\cdot)\chi_{\check{V}}(y).$$

Note that $|Z_G(y)| \neq 0$ in F since $\mathrm{char}(F) \nmid |G|$. Hence $\mathbb{1}_C$ lies in the linear span of irreducible characters. □

Note that the proof actually gives the transition matrix between two bases in terms of character values.

Corollary 11.4.7. *Suppose that G splits over F. Then the number of irreducible representations of G over F equals that of conjugacy classes in G. Moreover, we have*

$$|G| = \sum_{V:\text{irred.}} n_V \dim_F V = \sum_{V:\text{irred.}} (\dim_F V)^2;$$

the rst equality actually holds without assuming G split. Here n_V stands for the multiplicity of V in ${}_{FG}FG$.

Proof. The rst assertion has just been proved. The second one follows from Proposition 11.1.1. □

Exercise 11.4.8. Without the splitting assumption, show that
- ⋆ the number of irreducible representations is less or equal then that of conjugacy classes;
- ⋆ $|G| = \sum_{V:\text{irred.}} n_V \cdot \dim_F V \leq \sum_{V:\text{irred.}} (\dim_F V)^2$.

Hint. Either pass to the splitting eld, or use the decomposition in Proposition 11.1.1 and calculate the dimension of $Z(FG)$.

Exercise 11.4.9. Let $R_F(G)$ denote the free abelian group generated by the isomorphism classes of irreducible representations of G over F. The elements of $R_F(G)$ are thus formal $\mathbb{Z}$-linear combinations $\sum_{[V]} a_V[V]$ of classes (denoted by $[\cdot]$). De ne a binary operation on $R_F(G)$ by

$$[V] \cdot [W] := [V \otimes W]$$

on generators, and extend it to $R_F(G)$ by linearity. Show that $(R_F(G), +, \cdot)$ is an associative ring, called the *representation ring* of G. Relate it to the characters by $\sum_V a_V[V] \mapsto \sum_V a_V\chi_V$.

The elements in $R_F(G)$ are called *virtual characters*.

Exercise 11.4.10. Determine the splitting elds for the cyclic groups $\mathbb{Z}/n\mathbb{Z}$.

Example 11.4.11. Here the base eld is $F := \mathbb{Q}$. Consider the group $Q := \{\pm 1, \pm i, \pm j, \pm k\}$ of quaternion units. It is the group of order 8 subject to the relations $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, and that ± 1 is central in Q. The commutator subgroup of Q is $\{\pm 1\}$ and $Q/\{\pm 1\} \simeq (\mathbb{Z}/2\mathbb{Z})^2$. Thus we get four irreducible 1-dimensional representations $Q \twoheadrightarrow (\mathbb{Z}/2\mathbb{Z})^2 \to \{\pm 1\}$.

Let $\mathbb{H} = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$ be Hamilton's quaternion algebra over $\mathbb{Q}$, on which Q acts by left multiplication. Since Q spans $\mathbb{H}$ and $\mathbb{H}$ is a division algebra, $\mathbb{H}$ is a 4-dimensional irreducible representation of Q. By the second equality in Exercise 11.4.8, these five representations exhaust the irreducibles of Q over $\mathbb{Q}$, each occurring with multiplicity one in $\mathbb{Q}Q$.

The last representation $\mathbb{H}$ is not absolutely irreducible. Choose any quadratic field extension $E/\mathbb{Q}$ such that $E \otimes_{\mathbb{Q}} \mathbb{H} \simeq M_2(E)$, we see that $\mathbb{H}_E \simeq E^2 \oplus E^2$ as EQ-modules. By the way, there are plenty of minimal splitting fields of Q: any quadratic extension $E/\mathbb{Q}$ ramified at ∞ and 2 (in the parlance of algebraic number theory) will do.

LECTURE 12

INDUCTION OF REPRESENTATIONS

We set out to address the important operation of *induction of representations*.

12.1 Change of rings

Let $A, B, \Bbbk$ be rings and consider bimodules

$$ {}_AN_B, \quad {}_BM_\Bbbk, \quad {}_AL_\Bbbk. $$

The reader can safely disregard the ring $\Bbbk$ here: one usually takes $\Bbbk = F$ when talking about F-algebras, or simply puts $\Bbbk = \mathbb{Z}$ in order to make it irrelevant.

Lemma 12.1.1. *There is a canonical isomorphism*

$$ \mathrm{Hom}_{(A,\Bbbk)-\boldsymbol{Mod}}({}_AN \underset{B}{\otimes} M_\Bbbk, {}_AL_\Bbbk) \simeq \mathrm{Hom}_{(B,\Bbbk)-\boldsymbol{Mod}}({}_BM_\Bbbk, \mathrm{Hom}({}_AN, {}_AL)) $$

between right $\Bbbk$-modules, which is functorial in (N, M, L), i.e. it de nes an isomorphism between functors from

$$ ((A,B)-\boldsymbol{Mod})^{\mathrm{op}} \times ((B,\Bbbk)-\boldsymbol{Mod})^{op} \times ((A,\Bbbk)-\boldsymbol{Mod}) $$

to $\boldsymbol{Mod}-\Bbbk$. Here $\mathrm{Hom}({}_AN, {}_AL)$ operates on the right of N, its $(B,\Bbbk)$-bimodule structure is de ned by the familiar convention

$$ bft : n \mapsto ((nb)f)t, \quad b \in B, f \in \mathrm{Hom}({}_AN, {}_AL), t \in \Bbbk, $$

and both Hom-sets admit obvious right $\Bbbk$-module structures

Proof. By the categorical characterization of $- \underset{B}{\otimes} -$, the left-hand side is canonically isomorphic to the set $\mathbf{Bil}(N, M; L)$ of B-balanced maps

$$ T : N \times M \to L. $$

An element $\varphi \in \mathrm{Hom}({}_AN \underset{B}{\otimes} M_\Bbbk, {}_AL_\Bbbk)$ corresponds to the balanced map $T_\varphi : (n, m) \mapsto \varphi(n \otimes m)$; recall that T being balanced means

- ⋆ $T(nb, m) = T(n, bm)$ for all $n \in N$, $m \in M$;
- ⋆ T is additive in N and M;
- ⋆ $T(an, mt) = aT(n, m)t$ for all $a \in A$, $t \in \Bbbk$.

On the other hand, we have a canonical isomorphism

$$\mathbf{Bil}(N, M; L) \simeq \mathrm{Hom}({}_B M_{\Bbbk}, \mathrm{Hom}({}_A N, {}_A L))$$

de ned as follows: to $T \in \mathbf{Bil}(N, M; L)$ is associated the map

$$m \mapsto [n \mapsto T(n, m)], \quad m \in M, n \in N.$$

It is immediate that the linearity conditions with respect to A, B and $\Bbbk$ translate precisely into the de nitions of $\mathbf{Bil}(M, N; L)$. The assertion follows at once. □

De nition 12.1.2. Given a ring homomorphism $A \to B$, we deduce two functors P and I from the category of $(A, \Bbbk)$-bimodules to that of $(B, \Bbbk)$-bimodules.

- ⋆ Take $N := {}_B B_A$, and de ne $P = P_{A\to B} := N \underset{A}{\otimes} - = B \underset{A}{\otimes} -$.
- ⋆ Take $N := {}_A B_B$, and de ne $I = I_{A\to B} := \mathrm{Hom}({}_A N, -) = \mathrm{Hom}({}_A B, -)$; we de ne the $(B, \Bbbk)$-bimodule structure on this Hom-set as above.

For every $(B, \Bbbk)$-bimodule L, we may regard L as an $(A, \Bbbk)$-bimodule by letting A acts on L via $A \to B$. This can also be understood by the identi cation

$$\mathrm{Hom}({}_B B, {}_B L) \xrightarrow{\sim} L$$

given by evaluation at $1 \in B$; the left-hand side admits an $(A, \Bbbk)$-bimodule structure from ${}_B B_A$. This is usually called a *forgetful functor*, since the A-module structure is coarser than the B-module structure.

Exercise 12.1.3. Check the details.

Proposition 12.1.4. *There are canonical isomorphisms of right $\Bbbk$-modules*

$$\mathrm{Hom}(L, I(M)) \simeq \mathrm{Hom}({}_A L, M),$$
$$\mathrm{Hom}(P(M), L) \simeq \mathrm{Hom}(M, {}_A L),$$

which are functorial in ${}_A M_{\Bbbk}$ and ${}_B L_{\Bbbk}$.

Proof. For the rst isomorphism, apply Lemma 12.1.1 with $N = {}_A B_B$ to deduce functorial isomorphisms

$$\mathrm{Hom}({}_A L, M) \simeq \mathrm{Hom}({}_A B \underset{B}{\otimes} L, {}_A M) \simeq \mathrm{Hom}({}_B L, \mathrm{Hom}({}_A B, M)).$$

For the second one, the same Lemma with $N = {}_B B_A$ yields

$$\mathrm{Hom}({}_B B \underset{A}{\otimes} M, L) \simeq \mathrm{Hom}({}_A M, \mathrm{Hom}({}_B B, L)) \simeq \mathrm{Hom}(M, {}_A L).$$

□

These isomorphisms characterize I (resp. P) as the right (resp. left) *adjoint* of the forgetful functor $L \mapsto {}_AL$: see [12, §1.8] for a review on adjoint functors. These three functors are, in some sense, the master functors in the our study.

Proposition 12.1.5. *Given rings A, B, C and homomorphisms $A \to B \to C$, we denote by $I_{A\to B}$, $P_{B\to C}$, etc., to denote the corresponding functors. There are canonical isomorphisms*

$$I_{B\to C} \circ I_{A\to B} \simeq I_{A\to C},$$
$$P_{B\to C} \circ P_{A\to B} \simeq P_{A\to C}.$$

Proof. The first one comes from Lemma 12.1.1, namely

$$\mathrm{Hom}({}_BC, \mathrm{Hom}({}_AB, -)) \simeq \mathrm{Hom}({}_A(B \underset{B}{\otimes} C), -) \simeq \mathrm{Hom}({}_AC, -)$$

as functors A−**Mod** → **Mod**−$\Bbbk$. The second one is even easier: use the usual constraints for $\otimes$-functor to get $C \underset{B}{\otimes} (B \otimes A-) \simeq C \underset{A}{\otimes} -$. □

Remark 12.1.6. A more conceptual approach, albeit less explicit, is to note the obvious identity ${}_A({}_B(-)) = {}_A(-)$ for forgetful functors, and then apply the Proposition 12.1.4 which characterizes P and I.

12.2 Induced representations

In this section, we fix a field F, a group G and a subgroup $H \hookrightarrow G$. Therefore we obtain the inclusion $FH \to FG$ of group algebras over F. In what follows, representations are always taken over F.

Recall that the *forgetful functor* from FG-**Mod** to FH-**Mod** corresponds to the restriction of representations from G to H, denoted by $\mathrm{Res}^G_H : \mathbf{Rep}_F(G) \to \mathbf{Rep}_F(H)$. It is natural to study the representations of G by looking at their decomposition upon restriction to H. More precisely, given a representation W of H, how to construct a representation of G that spins off a W after applying Res^G_H, in the most economical ways?

Definition 12.2.1 (Induced representations)**.** Define functors $\mathbf{Rep}_F(H) \to \mathbf{Rep}_F(G)$ by setting, for all representation (W, σ) of H:

$$\mathrm{Ind}^G_H(W) := \{f : G \to W,\ \forall h \in H,\ f(hg) = \sigma(h)(f(g))\},$$
$$\mathrm{ind}^G_H(W) := \left\{f \in \mathrm{Ind}^G_H(W) : \mathrm{Supp}(f) \text{ is finite mod } H\right\}.$$

Here $\mathrm{Supp}(f) := \{x : f(x) \neq 0\}$ is the *support* of f, and G acts on these function spaces via *right translation* $f(\cdot) \mapsto f(\cdot g)$. Given $\varphi \in \mathrm{Hom}_H(W_1, W_2)$, the corresponding morphisms $\mathrm{Ind}^G_H(W_1) \to \mathrm{Ind}^G_H(W_2)$ is given by applying φ pointwise to the function spaces. Note that $\mathrm{ind}^G_H(-) \hookrightarrow \mathrm{Ind}^G_H(-)$.

Remark 12.2.2. The notation $W \mapsto W^G$ for $\mathrm{ind}^G_H(-)$ is prevalent in the literature; some authors write c-Ind^G_H instead. The restriction functor $\mathrm{Res}^G_H(-)$ is sometimes denoted as $V \mapsto V_H$.

We are going to relate these constructions to the abstract change-of-ring functors in De nition 12.1.2. Observe that every left FG-module can be turned into an (FG, F)-bimodule; the ring $\Bbbk$ in the previous section is taken to be F.

Lemma 12.2.3. *Upon identifying the categories of left FH (resp. FG)-modules and the representations of H (resp. of G), there are isomorphisms of functors*

$$\mathrm{Ind}_H^G \xrightarrow{\sim} I = I_{FH\to FG},$$
$$\mathrm{ind}_H^G \xrightarrow{\sim} P = P_{FH\to FG}.$$

The construction of $\mathrm{Ind}_H^G \xrightarrow{\sim} I$ goes as follows. For every $f : G \to W$ in $\mathrm{Ind}_H^G(W)$ we associate the homomorphism $\varphi \in \mathrm{Hom}({}_{FH}FG, {}_{FH}W)$ by $g \mapsto f(g), \forall g \in G$. For $\mathrm{ind}_H^G \xrightarrow{\sim} P$, given $f : G \to W$ in $\mathrm{ind}_H^G(W)$ we associate $\sum_{\bar{g}\in G/H} g^{-1} \otimes f(g) \in FG \underset{FH}{\otimes} W$, where $g \in G$ is any element in the coset $\bar{g} \in G/H$.

Proof. The inverses are given as follows. For $\varphi \in \mathrm{Hom}({}_{FH}FG, {}_{FH}W)$ we obtain $f : G \to W$ by restricting φ to $G \subset FG$. On the other hand, note that

$$FG \underset{FH}{\otimes} W = \bigoplus_{\bar{g}\in G/H} \bar{g}(FH) \underset{FH}{\otimes} W.$$

Given $\bar{g} \in G/H$, the choice of a representative g in the coset $\bar{g}$ furnishes an isomorphism $\bar{g}(FH) \underset{FH}{\otimes} W = g \otimes W \xrightarrow{\sim} W$. Thus an element in $FG \underset{FH}{\otimes} W$ induces a function $G \to W$, which gives the inverse. All these morphisms are evidently functorial in W and respect FG-module structures. □

Proposition 12.2.4 (Frobenius reciprocity)**.** *There are functorial isomorphisms*

$$\mathrm{Hom}_G(\mathrm{ind}_H^G(-), -) \simeq \mathrm{Hom}_H(-, \mathrm{Res}_H^G(-)),$$
$$\mathrm{Hom}_G(-, \mathrm{Ind}_H^G(-)) \simeq \mathrm{Hom}_H(\mathrm{Res}_H^G(-), -),$$

i.e. ind_H^G *is a left adjoint of* Res_H^G *and* Ind_H^G *is a right adjoint thereof.*

Proof. Apply the Lemma 12.2.3 and Proposition 12.1.4. □

Exercise 12.2.5. Describe these isomorphisms more explicitly. For example, the isomorphism

$$\mathrm{Hom}_G(V, \mathrm{Ind}_H^G(W)) \xrightarrow{\sim} \mathrm{Hom}_H(\mathrm{Res}_H^G(V), W)$$

is given by $f \mapsto [v \mapsto f(v)(1)]$; its inverse is $\psi \mapsto [v \mapsto \psi(gv)]$.

Corollary 12.2.6. *We have* $\mathrm{ind}_H^G(-) = \mathrm{Ind}_H^G(-)$ *whenever* $(G : H)$ *is nite. This is the case when G is a nite group.*

Proof. Immediate from the de nitions. □

Corollary 12.2.7 (Transitivity of inductions)**.** *Let $K \subset H \subset G$ be groups. We have* $\mathrm{Ind}_H^G \mathrm{Ind}_K^H \simeq \mathrm{Ind}_K^G$ *and* $\mathrm{ind}_H^G \mathrm{ind}_K^H \simeq \mathrm{ind}_K^G$.

Proof. Apply the Lemma 12.2.3 and Proposition 12.1.5. Alternatively, we may de ne

$$\mathrm{Ind}_H^G\mathrm{Ind}_K^H(W) \rightleftarrows \mathrm{Ind}_K^G(W)$$

$$\left[\varphi : G \to \mathrm{Ind}_K^H(W)\right] \longmapsto [G \ni g \mapsto \varphi(g)(1) \in W]$$

$$[g \mapsto [H \ni h \mapsto \psi(hg)]] \longmapsfrom [\psi : G \to W]\,.$$

The details are left to the reader. The case of ind_K^G can be treated in a similar manner. □

12.3 Mackey's criterion

The eld F is kept xed. In order to construct representations of a group G from smaller groups by the recipe above, it is important to know to decomposition of induced representations. In particular, one would like to know when is an induced representation irreducible.

We begin with an important restriction-induction formula due to G. Mackey. Some preliminaries are in order.

De nition 12.3.1. Let (W, σ) be a representation of a group H and $w : H' \xrightarrow{\sim} H$ be an isomorphism. We obtain thus a representation (W^w, σ^w) of H' by pulling back via w, namely $W^w = W$ as vector spaces and $\sigma^w(h') := \sigma(w(h'))$ for all $h' \in H'$. In what follows, w will be obtained by conjugation $x \mapsto wxw^{-1}$ using an element w in an ambient group G containing both H and H'; actually this forces $H' = H^w := w^{-1}Hw$. We shall retain the notation (W^w, σ^w) in that case.

Lemma 12.3.2. *Let G be a group and K, H be subgroups with nite index. Let (W, σ) be an irreducible representation of H over F. For any $w \in G$, let (W^w, σ^w) be the pull-back of (W, σ) to $H^w := w^{-1}Hw$ as above. There is an isomorphism of representations of H*

$$\mathrm{Res}_K^G\mathrm{ind}_H^G(W) \xrightarrow{\sim} \bigoplus_{\bar{w}\in H\backslash G/K} \mathrm{ind}_{H^w\cap K}^K\mathrm{Res}_{H^w\cap K}^{H^w}(W^w)$$

where $w \in G$ is any representative of double coset $\bar{w}$. The morphism is functorial in W.

The summand corresponding to $\bar{w}$ is easily seen to be independent (up to isomorphism) of the choice of w.

Proof. Firstly, recall that $\mathrm{ind}_H^G(W)$ is realized as a space of functions $G \to W$ with compact support modulo H, on which G acts by right translation. For each double coset $HwK \subset G$, de ne

$$\mathcal{F}_w := \{f \in \mathrm{ind}_H^G(W) : \mathrm{Supp}(f) \in HwK\}.$$

Each of them is invariant under the K-action restricted from that of G. Hence

$$\mathrm{Res}_K^G\mathrm{ind}_H^G(W) = \bigoplus_{\bar{w}\in H\backslash G/K} \mathcal{F}_w \quad \text{as representations of } K.$$

It remains to recognize the summands $\mathcal{F}_w$. Fix w, we have homomorphisms between representations of K:

$$\begin{array}{lcl}
\mathcal{F}_w = \{f : HwK \to W : \forall h \in H,\ f(h\cdot) = \sigma(h)(f(\cdot))\} & \ni & f \\
\simeq \downarrow & & \downarrow \\
\left\{f' : wK \to W : \forall h \in H \cap wKw^{-1},\ f'(h\cdot) = \sigma(h)(f'(\cdot))\right\} & \ni & f' := f|_{wK} \\
\simeq \downarrow & & \downarrow \\
\{f'' : K \to W : \forall k \in H^w \cap K,\ f''(k\cdot) = \sigma^w(k)(f''(\cdot))\} & \ni & f''(\cdot) := f'(w\cdot).
\end{array}$$

Here the functions are implicitly assumed to have finite support modulo left multiplication by H, $H \cap wKw^{-1}$ and $H^w \cap K$, respectively. The first arrow is an isomorphism, the inverse being $f' \mapsto [f(hx) := \sigma(h)f'(x)]$ for all $x \in wK$, $h \in H$; one readily verifies that $f' \mapsto f$ well-defined. The second arrow is a "transport of structure" isomorphism in Bourbaki's jargon; it is again a routine check. The bottom row is exactly $\mathrm{ind}_{H^w\cap K}^{K}\mathrm{Res}_{H^w\cap K}^{H^w}(W^w)$ and the required functoriality is clear. This completes the proof. □

Exercise 12.3.3. Let N be a normal subgroup of G of finite index, and W be a representation of N. Show that $\mathrm{Res}_N^G\mathrm{ind}_N^G(W)$ is

$$\mathrm{Res}_N^G\mathrm{ind}_N^G(W) \simeq \bigoplus_{\bar{g}\in G/N} W^g$$

where g is a representative in G of $\bar{g}$.

Theorem 12.3.4. *Let G be a finite group, H a subgroup of G, and assume that* $\mathrm{char}(F) \nmid |G|$ *and F is the splitting field for G and H. Let W be an irreducible representation of H, then* $\mathrm{ind}_H^G(W)$ *is irreducible if and only if W^w and W "do not interact" in the sense that*

$$\mathrm{Hom}_{H^w\cap H}\left(\mathrm{Res}_{H^w\cap H}^{H}(W^w), \mathrm{Res}_{H^w\cap H}^{H}(W)\right) = \{0\}$$

for every $w \in G$, $w \notin H$.

Proof. By Maschke's theorem and the splitting assumption, $\mathrm{ind}_H^G(W)$ is irreducible if and only if $\mathrm{End}_G(\mathrm{ind}_H^G(W)) = F$. Apply the previous Lemma together with Frobenius reciprocity (Proposition 12.2.4) to the endomorphism space:

$$\begin{aligned}
\mathrm{End}_G(\mathrm{ind}_H^G(W)) &\simeq \mathrm{Hom}_H(\mathrm{Res}_H^G\mathrm{ind}_H^G(W), W) \\
&= \bigoplus_{\bar{w}\in H\backslash G/H} \mathrm{Hom}_H(\mathrm{ind}_{H^w\cap H}^{H}\mathrm{Res}_{H^w\cap H}^{H^w}(W^w), W) \\
&= \bigoplus_{\bar{w}\in H\backslash G/H} \mathrm{Hom}_{H^w\cap H}(\mathrm{Res}_{H^w\cap H}^{H^w}(W^w), \mathrm{Res}_{H^w\cap H}^{H}(W)),
\end{aligned}$$

where we have used the property that $\mathrm{ind}(\cdots) = \mathrm{Ind}(\cdots)$ for finite groups. For the identity double coset $\bar{w} = H$ we get the summand $\mathrm{End}_H(W) = F$, hence $\mathrm{ind}_H^G(W)$ is irreducible if and only if the other Hom-sets are all zero. □

12.4 Induced characters

In this section, G will be assumed to be a finite group, $H \subset G$ is a subgroup and F is an arbitrary field. The representations hereafter are assumed to be finite-dimensional over F. Recall that for a representation V of G (resp. W of H), we have defined the character χ_V (resp. χ_W) as a *class function* on G (resp. H).

Note that the group G acts on the coset space G/H by left multiplication. The elements in G/H will be denoted as $\bar{g}$, etc., and their representatives in G will be denoted as g, etc.

Proposition 12.4.1. *Let W be a representation of H. For every $x \in G$, we have*

$$\chi_{\mathrm{ind}_H^G(W)}(x) = \sum_{\substack{\bar{g}\in G/H \\ x\bar{g}=\bar{g}}} \chi_W(g^{-1}xg)$$

where $g \in G$ is any representative of the coset $\bar{g}$.

In particular, $\chi_{\mathrm{ind}_H^G(W)}(x) \neq 0$ only if x is conjugate to some element of H.

Proof. Write the underlying F-vector space of $\mathrm{ind}_H^G(W)$ as

$$FG \underset{FH}{\otimes} W = \bigoplus_{\bar{g}\in G/H} \bar{g}FH \underset{FH}{\otimes} W.$$

The element x permutes the elements of G/H and acts on $FG \underset{FH}{\otimes} W$ through the first tensor slot, hence the direct summands above are permuted accordingly. Only those $\bar{g} \in G/H$ with $x\bar{g} = \bar{g}$ contribute to $\mathrm{Tr}\left(x | FG \underset{FH}{\otimes} W\right)$.

Choose any representative $g \in G$ of $\bar{g}$, so that $x\bar{g} = \bar{g}$ if and only if $xgH = gH$, i.e. $g^{-1}xg \in H$ (Note: this justifies the formula in the Proposition). Moreover, $x \cdot (g \otimes w) = gg^{-1}xg \otimes w = g \otimes (g^{-1}xg)w$ whenever $g^{-1}xg \in H$, thus the action of x on $g \otimes W$ is the same that of $g^{-1}xg$ on W, after identifying $g \otimes W$ and W. Summing over all the x-fixed elements $\bar{g} \in G/H$ yields the character formula. □

Corollary 12.4.2. *We have* $\dim_F(\mathrm{ind}_H^G(W)) = (G : H) \dim_F W$.

Proof. This can be deduced directly from the definitions. Here we derive it from 12.4.1 by putting $x = 1$. □

Hereafter we assume $\mathrm{char}(F) \nmid |G|$. Let $\xi, \eta : G \to F$ be class functions. We define

$$(\xi|\eta)_G := |G|^{-1} \sum_{g\in G} \xi(g)\eta(g^{-1}).$$

From the orthogonality relations for characters we deduce

$$\dim_F \mathrm{Hom}_G(V_1, V_2) = (\chi_{V_1}|\chi_{V_2})_G$$

for any representations V_1, V_2 of G.

The formula in Proposition 12.4.1 can be used to de ne the induction ind_H^G of a *class function* from H to G. Similarly, we may de ne the *restriction of class functions* from G to H, which is simply $\mathrm{Res}_H^G : f \mapsto f|_H$. It re ects the restriction of representations on the level of characters.

Below is the classical form of Frobenius reciprocity expressed in terms of characters. Remarkably, this highly powerful tool was established (with $F = \mathbb{C}$) at the very beginning of representation theory (1898).

Figure 12.1: René Magritte. *La clairvoyance*. Brussels, 1936.

Corollary 12.4.3. *Let V (resp. W) be a representation of G (resp. H) over F, we have*

$$(\chi_V|\mathrm{ind}_H^G(\chi_W))_G = (\mathrm{Res}_H^G(\chi_V)|\chi_W)_H.$$

Proof. From the discussion above, this follows from Proposition 12.2.4 by taking $\dim_F$. □

12.5 An application: supersolvable groups

In this section, groups are always nite and the representations are assumed to be nite-dimensional over F. Furthermore, we assume that $\mathrm{char}(F) \nmid |G|$ and F is a splitting eld, for every group G in sight.

De nition 12.5.1. A nite group G is called *supersolvable* if there exists an ascending chain $\{1\} = G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_n = G$ of normal subgroups $G_i \lhd G$, such that G_i/G_{i-1} is cyclic for all $1 \leq i \leq n$.

Abelian groups are supersolvable. Quotients and subgroups of a supersolvable group are still supersolvable.

Lemma 12.5.2. *Let G be a non-abelian supersolvable group. There exists a normal, abelian subgroup which is not contained in the center $Z(G)$ of G.*

Proof. The group $\bar{G} := G/Z(G)$ is again supersolvable. Take the first subgroup $\bar{G}_1$ (cyclic!) in an ascending chain in $\bar{G}$ that witnesses its supersolvability. The inverse image A of $\bar{G}_1$ in G is normal, properly containing $Z(G)$, and abelian. Indeed, A is generated by $Z(G)$ together with *one* element whose image generates $\bar{G}_1$. □

Lemma 12.5.3 (Clifford). *Let G be a finite group and $N \lhd G$ be a normal subgroup. Let (V, ρ) be an irreducible representation of G. We have*

$$\mathrm{Res}^G_N(V) \simeq \left(\bigoplus_{i=1}^{n} (W_i)^{\oplus m} \right)$$

where $W_1, \ldots, W_n$ are mutually non-isomorphic irreducible representations of N, and G permutes the subspaces $W_i^{\oplus m}$. Furthermore, $V \simeq \mathrm{ind}^G_H(W')$ where $W' := W_1^{\oplus m}$ and $H := \{g \in G : \rho(g)W_1 \simeq W_1 \text{ in } \mathbf{Rep}_F(N)\}$, $[G : H] = n$.

Proof. Pick any irreducible subrepresentation W of $\mathrm{Res}^G_N(V)$. By the irreducibility of V, we see $\mathrm{Res}^G_N(V) = \sum_{\bar{g} \in G/N} \rho(g)W$. It is crucial to observe $\rho(g)U \simeq U^{g^{-1}}$ in $\mathbf{Rep}_F(N)$ (notation in §12.3) for any subrepresentation U of $\mathrm{Res}^G_N(V)$, since $N \lhd G$. Set $H := \{g \in G : \rho(g)W \simeq W\} \rhd N$. We obtain

$$W' := \sum_{\bar{h} \in H/N} \rho(h)W \simeq W^{\oplus m}, \quad \text{for some } m,$$

$$\mathrm{Res}^G_N(V) = \sum_{\bar{g} \in G/H} \rho(g)W' \simeq \sum_{\bar{g} \in G/H} (W^{\oplus m})^{g^{-1}} \simeq \sum_{\bar{g} \in G/H} (\rho(g)W)^{\oplus m}.$$

The last sum is direct and the choices of representatives g, h are irrelevant. It remains to use

$$FG \otimes_{FH} W' \xrightarrow{\sim} \bigoplus_{\bar{g} \in G/H} \rho(g)(W') = V \quad \text{in } FG - \mathbf{Mod}$$

defined by $g \otimes v \mapsto \rho(g)v$. □

Exercise 12.5.4. Let $\rho : G \twoheadrightarrow \bar{G}$ be a surjective homomorphism, $\bar{H}$ a subgroup of $\bar{G}$ and σ a representation of $\bar{H}$. Set $H := \rho^{-1}(\bar{H})$. One may regard σ (resp. $\mathrm{Ind}^{\bar{G}}_{\bar{H}}(\sigma)$) as a representation of H (resp. of G) by pulling back via ρ. Show that there is a natural isomorphism

$$\mathrm{Ind}^G_H(\sigma) \simeq \mathrm{Ind}^{\bar{G}}_{\bar{H}}(\sigma)$$

of representations of G.

Exercise 12.5.5. Show that the irreducible representations of abelian groups over F (assumed to be a splitting field) are all 1-dimensional. **Hint**. Here the group algebra over F must split into a direct product of F's.

Theorem 12.5.6. *Let G be a supersolvable group. Every irreducible representation of G over F is induced from an 1-dimensional representation of some subgroup.*

Proof. Let (V, ρ) be an irreducible representation of G over F. We may assume $\ker(\rho) = \{1\}$ upon passing to $G/\ker(\rho)$ and applying Exercise 12.5.4. If G is abelian, Exercise 12.5.5 will conclude our proof. Otherwise we may take a non-central abelian normal subgroup $A \lhd G$ by virtue of Lemma 12.5.2. Consider $\mathrm{Res}^G_A(V)$. Were it isotypic (i.e. $n = 1$ in the Lemma), A would act on V by scalar multiplication as A is abelian, so $\rho(A) \subset Z(\rho(G))$ which is contradictory since $\ker(\rho) = \{1\}$. Therefore V is of the form $\mathrm{ind}^G_H(W)$ where $H \subsetneq G$. Certainly W itself must be irreducible, and H is also supersolvable. We conclude by induction on $|G|$ and by Corollary 12.2.7. □

The representations induced from 1-dimensional ones are called *monomial representations*; a group whose irreducibles are all monomial is called an *M-group*. We conclude that supersolvable groups are M-groups.

Exercise 12.5.7. Describe the irreducible representations of the symmetric group $\mathfrak{S}_3$ over splitting fields.

LECTURE 13

REPRESENTATIONS OF SYMMETRIC GROUPS

We deal with the ordinary representation theory of the symmetric groups in this lecture. The approach adopted here is largely combinatorial; we shall follow [13, 22] rather closely. Another prevalent approach is based on the use of idempotents, see eg. [12, §5.4].

13.1 Review: the symmetric groups

De nition 13.1.1. Let X be a nite set. The *symmetric group* $\mathfrak{S}_X$ is the group of bijections $X \to X$ under composition: $f \cdot g = f \circ g$. If $|X| = n$, we may identify X with the set $\{1, \ldots, n\}$ and write $\mathfrak{S}_n$ instead. Fix $n \in \mathbb{Z}_{\geq 1}$. Elements in $\mathfrak{S}_n$ are called *permutations* of the letters $1, \ldots, n$.

It is often convenient to represent an element $\sigma \in \mathfrak{S}_n$ as a product of disjoint *cycles* by decomposing $\{1, \ldots, n\}$ into orbits under σ. A cycle is written in the form

$$(\lambda_1 \cdots \lambda_m) \in \mathfrak{S}_n$$

where $\lambda_1, \ldots \lambda_m \in \{1, \ldots, n\}$ (unique up to cyclic permutations); it maps

$$\lambda_1 \mapsto \lambda_2 \mapsto \cdots \mapsto \lambda_{m+1} \mapsto \lambda_1$$

whereas the other letters are left intact. The integer m above is called the *length* of the cycle. Two cycles are called disjoint if the λ_i's thereof do not overlap. Let us record some basic facts.

1. Disjoint cycles commute in $\mathfrak{S}_n$.

2. Every element $\sigma \in \mathfrak{S}_n$ can be written as a product $\sigma = \tau_1 \cdots \tau_r$ where the τ_i are disjoint cycles (we may remove those of length 1); they are unique up to order. The collection of the lengths of $\tau_1, \ldots \tau_r$ is called the *cycle type* of σ.

3. Let $\sigma \in \mathfrak{S}_n$ and τ be a cycle; without loss of generality we may assume $\tau = (12\cdots k)$, $k \leq n$, then the conjugate $\sigma\tau\sigma^{-1}$ is again a cycle, given by

$$\sigma(12\cdots k)\sigma^{-1} = (\sigma(1)\sigma(2)\cdots\sigma(k)).$$

4. Consequently, the conjugacy classes in $\mathfrak{S}_n$ are in bijection with the cycle types, which are in turn in bijection with the *partitions* of n. Recall that a partition λ of n is a datum $\lambda = (\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r)$, $\lambda_i \in \mathbb{Z}_{\geq 1}$ for each i, such that $\lambda_1 + \cdots + \lambda_r = n$.

Notation 13.1.2. As is customary, we write $\lambda \vdash n$ to mean that λ is a partition of n.

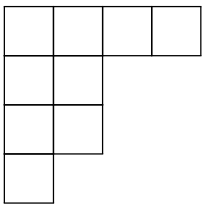
Cycles of length 2 are called *transpositions*, i.e. of the form (ab) with $1 \leq a, b \leq n$. Transpositions of the form $(k\ k+1)$ generate $\mathfrak{S}_n$.

Moreover, we have the *sign homomorphism* $\operatorname{sgn} : \mathfrak{S}_n \to \{\pm 1\}$, characterized by $\operatorname{sgn}(\tau) = -1$ for every transposition τ.

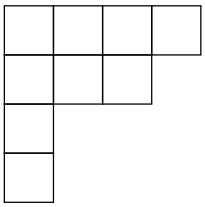
13.2 Young diagrams, tableaux and tabloids

We have seen that the conjugacy classes of $\mathfrak{S}_n$ are in bijection with the partitions $\lambda = (\lambda_1 \geq \cdots \geq \lambda_r) \vdash n$. The latter can be conveniently visualized via the *Young diagram*[1]: one puts λ_1 boxes in the first row, λ_2 boxes in the second row, etc. For example, the partition $\lambda = (4 \geq 2 \geq 2 \geq 1) \vdash 9$ is represented as

(13.1)

$\lambda =$ 

Two partitions λ, μ are called *conjugate* if their Young diagrams are related by interchanging rows and columns; in this case we write $\mu = \bar{\lambda}$. For example, the conjugate of the $\lambda = (4 \geq 2 \geq 2 \geq 1)$ is $\bar{\lambda} := (4 \geq 3 \geq 1 \geq 1)$, visualized as

$\bar{\lambda} =$ 

A *Young tableau* of shape λ is the Young diagram corresponding to λ, say with n boxes, in which the integers $1, \ldots, n$ are filled without repetition. Taking up the example (13.1), we may fill it in the following manner

(13.2)

$t =$

9	3	4	2
5	7		
1	6		
8			

[1]Named after the British mathematician Alfred Young; also known as Ferrers diagram.

The group $\mathfrak{S}_n$ acts on the set of Young tableaux with n boxes by permuting the numbers therein. For a given tableau t, de ne the *row stabilizer* R_t as the subgroup of elements in $\mathfrak{S}_n$ which x each row set-wise. In the example (13.2) we have $R_t = \mathfrak{S}_{\{2,3,4,9\}} \times \mathfrak{S}_{\{5,7\}} \times \mathfrak{S}_{\{1,6\}}$ viewed as a subgroup of $\mathfrak{S}_9$.

Two tableaux with n boxes are called row equivalent if $t_1 = \sigma t_2$ for $\sigma \in R_{t_2}$. This is easily seen to be an equivalence relation which does not alter the shapes. A row equivalence class of tableaux of shape λ is called a *tabloid* of shape λ. The tabloid containing a tableau t is denoted by $\{t\}$. Tabloids are commonly visualized by removing the vertical edges in the tableau. For instance, for t as in (13.2) we shall write

$$\{t\} = \begin{array}{|cccc|}\hline 9 & 3 & 4 & 2 \\ \hline 5 & 7 \\ \cline{1-2} 1 & 6 \\ \cline{1-2} 8 \\ \cline{1-1}\end{array}$$

Again, $\mathfrak{S}_n$ acts on the set of tabloids of a given shape via $\sigma\{t\} = \{\sigma t\}$. Likewise we may de ne column equivalence and the column stabilizer C_t of a tableau t.

De nition 13.2.1. Given $\lambda = (\lambda_1 \geq \cdots)$ and $\mu = (\mu_1 \geq \cdots)$ such that $\lambda, \mu \vdash n$, we say λ dominates μ, written as $\lambda \rhd \mu$, if

$$\sum_{i \leq k} \lambda_i \geq \sum_{i \leq k} \mu_i, \quad \forall k \in \mathbb{Z}_{\geq 1}.$$

Here we may impose $\lambda_i = 0$ for i su ciently large; the same for μ_i.

The dominance relation of partitions or Young diagrams de nes a *partial order* on the set of partitions of n, i.e.

- $\star$ $(\lambda \rhd \mu) \wedge (\mu \rhd \nu) \implies \lambda \rhd \nu$,
- $\star$ $(\lambda \rhd \mu) \wedge (\mu \rhd \lambda) \iff \lambda = \mu$.

It is "partial" since not every pair (λ, μ) is comparable with respect to $\rhd$.

Lemma 13.2.2. *Suppose $\lambda, \mu \vdash n$. If there exist tableaux t and s of shape λ and μ, respectively, such that for each $i \geq 1$ the elements of the i-th row of s are all in di erent columns of t, then we must have $\lambda \rhd \mu$.*

Proof. The rst row of s has μ_1 elements which can be placed in di erent columns of t. Upon rearranging the entries of t in each column (i.e. upon applying to t a permutation from C_t), we may assume that these numbers sit in the rst row. Hence $\lambda_1 \geq \mu_1$.

The entries of the second row of s can be placed in di erent columns of t. Again, we may rearrange the entries in each column of t without touching the entries placed at the previous step, so that these numbers sit in the rst two rows of t. Therefore $\lambda_1 + \lambda_2 \geq \mu_1 + \mu_2$. Proceeding inductively, the numbers from the rst k rows of s can be placed in the rst k rows of t, and the inequality $\sum_{i \leq k} \lambda_i \geq \sum_{i \leq k} \mu_i$ follows, for each k. □

De nition 13.2.3 (The lexicographic order)**.** Let $\lambda = (\lambda_1 \geq \cdots)$ and $\mu = (\mu_1 \geq \cdots)$ be partitions of n. We write $\lambda > \mu$ if there exists $k \in \mathbb{Z}_{\geq 1}$ such that

$$\lambda_i = \lambda_i, \quad \forall i < k$$
$$\lambda_k > \mu_k.$$

This is easily seen to be a total order: any two partitions of n are comparable.

Lemma 13.2.4. *If $\lambda \rhd \mu$, then $\lambda \geq \mu$; that is, $\geq$ refines $\rhd$.*

Proof. There is nothing to prove when $\lambda = \mu$. Suppose $\lambda \neq \mu$, choose the minimal $k \in \mathbb{Z}_{\geq 1}$ such that $\lambda_k \neq \mu_k$. This is the required k in the definition of $\lambda > \mu$. □

13.3 Specht modules

Let F be any field. Let $\lambda = (\lambda_1 \geq \cdots \geq \lambda_r) \vdash n$.

Definition 13.3.1. The *permutation module* M^λ is the (free) F-vector space generated by the tabloids of shape λ. The $\mathfrak{S}_n$-action $\sigma\{t\} = \{\sigma t\}$ on tabloids affords a left $F\mathfrak{S}_n$-module structure on M^λ.

Thus an element of M^λ can be expressed as an F-linear combination $\sum_{\text{shape}\{t\}=\lambda} a_t\{t\}$ with unique coefficients.

Exercise 13.3.2. Show that $\dim_F M^\lambda = (n!)/(\lambda_1! \cdots \lambda_r!)$ for any $\lambda \vdash n$.

Definition 13.3.3. Let t be a Young tableau of shape $\lambda \vdash n$.

1. Define the corresponding signed column sum as
$$\kappa_t := \sum_{\sigma \in C_t} \operatorname{sgn}(\sigma)\sigma \in F\mathfrak{S}_n.$$
2. The *polytabloid* e_t associated to the tableau t is defined as
$$e_t := \kappa_t\{t\} \in M^\lambda.$$
In this case we say e_t is a polytabloid of shape λ.
3. The *Specht module* S^λ associated to λ is the left $F\mathfrak{S}_n$-submodule of M^λ spanned by polytabloids of shape λ.

Proposition 13.3.4. *Let t be a tableau with n boxes and $\sigma \in \mathfrak{S}_n$. We have*

1. *$R_{\sigma t} = \sigma R_t \sigma^{-1}$ and $C_{\sigma t} = \sigma C_t \sigma^{-1}$;*
2. *$\kappa_{\sigma t} = \sigma \kappa_t \sigma^{-1}$;*
3. *$e_{\sigma t} = \sigma e_t$.*

Proof. The first statement concerning row and column stabilizers result from an easy "transport of structure" by σ. As for the second statement, it suffices to note $\operatorname{sgn}(\sigma\tau\sigma^{-1}) = \operatorname{sgn}(\tau)$ for all $\tau \in \mathfrak{S}_n$. Therefore
$$e_{\sigma t} = \kappa_{\sigma t}\{\sigma t\} = \sigma \kappa_t \sigma^{-1}\sigma\{t\} = \sigma e_t$$
and the third statement follows. □

Recall that a left $F\mathfrak{S}_n$-module M is called *cyclic* if there exists $e \in M$ such that $M = F\mathfrak{S}_n e$. Since the tableaux of shape λ form a single orbit under $\mathfrak{S}_n$, we get the following corollary of the last assertion.

Corollary 13.3.5. *The Specht module S^λ is cyclic. In fact, for any polytabloid e_t of shape λ we have $S^\lambda = \mathfrak{S}_n e_t$.*

Below is an example borrowed from [22, p.61]. Consider the tableau

$$t = \begin{array}{|c|c|c|}\hline 4 & 1 & 2 \\ \hline 3 & 5 \\ \cline{1-2}\end{array}$$

The column stabilizer C_t is generated by the transpositions (34) and (15). We have $\kappa_t = (1-(34))(1-(15))$ and

$$e_t = \begin{array}{|c|c|c|}\hline 4 & 1 & 2 \\ \hline 3 & 5 \\ \cline{1-2}\end{array} - \begin{array}{|c|c|c|}\hline 3 & 1 & 2 \\ \hline 4 & 5 \\ \cline{1-2}\end{array} - \begin{array}{|c|c|c|}\hline 4 & 5 & 2 \\ \hline 3 & 1 \\ \cline{1-2}\end{array} + \begin{array}{|c|c|c|}\hline 3 & 5 & 2 \\ \hline 4 & 1 \\ \cline{1-2}\end{array}.$$

Proposition 13.3.6. *For each partition λ we have $S^\lambda \neq \{0\}$.*

Proof. Construct a tableau t of shape λ by inserting numbers into the rows consecutively, eg.

$$t = \begin{array}{|c|c|c|c|}\hline 1 & 2 & 3 & 4 \\ \hline 5 & 6 \\ \cline{1-2} 7 \\ \cline{1-1}\end{array}.$$

It is then clear that $\{t\}$ appears with coe cient one in the expression $\sum_{\sigma\in C_t} \operatorname{sgn}(\sigma)\sigma\{t\}$. □

Lemma 13.3.7. *Let H be a subgroup of $\mathfrak{S}_n$. Put $H^- := \sum_{h\in H} \operatorname{sgn}(h)h \in F\mathfrak{S}_n$.*

1. *For every $\sigma \in H$ we have $\sigma H^- = H^-\sigma = \operatorname{sgn}(\sigma)H^-$.*
2. *For every transposition $\tau \in H$, we have $H^- \in F\mathfrak{S}_n \cdot (1-\tau)$.*
3. *If t is a tableau with n boxes, $b \neq c \in \{1,\dots,n\}$ such that b, c lie in the same row of t and $(bc) \in H$, then $H^-\{t\} = 0$.*

Proof. The rst assertion is clear from the multiplicativity of sgn. To prove the second one, we use the coset decomposition $H = \bigsqcup_{i=1}^{s} \kappa_i\{1,\tau\}$ with respect to the subgroup generated by τ, by choosing representatives $\kappa_1,\dots,\kappa_s$. Then

$$H^- = \left(\sum_{i=1}^{s} \operatorname{sgn}(\kappa_i)\kappa_i\right)\cdot(1-\tau).$$

To prove the nal assertion, note that $(bc)\{t\} = \{t\}$. Set $\tau := (bc)$, we have $(1-\tau)\{t\} = 0$ and the assertion follows from the previous one. □

Exercise 13.3.8. Show that $S^\lambda \simeq \mathbb{1}$ (the trivial representation) when $\lambda = (n)$, and $S^\lambda \simeq \operatorname{sgn}$ when $\lambda = (1\cdots 1)$.

Lemma 13.3.9. *Let $\lambda, \mu \vdash n$. Let t and s be tableaux of shape λ and μ, respectively.*

1. *If $\kappa_t\{s\} \neq 0$, then $\lambda \rhd \mu$.*
2. *If $\lambda = \mu$ and $\kappa_t\{s\} \neq 0$, then $\kappa_t\{s\} = \pm e_t$.*

Proof. Suppose $\kappa_t\{s\} \neq 0$. For any two numbers b, c in the same row of s, they cannot lie in the same column of t; otherwise the preceding Lemma with $H := C_t \ni (bc)$ would imply $\kappa_t\{s\} = 0$. Hence the Lemma 13.2.2 implies $\lambda \rhd \mu$.

Suppose in addition that $\lambda = \mu$. We claim that there exists $\sigma \in C_t$ such that $\{s\} = \sigma\{t\}$. Indeed, we start by permuting the entries in the first column of t, so that an entry x thereof lies in the i-th row of t if and only if it lies in the i-th row of s (but probably in different columns); this can always be done according to the discussions above. Working column-by-column we eventually arrive at $\{s\} = \sigma\{t\}$ where $\sigma \in C_t$, hence the claim. The previous Lemma with $H = C_t$ yields

$$\kappa_t\{s\} = \kappa_t\sigma\{t\} = \operatorname{sgn}(\sigma)\kappa_t\{t\} = \operatorname{sgn}(\sigma)e_t$$

as asserted. □

Corollary 13.3.10. *Let $m \in M^\lambda$ and t be a tableau of shape λ. Then $\kappa_t m \in F \cdot e_t$.*

Proof. Write $m = \sum_{i=1}^r c_i\{s_i\}$, where s_i are tableaux of shape λ. Now apply the previous Lemma. □

Proposition 13.3.11. *Let $\lambda, \mu \vdash n$. Let $\varphi \in \operatorname{Hom}_{F\mathfrak{S}_n}(M^\lambda, M^\mu)$. If $\varphi|_{S^\lambda} \neq 0$, then $\lambda \rhd \mu$. If $\lambda = \mu$, then $\varphi|_{S_\lambda}$ is multiplication by some scalar in F.*

Proof. By assumption there exists $e_t \in S^\lambda$ such that

$$0 \neq \varphi(e_t) = \varphi(\kappa_t\{t\}) = \kappa_t\varphi(\{t\}).$$

By writing $\varphi(\{t\}) = \sum_{i=1}^r c_i\{s_i\}$ where s_i are tableaux of shape μ. Lemma 13.3.9 then implies $\lambda \rhd \mu$.

Assume $\lambda = \mu$. We have just seen that $\varphi(e_t) = \sum_{i=1}^r c_i\kappa_t\{s_i\}$. Corollary 13.3.10 says that $\varphi(e_t) = ce_t$ for some $c \in F$. By (i) the $\mathfrak{S}_n$-equivariance of φ and (ii) the cyclicity of S^λ, it follows that $\varphi(x) = cx$ for every $x \in S^\lambda$. □

Remark 13.3.12. The construction so far is combinatorial. It makes no use of the field structure of F. In fact F can be any commutative ring, such as $\mathbb{Z}$.

13.4 Representations of $\mathfrak{S}_n$

Although this is not absolutely necessary, we begin by paraphrasing the earlier constructions in terms of induced representations. Here we define the induction functor ind_H^G as $FG \otimes_{FH} -$.

For a partition $\lambda = (\lambda_1 \geq \cdots \geq \lambda_r) \vdash n$, the corresponding *Young subgroup* of $\mathfrak{S}_n$ is defined as

$$\begin{aligned}\mathfrak{S}[\lambda] &:= \mathfrak{S}_{\{1,\ldots,\lambda_1\}} \times \mathfrak{S}_{\{\lambda_1+1,\ldots,\lambda_1+\lambda_2\}} \times \cdots \times \mathfrak{S}_{\{n-\lambda_r+1,\ldots,n\}} \\ &\simeq \prod_{i=1}^r \mathfrak{S}_{\lambda_i}.\end{aligned}$$

We shall x λ in what follows. Let us denote by $\mathbf{t}$ the tableau of shape λ given by

$$\mathbf{t} := \begin{array}{|c|c|c|c|} \hline 1 & 2 & \cdots & \lambda_1 \\ \hline \lambda_1+1 & \vdots & & \\ \cline{1-2} n-\lambda_r+1 & \cdots & n & \\ \cline{1-3} \end{array}$$

Note that $R_{\mathbf{t}} = \mathfrak{S}[\lambda]$ and $C_{\mathbf{t}} \simeq \mathfrak{S}[\bar{\lambda}]$ where $\bar{\lambda}$ is the conjugate Young diagram of λ with rows and columns swapped.

Proposition 13.4.1. *Fix a nonzero vector v_0 in the underlying F-vector space of the trivial representation $\mathbb{1}$ of $\mathfrak{S}[\lambda]$. The homomorphism between representations of $\mathfrak{S}_n$ over F*

$$\begin{aligned} \mathrm{ind}_{R_{\mathbf{t}}}^{\mathfrak{S}_n}(\mathbb{1}) &\longrightarrow M^{\lambda} \\ \sigma \otimes v_0 &\longmapsto \sigma\{\mathbf{t}\}, \quad \sigma \in \mathfrak{S}_n \end{aligned}$$

is an isomorphism.

Proof. Routine. □

Proposition 13.4.2. *Consider the* 1*-dimensional representation* sgn *of $C_{\mathbf{t}}$, which is the restriction of* sgn : $\mathfrak{S}_n \to \{\pm 1\}$, *and x a nonzero vector u_0 in its underlying F-vector space. The homomorphism*

$$\begin{aligned} \mathrm{ind}_{C_{\mathbf{t}}}^{\mathfrak{S}_n}(\mathrm{sgn}) &\longrightarrow M^{\lambda} \\ \sigma \otimes u_0 &\longmapsto \sum_{\tau \in C_{\sigma\mathbf{t}}} \mathrm{sgn}(\tau)\{\tau\sigma\mathbf{t}\} =: e_{\sigma\mathbf{t}}. \end{aligned}$$

between representations of $\mathfrak{S}_n$ is well-de ned. In particular, its image equals S^{λ}.

Proof. If this map is well-de ned, it will be a homomorphism of representations since $e_{g\sigma\mathbf{t}} = g e_{\sigma\mathbf{t}}$ for any $g, \sigma \in \mathfrak{S}_n$, by Proposition 13.3.4. It is indeed well-de ned by the part 1 of Lemma 13.3.7 with $H := C_{\mathbf{t}}$, which yields $e_{\sigma h\mathbf{t}} = \sigma h \kappa_{\mathbf{t}}\{\mathbf{t}\} = \mathrm{sgn}(h) e_{\sigma\mathbf{t}}$ for all $h \in C_{\mathbf{t}}$. □

All in all, the Specht module S^{λ} is characterized as the image of a canonical intertwining operator $\mathrm{ind}_{C_{\mathbf{t}}}^{\mathfrak{S}_n}(\mathrm{sgn}) \to \mathrm{ind}_{R_{\mathbf{t}}}^{\mathfrak{S}_n}(\mathbb{1})$.

Henceforth we assume $\mathrm{char}(F) \nmid |\mathfrak{S}_n| = n!$. Equivalently, either $\mathrm{char}(F) = 0$ or $p := \mathrm{char}(F) > n$.

Theorem 13.4.3. *For λ ranging over the partitions of n, the Specht modules S^{λ} form a complete set of isomorphism classes of irreducible representations of $\mathfrak{S}_n$ over F. Moreover, each S^{λ} is absolutely irreducible.*

Proof. We divide the proof into three steps.

1. S^λ **is absolutely irreducible for each** λ. It su ces to show $\mathrm{End}_{\mathfrak{S}_n}(S^\lambda) = F$. By Maschke's theorem we may take a subrepresentation T of M^λ such that $M^\lambda = S^\lambda \oplus T$. Using this, every $\psi \in \mathrm{Hom}_{\mathfrak{S}_n}(S^\lambda, S^\lambda)$ can be extended to $\varphi \in \mathrm{Hom}_{\mathfrak{S}_n}(M^\lambda, M^\lambda)$. If $\psi \neq 0$, Proposition 13.3.11 implies ψ is a scalar multiplication from F.
2. $S^\lambda \simeq S^\mu$ **only when** $\lambda = \mu$. Let $\psi \in \mathrm{Hom}_{\mathfrak{S}_n}(S^\lambda, S^\mu)$, $\psi \neq 0$. As before, ψ can be extended to $\varphi \in \mathrm{Hom}_{\mathfrak{S}_n}(M^\lambda, M^\mu)$. This time the Proposition 13.3.11 yields $\lambda \rhd \mu$. By symmetry $\mu \rhd \lambda$ as well, hence $\lambda = \mu$.
3. **Every irreducible representation is isomorphic to some** S^λ. By general theory, the number of irreducible representations of $\mathfrak{S}_n$ (up to isomorphism) is less or equal then the number of conjugacy classes. Since the partitions of n and the conjugacy classes in $\mathfrak{S}_n$ are in bijection, we conclude by the previous steps.

□

Corollary 13.4.4. *Any eld F with $\mathrm{char}(F) \nmid n!$ is a splitting eld of G.*

Corollary 13.4.5. *Let μ be a partition. We have the decomposition*

$$M^\mu = \bigoplus_{\lambda \geq \mu} (S^\lambda)^{\oplus m_{\lambda,\mu}}$$

in the ordering of De nition 13.2.3, and $m_{\mu,\mu} = 1$.

Proof. In Proposition 13.3.11 it is shown that $\mathrm{Hom}_{\mathfrak{S}_n}(S^\lambda, M^\mu) \neq \{0\}$ only if $\lambda \rhd \mu$, which implies $\lambda \geq \mu$ by Lemma 13.2.4. Furthermore, when $\lambda = \mu$ the Hom-set equals F. □

In other words, the characters of M^μ and S^λ form two bases of the space of class functions on $\mathfrak{S}_n$, as λ, μ varies. They are related by an *upper-triangular matrix* with diagonal entries equal to 1. This transition matrix and its inverse are, however, not so easy to compute. The multiplicities $m_{\lambda,\mu}$ here actually equal the combinatorially de ned *Kostka numbers*.

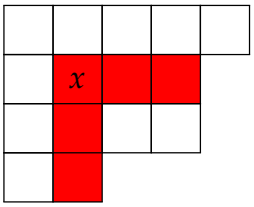
13.5 Odds and ends

Due to the combinatorial nature of our constructions, much information about the Specht modules can be e ectively computed from the Young tableaux. We do not have time to go further. Let us indicate some aspects.

1. **Standard tableaux**. Let $\lambda \vdash n$. The polytabloids span S^λ. A nice basis is given by the polytabloids e_t indexed by *standard tableaux* of shape λ. A tableau is called standard if its rows and columns are increasing sequences. The dimension of S^λ, or the number of standard tableaux of shape λ, also admits an elegant description, the *hook length formula* (Frame-Robinson-Thrall, 1954):

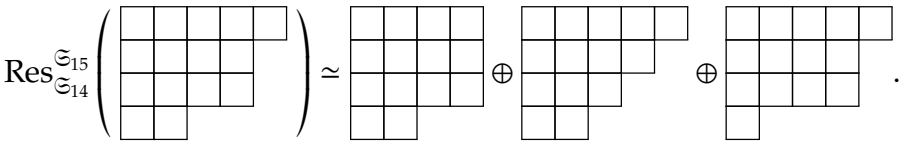
$$\dim_F S^\lambda = \frac{n!}{\prod_x \mathrm{hook}(x)},$$

where x ranges over the boxes in the Young diagram for λ and hook(x) is the length (i.e. the number of boxes) of the "hook" with corner x, as depicted below



$(n = 15)$.

2. **Branching laws**. There is a combinatorial description of $\mathrm{Res}^{\mathfrak{S}_n}_{\mathfrak{S}_{n-1}}(S^\lambda)$ when $\mathrm{char}(F) \nmid n!$. Roughly speaking, its decomposition is given by removing one box from λ to obtain a new Young diagram, in all possible ways. An illustration:



In particular, the restricted representation decomposes with multiplicity one. Thanks to the Frobenius reciprocity, one has a similar recipe for decomposing $\mathrm{ind}^{\mathfrak{S}_{n+1}}_{\mathfrak{S}_n}(S^\lambda)$.

3. **Modular representations**. When $p := \mathrm{char}(F)$ divides $n!$, the Specht modules S^λ are no longer irreducible in general. A partition λ is called p-singular if $\lambda_{i+1} = \cdots = \lambda_{i+p} > 0$ for some $i \geq 0$; otherwise it is called p-regular. For p-regular λ, there is a unique irreducible quotient D^λ of S^λ. It is known (James, 1976) that $\{D_\lambda : \lambda \text{ is } p\text{-regular}\}$ exhausts all the irreducibles of $\mathfrak{S}_n$, and they are absolutely irreducible.

4. It would be much more satisfactory to treat the theory of symmetric functions and Schur-Weyl duality in parallel. But we do not have time to zhēténg anymore.

LECTURE 14

BRAUER INDUCTION THEOREM

The aim of this lecture is to prove the celebrated *Brauer induction theorem*. Apart from its intrinsic beauty and applications, the proof will make use of many of our previous results; therefore we are in a position to refresh our knowledge.

14.1 Group-theoretic backgrounds

In what follows, G is a finite group. The identity element of a group will be denoted by 1. Let p be a prime number.

- ⋆ G is called a p-group if $|G| = p^m$ for some m.
- ⋆ A subgroup H of G is called a Sylow p-subgroup if H is a p-group and the index $(G : H)$ is not divisible by p.

The Sylow p-subgroups exist and are conjugate to each other. All these are standard results in undergraduate algebra, see eg. [16, I.6] for a detailed discussion.

Next, note that every finite cyclic group A has a canonical decomposition $A = A_{p'} \times A_p$ where

- ⋆ $A_{p'}$ is a cyclic subgroup of order prime to p,
- ⋆ A_p is a p-subgroup.

For each $x \in G$, let $\langle x \rangle$ denote the cyclic subgroup of G generated by x. Write $\langle x \rangle = \langle x \rangle_{p'} \times \langle x \rangle_p$ as above, there is a unique decomposition

$$x = x_{p'} x_p = x_p x_{p'}$$

where $x_{p'} \in \langle x \rangle_{p'}$, $x_p \in \langle x \rangle_p$.

Definition 14.1.1. Let p be a prime number. We call G a p-elementary group if it is of the form $G = C \times P$ where C is a cyclic group of order prime to p, and P is a p-group.

We call G a p-quasi-elementary group if it is of the form $G = C \rtimes P$ where C and P are as above.

In a p-quasi-elementary group G, the component C in the semi-direct product $G = C \rtimes P$ is characterized by

$$C = G_{p'} := \{x \in G : x = x_{p'}\}. \tag{14.1}$$

Indeed, the inclusion $C \subset G_{p'}$ is evident. Conversely, given $x \in G_{p'}$, its image in $G/C \simeq P$ is of order prime to p, hence trivial since P is a p-group. Thus $x \in C$.

Lemma 14.1.2. *If G is p-elementary (resp. p-quasi-elementary), then so are the subgroups of G.*

Proof. Firstly we notice the following property: a group G is p-quasi-elementary if and only if $G_{p'}$ is a cyclic subgroup. The "only if" part follows from the preceding discussion. Conversely, if $G_{p'}$ is a subgroup then it is normal and equals the direct product of all Sylow ℓ-subgroups ($\ell \neq p$). Choose a Sylow p-subgroup P of G; by considerations of cardinality we have $G = G_{p'} \rtimes P$.

Let H be a subgroup of G. We have $H_{p'} = H \cap G_{p'}$. If G is p-quasi-elementary then $H_{p'}$ is a cyclic subgroup of H, thus H is p-quasi-elementary as well; in this case we write $H = H_{p'} \rtimes P_H$. If G is p-elementary, then there is a unique Sylow p-subgroup P of G. Therefore $P_H = H \cap P$ commutes with $H_{p'} \subset G_{p'}$, and one gets $H = C_H \times P_H$, showing that H is p-elementary. □

Remark 14.1.3. Note that p-elementary groups are supersolvable. This fact is trivial for the cyclic part C, whilst the supersolvability (in fact, nilpotence) for the p-groups is a standard fact – see [16, I.6.6].

14.2 Representation-theoretic backgrounds

We x a eld F and assume $\mathrm{char}(F) \nmid |G|$, although this is not always necessary. The representations below are all nite-dimensional over F.

Proposition 14.2.1. *Let H be a subgroup of a nite group G. Let W (resp. V) be a representation of H (resp. G). There is a canonical isomorphism*

$$\mathrm{ind}_H^G \left(W \otimes \mathrm{Res}_H^G(V)\right) \xrightarrow{\sim} \mathrm{ind}_H^G(W) \otimes V.$$

Proof. We give a proof using adjunction of functors. Let U be a representation of G over F. We have functorial isomorphisms

$$\begin{aligned}\mathrm{Hom}_G\left(\mathrm{ind}_H^G(W \otimes \mathrm{Res}_H^G(V)), U\right) &\simeq \mathrm{Hom}_H\left(W \otimes \mathrm{Res}_H^G(V), \mathrm{Res}_H^G(U)\right) \simeq \\ \mathrm{Hom}_H\left(W, \mathcal{H}\mathrm{om}(\mathrm{Res}_H^G(V), \mathrm{Res}_H^G(U))\right) &= \mathrm{Hom}_H\left(W, \mathrm{Res}_H^G \mathcal{H}\mathrm{om}(V, U)\right) \simeq \\ \mathrm{Hom}_G\left(\mathrm{ind}_H^G(W), \mathcal{H}\mathrm{om}(V, U))\right) &\simeq \mathrm{Hom}_G\left(\mathrm{ind}_H^G(W) \otimes V, U\right),\end{aligned}$$

where $\mathcal{H}\mathrm{om}(\cdots)$ signi es that the Hom-space of F-vector spaces in question is regarded as a representation. This concludes the proof. □

Exercise 14.2.2. Besides $(\mathrm{ind}_H^G, \mathrm{Res}_H^G)$, which pair of adjoint functors have we used in the proof? Try to justify it.

Exercise 14.2.3. Prove Proposition 14.2.1 by using the explicit map

$$\begin{aligned}(FG \underset{FH}{\otimes} W) \underset{F}{\otimes} V &\longrightarrow FG \underset{FH}{\otimes} (W \underset{F}{\otimes} V)\\ (g \otimes w) \otimes v &\longmapsto g \otimes (w \otimes g^{-1}v).\end{aligned}$$

Show that it is an isomorphism of left FG-modules.

Definition 14.2.4. Define the representation ring $R_F(G)$ of G as the $\mathbb{Z}$-module generated by the symbols $[V]$, where $[V]$ ranges over the isomorphism classes of representations of G, subject to the relation

$$[V \oplus W] = [V] + [W].$$

The ring structure on $R_F(G)$ is prescribed by $[V] \cdot [W] = [V \otimes W]$. It is a commutative ring with unit $[\mathbb{1}]$, the class of the trivial representation.

Note that ind_H^G, Res_H^G induce maps $R_F(H) \to R_F(G)$, $R_F(G) \to R_F(H)$, respectively. They are homomorphisms of additive groups.

Definition 14.2.5. Let $\mathcal{H}$ be a family of subgroups of G. Define $R_{\mathcal{H}}(G)$ as the following additive subgroup of $R_F(G)$

$$\sum_{H \in \mathcal{H}} \mathrm{ind}_H^G(R_F(H)).$$

Sometimes one has to switch to the setup of *characters* χ_V. To facilitate the transition, note that there is a homomorphism from $R_F(G)$ to the ring of class functions on G (with respect to pointwise addition and multiplication), given by $[V] \mapsto \chi_V$. It is injective whenever $\mathrm{char}(F) = 0$, in which case the image is precisely the $\mathbb{Z}$-linear combinations of irreducible characters. Later on, we will denote by $X_F(G)$ the image of this homomorphism.

Lemma 14.2.6. *For any family $\mathcal{H}$, the additive subgroup $R_{\mathcal{H}}(G)$ is actually an ideal of the ring $R_F(G)$.*

Proof. It suffices to prove that $[\mathrm{ind}_H^G(W) \otimes V] \in R_{\mathcal{H}}(G)$ for every $H \in \mathcal{H}$, $[W] \in R_F(H)$ and $[V] \in R_F(G)$. By Proposition 14.2.1,

$$\mathrm{ind}_H^G(W) \otimes V \simeq \mathrm{ind}_H^G(W \otimes \mathrm{Res}_H^G(V))$$

hence its class lies in $R_{\mathcal{H}}(G)$. □

14.3 Brauer's theorem

In this section we assume $\mathrm{char}(F) = 0$ and F is a splitting field of all the subgroups of G; see Corollary 14.4.2 for a substantial improvement of the latter assumption. We will follow the slick proof due to Goldschmidt and Issacs [8]; see also [12, §5.12]. The reader may consult [16, XVIII.10] for another elegant proof due to Brauer and Tate (1955).

Theorem 14.3.1 (Brauer, 1947). *Let $\mathcal{H}$ be the set of all p-elementary subgroups of G, for various prime numbers p. Then $R_F(G) = R_{\mathcal{H}}(G)$.*

Corollary 14.3.2. *De ne $\mathcal{H}$ as above. Every element in $R_F(G)$ can be expressed as*

$$\sum_{H\in\mathcal{H}} \sum_{\substack{\xi:\text{rep of } H \\ \dim \xi = 1}} c_\xi \cdot \operatorname{ind}_H^G(\xi)$$

for coe cients $c_\xi \in \mathbb{Z}$.

Proof. Use the fact that (i) p-elementary groups are supersolvable, and (ii) supersolvable groups are M-groups. □

In what follows, we denote by $\mathbb{1}$ the trivial representation; the ambient group will be clear according to the context. De ne $\mathcal{H}'$ to be the set of p-quasi-elementary subgroups of G, for various prime numbers p.

Lemma 14.3.3. *For $\mathcal{H}'$ chosen as above, the additive subgroup*

$$P(\mathcal{H}') := \sum_{H\in\mathcal{H}'} \mathbb{Z}\cdot[\operatorname{ind}_H^G(\mathbb{1})] \quad \subset R_F(G)$$

is actually a subring (possibly without 1).

Proof. It su ces to show that for every $H, K \in \mathcal{H}'$, we have

$$[\operatorname{ind}_H^G(\mathbb{1})]\cdot[\operatorname{ind}_K^G(\mathbb{1})] \in P(\mathcal{H}').$$

By Proposition 14.2.1 we have

$$\begin{aligned}\operatorname{ind}_H^G(\mathbb{1})\otimes\operatorname{ind}_K^G(\mathbb{1}) &\simeq \operatorname{ind}_H^G\left(\mathbb{1}\otimes\operatorname{Res}_H^G(\operatorname{ind}_K^G(\mathbb{1}))\right)\\ &= \operatorname{ind}_H^G\left(\operatorname{Res}_H^G(\operatorname{ind}_K^G(\mathbb{1}))\right)\end{aligned}$$

The term $\operatorname{Res}_H^G(\operatorname{ind}_K^G(\mathbb{1}))$ can be expressed as a direct sum of representations of the form $\operatorname{ind}_L^H(\mathbb{1})$ by Mackey's theorem, where L ranges over some subgroups of H. In particular $L \in \mathcal{H}'$ by Lemma 14.1.2. This su ces to conclude since $\operatorname{ind}_H^G \circ \operatorname{ind}_L^G \simeq \operatorname{ind}_L^G$. □

Lemma 14.3.4 (Banaschewski). *Let X be a nite set, $X \neq \emptyset$ and let 1_X denote the constant function $X \to \{1\}$. Let A be a ring (possibly without 1) of functions $X \to \mathbb{Z}$ under pointwise addition and multiplication. If $1_X \notin A$, then there exists $x \in X$ and a prime number p such that $\forall a \in A,\ a(x) \in p\mathbb{Z}$.*

Proof. Note that for every $x \in X$, the set $I_x = \{a(x) : a \in A\}$ is a subgroup of $\mathbb{Z}$, hence is of the form $n_x\mathbb{Z}$ for some $n_x \in \mathbb{Z}_{\geq 1}$. Suppose on the contrary that for every $x \in X$ we have $1 \in I_x$. Then we may choose a family $(a_x)_{x\in X}$ of elements in A such that

$$\prod_{x\in X}(1_X - a_x) = 0$$

as functions $X \to \mathbb{Z}$. Expanding this nite product shows that $1_X \in A$. □

Now we can establish an important intermediate step towards Brauer's theorem.

Proposition 14.3.5 (Solomon)**.** *With the notations as before, we have* $[\mathbb{1}] \in P(\mathcal{H}')$.

Proof. For every subgroup H of G, write $\mathbb{1}_H^G : G \to F$ for the character of $\mathrm{ind}_H^G(\mathbb{1})$. It is clearly $\mathbb{Z}$-valued. In fact, the induced character formula asserts that

$$\mathbb{1}_H^G(x) = |\{\bar{g} = gH \in G/H : g^{-1}xg \in H\}|.$$

We may embed $R_F(G)$ into the ring of class functions on G via $[V] \mapsto \chi_V$. In view of the preceding lemmas applied to $A = P(\mathcal{H}')$, it su ces to show that for each $x \in G$ and prime number p, there exists $H \in \mathcal{H}'$ such that $\mathbb{1}_H^G(x) \notin p\mathbb{Z}$.

Fix $x \in G$. We shall use the familiar decomposition $\langle x \rangle = C \times \langle x \rangle_p$ where $C := \langle x \rangle_{p'}$. Put

$$N := \text{the normalizer of } C \text{ in } G,$$
$$\bar{H} := \text{a Sylow } p\text{-subgroup of } N/C.$$

Write $\bar{H} = H/C$. We contend that $H \in \mathcal{H}'$. Indeed, let P be a Sylow p-subgroup of H, then $H = C \rtimes P$ by considerations of cardinality, thus H is p-quasi-elementary.

Claim: $\mathbb{1}_H^G(x) = \mathbb{1}_H^N(x)$. From the induced character formula alluded above for G and N, we only need to show $g^{-1}xg \in H \Rightarrow g \in N$ for every $g \in G$. Indeed, $g^{-1}xg \in H$ implies $g^{-1}\langle x \rangle_{p'} g \subset H_{p'}$, whilst $\langle x \rangle_{p'} = C = H_{p'}$.

Next, observe that $\langle x \rangle \subset N$ acts on N/H by left translation. The subgroup C acts trivially since $C \lhd N$ and $C \subset H$. Thus we deduce an action of the p-group $\langle x \rangle / C$ on N/H. Counting $|N/H|$ by collecting the $\langle g \rangle / C$-orbits, we obtain

$$\begin{aligned}[N : H] &= |\ \text{xed points}| + \overbrace{\text{lengths of the other orbits}}^{\in p\mathbb{Z}} \\ &\equiv |\{\bar{g} \in N/H : x\bar{g} = \bar{g}\}| \mod p \\ &\equiv \mathbb{1}_H^N(x) \mod p.\end{aligned}$$

Since $[N : H] = [N/C : \bar{H}]$ is coprime to p by construction, it follows that $\mathbb{1}_H^G(x) = \mathbb{1}_H^N(x) \notin p\mathbb{Z}$, as required. □

Lemma 14.3.6 (Issacs)**.** *Suppose that $G = N \rtimes P$ where P is a Sylow p-subgroup of G. Let $\lambda : N \to F^\times$ be a homomorphism and set*

$$G_\lambda := \{g \in G : \lambda^g(\cdot) := \lambda(g \cdot g^{-1}) = \lambda(\cdot)\},$$
$$Z_N(P) := \{g \in N : \forall \pi \in P,\ g\pi = \pi g\}.$$

If $Z_N(P) \subset \ker(\lambda)$ and $P \subset G_\lambda$, then λ is trivial.

Proof. Let $\nu \in N$, we contend that $\lambda(\nu) = 1$. Since $G_\lambda \supset P$, the conjugation action of P on N leaves the ber $\lambda^{-1}(\lambda(\nu))$ stabe; the xed-point set is $Z_N(P) \cap \lambda^{-1}(\lambda(\nu))$. Since $Z_N(P) \subset \ker(\lambda)$, it remains to show the existence of P- xed points.

As in the previous proof, we argue by counting the orbit-lengths in $\lambda^{-1}(\lambda(\nu))$. Since P is a p-group,

$$|\ker(\lambda)| = |\lambda^{-1}(\lambda(\nu))| \equiv |P\text{-}\ \text{xed points}| \mod p.$$

As $\ker(\lambda) \subset N$ is of order prime to p, xed points exist. □

Proof of Theorem 14.3.1. By Lemma 14.2.6, $R_{\mathcal{H}}(G)$ is an ideal of $R_F(G)$ and it su ces to show $[\mathbb{1}] \in R_{\mathcal{H}}(G)$. In view of Proposition 14.3.5 and the transitivity of the ind-functors, we may reduce to the case where G is p-quasi-elementary for some prime number p. Furthermore, by induction on $|G|$, we are reduced to show that

$$[\mathbb{1}] \in \sum_{H \subsetneq G} \operatorname{ind}_H^G(R_F(H)) \tag{14.2}$$

whenever G is p-quasi-elementary but not p-elementary.

Write $G = C \rtimes P$ as in the De nition 14.1.1 and set $Z := Z_C(P)$ (cf. Lemma 14.3.6). We must have $Z \subsetneq C$, otherwise $G = C \times P$ would be p-elementary. Set $H := Z \times P \subsetneq G$.

Claim: $\operatorname{Res}_C^G \operatorname{ind}_H^G(\mathbb{1}) \simeq \operatorname{ind}_Z^C(\mathbb{1})$. This follows from Mackey's theorem and the fact $G = CH$, $C \cap H = Z$.

Claim: $\mathbb{1}$ appears in $\operatorname{ind}_H^G(\mathbb{1})$ with multiplicity one. Indeed this is a consequence of Frobenius reciprocity. Thus one can write $\operatorname{ind}_H^G(\mathbb{1}) = \mathbb{1} \oplus \bigoplus_\xi \xi$, for various irreducible representations $\xi \neq \mathbb{1}$.

Now we have $\operatorname{ind}_Z^C(\mathbb{1}) = \mathbb{1} \oplus \bigoplus_\xi \operatorname{Res}_C^G(\xi)$. Again, Frobenius reciprocity implies that $\mathbb{1}$ appears in $\operatorname{ind}_Z^C(\mathbb{1})$ with multiplicity one. Hence for each ξ in the decomposition, $\operatorname{Res}_C^G(\xi)$ is a sum of nontrivial one-dimensional representations $\lambda : C \to F^\times$.

Claim: for each $\lambda \neq \mathbb{1}$ as above, we have $Z \subset \ker(\lambda)$. Indeed, $\operatorname{ind}_Z^C(\mathbb{1})(z) = \mathrm{id}$ for each $z \in Z$, since C is abelian (use the de nition). Hence $Z \subset \ker(\lambda)$ for each λ.

Fix ξ and a component λ of $\operatorname{Res}_C^G(\xi)$. Cli ord's theorem then implies that ξ is induced from some representation of G_λ. The last step is to apply Lemma 14.3.6 to $N = C$, which entails $G_\lambda \subsetneq G$, thereby establishing (14.2). □

Remark 14.3.7. Brauer's result is optimal provided that only $\mathbb{Z}$-linear combinations of representations are allowed. In fact, a theorem of Green (1955) asserts that if $\mathcal{L}$ is a family of subgroups of G such that $R_F(G) = R_{\mathcal{L}}(G)$, then every $H \in \mathcal{H}$ satis es $H \subset gLg^{-1}$, where $g \in G$ and $L \in \mathcal{L}$. Conjugation by g is of course permitted, since $\operatorname{ind}_{gLg^{-1}}^G(W) \simeq \operatorname{ind}_L^G(W^g)$ for every representation W of gLg^{-1}.

Remark 14.3.8. An earlier result in this direction is Artin's Theorem [12, Theorem 5.24], which expresses the characters of G in terms of induction from cyclic subgroups, at the expense of allowing coe cients in $|G|^{-1}\mathbb{Z}$. In this case one has more or less explicit formulas for the coe cients via Möbius inversion. The theorems of Artin and Brauer are proved in a single shot in [16].

14.4 Applications

We give two corollaries to Brauer's theorem. As before, we x a nite group G and a eld F of characteristic zero.

Recall that $X_F(G)$ is de ned as the space of class functions $f : G \to F$ of the form $f = \sum_{i=1}^r c_i \chi_{V_i}$ for some $c_i \in \mathbb{Z}$, $V_i \in \mathbf{Rep}_F(G)$.

Corollary 14.4.1. *Suppose that F is a splitting eld for G. A class function $f : G \to F$ belongs to $X_F(G)$ if and only if $f|_H \in X_F(H)$ for every p-elementary subgroup H of G, for various prime numbers p.*

Proof. The "only if" part is trivial. Assume that $f|_H \in X_F(H)$ for every p-elementary H and every prime number p. Write $1_G = \sum_{H,\xi} c_\xi \mathrm{ind}_H^G(\xi)$ by Theorem 14.3.1, where

- ⋆ H ranges over $\mathcal{H}$,
- ⋆ 1_G is the constant function 1 on G, or: the character of $\mathbb{1}$,
- ⋆ $\xi = \chi_W$ for some $W \in \mathbf{Rep}_F(H)$, $c_\xi \in \mathbb{Z}$ and $\mathrm{ind}_H^G(\cdots)$ denotes the induced character.

The character version of Proposition 14.2.1 yields

$$f = f \cdot 1_G = \sum_{H,\xi} c_\xi \mathrm{ind}_H^G(\xi \cdot f|_H).$$

By assumption $\xi \cdot f|_H \in X_F(H)$, hence $f \in X_F(G)$ since ind_H^G maps $X_F(H)$ to $X_F(G)$. □

For the next result (cf. [12, §5.13]), recall that $m \in \mathbb{Z}_{\geq 1}$ is called an *exponent* of a finite group G, if $\forall x \in G,\ x^m = 1$.

Corollary 14.4.2. *Let G be a finite group of exponent m. If F is a field of characteristic zero containing all the m-th roots of unity, then F is a splitting field of G.*

Proof. Take an extension $E \supset F$ so that E is a splitting field of G. Let (V, π) be an irreducible representation of G over E. We have to show (V, π) is defined over F. By Corollary 14.3.2 we may write

$$[V] = \sum_{\substack{H \in \mathcal{H} \\ \lambda \in \mathbf{Rep}_E(H)}} c_\lambda \left[\mathrm{ind}_H^G(\lambda)\right]$$

in $R_E(G)$, where $\lambda : G \to E^\times$ is 1-dimensional and $c_\lambda \in \mathbb{Z}$. We have $\lambda(x)^m = \lambda(x^m) = 1$ for each $x \in H$, hence $\lambda : G \to F^\times$, so the representation $\mathrm{ind}_H^G(\lambda)$ is actually defined over F. Collecting terms, we may write

$$[V] = \sum_{i=1}^{r} c_i [V_{i,E}]$$

for distinct irreducible representations $V_i \in \mathbf{Rep}_F(G)$ and $c_i \in \mathbb{Z}$. By Maschke's theorem, EG is semisimple and the $\mathbb{Z}$-module $R_E(G)$ has a basis consisting of classes of irreducible representations over E. Furthermore, $V_{i,E}$ and $V_{j,E}$ have an irreducible factor in common if and only if $V_i \simeq V_j$, equivalently: $i = j$.

All in all, the irreducibility of V then implies $c_i = 1$ for exactly one index i, say $i = 1$, and $c_j = 0$ for $j \neq 1$. Hence $V \simeq V_{1,E}$ is defined over F. □

Last but not the least.....

Happy Chinese New Year!

Figure 14.1: Lì Qún. *Fēngyīzúshítú*. Yan'an, 1944. Woodblock print

BIBLIOGRAPHY

[1] A. V. Arhangel'skii, K. R. Goodearl, and B. Huisgen-Zimmermann. Kiiti Morita (1915–1995). *Notices Amer. Math. Soc.*, 44(6):680–684, 1997.

[2] E. Artin. Zur Theorie der hyperkomplexen Zahlen. *Abh. Math. Sem. Univ. Hamburg*, 5(1):251–260, 1927.

[3] I. Assem, D. Simson, and A. Skowroński. *Elements of the representation theory of associative algebras. Vol. 1*, volume 65 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 2006. Techniques of representation theory.

[4] G. Benkart, I. Kaplansky, K. McCrimmon, D. J. Saltman, and G. B. Seligman. Nathan Jacobson (1910–1999). *Notices Amer. Math. Soc.*, 47(9):1061–1071, 2000.

[5] G. M. Bergman. A ring primitive on the right but not on the left. *Proc. Amer. Math. Soc.*, 15:473–475, 1964.

[6] C. W. Curtis. *Pioneers of representation theory: Frobenius, Burnside, Schur, and Brauer*, volume 15 of *History of Mathematics*. American Mathematical Society, Providence, RI, 1999.

[7] S. Ding, M.-C. Kang, and E.-T. Tan. Chiungtze C. Tsen (1898–1940) and Tsen's theorems. *Rocky Mountain J. Math.*, 29(4):1237–1269, 1999.

[8] D. M. Goldschmidt and I. M. Isaacs. Schur indices in nite groups. *J. Algebra*, 33:191–199, 1975.

[9] D. Hilbert. Die Theorie der algebraischen Zahlkörper. *Jahresber. Dtsch. Math.-Ver.*, 4:i–xviii + 175–546, 1897.

[10] N. Jacobson. Structure theory of simple rings without niteness assumptions. *Trans. Amer. Math. Soc.*, 57:228–245, 1945.

[11] N. Jacobson. *Basic algebra. I*. W. H. Freeman and Company, New York, second edition, 1985.

[12] N. Jacobson. *Basic algebra. II*. W. H. Freeman and Company, New York, second edition, 1989.

[13] G. D. James. *The representation theory of the symmetric groups*, volume 682 of *Lecture Notes in Mathematics*. Springer, Berlin, 1978.

[14] T. Y. Lam. *Lectures on modules and rings*, volume 189 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1999.

[15] T. Y. Lam. *A first course in noncommutative rings*, volume 131 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2001.

[16] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[17] S. Mac Lane. *Categories for the working mathematician*, volume 5 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1998.

[18] K. Morita. Duality for modules and its applications to the theory of rings with minimum condition. *Sci. Rep. Tokyo Kyoiku Daigaku Sect. A*, 6:83–142, 1958.

[19] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[20] P. M. Neumann. *The mathematical writings of Évariste Galois*. Heritage of European Mathematics. European Mathematical Society (EMS), Zürich, 2011.

[21] B. Pareigis. *Categories and functors*. Translated from the German. Pure and Applied Mathematics, Vol. 39. Academic Press, New York-London, 1970. Available at http://epub.ub.uni-muenchen.de/7244/1/7244.pdf.

[22] B. E. Sagan. *The symmetric group*, volume 203 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2001. Representations, combinatorial algorithms, and symmetric functions.

[23] W. Scharlau. *Quadratic and Hermitian forms*, volume 270 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1985.

[24] V. Srinivas. *Algebraic K-theory*. Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, second edition, 2008.

[25] E. Steinitz. Algebraische Theorie der Körper. *J. Reine Angew. Math.*, 137:167–309, 1910.

[26] M.-F. Vignéras. An elementary introduction to the local trace formula of J. Arthur. The case of finite groups. Jubiläum band DMV B.G. Teubner Stuttgart, http://www.math.jussieu.fr/~vigneras/dmv.pdf, 1991.

[27] J. H. M. Wedderburn. On Hypercomplex Numbers. *Proc. London Math. Soc.*, S2-6(1):77, 1907.

[28] H. Whitney. Tensor products of Abelian groups. *Duke Math. J.*, 4(3):495–528, 1938.

INDEX