MAT 534 Algebra I
Stony Brook University

Jason Starr
Fall 2022

MAT 534 Algebra 1, Notes on Rational Canonical Form

Contents

These notes develop the basic definitions and results about rings and modules, but in the special case that the ring is itself a vector space of a field, and the ring multiplication is bilinear for that vector space structure. The notes end with a quick proof of existence of the rational canonical form directly, without explicit mention of the structure theorem for finitely generated modules over a principal ideal domain (of course the key steps in the proof of rational canonical form are the same as the key steps in the more general structure theorem for finitely generated modules over a principal ideal domain).

1 Algebras

Let F be a field.

Definition 1.1. An associative, unital ring is commutative if the multiplication law is commutative. The **center** of an associative, unital ring A is the subset $Z(A)$ of elements a such that $a \cdot b$ equals $b \cdot a$ for every b in A. This is an associative, unital subring of A that is commutative; in fact, the center equals the intersection of all maximal commutative subrings of A. An F-**central algebra** is a pair (A, ϕ) of an associative, unital ring A and a homomorphism $\phi : F \to A$ of associative, unital rings whose image lies in the center of A (if A is nonzero, then automatically ϕ is injective). In particular, multiplication in A by $\phi(F)$ makes A into an F-vector space. The structure of an F-central algebra on an F-vector space A is equivalent to an F-bilinear map

$$\beta : A \times A \to A,$$

$\beta(a, \beta(b, c)) = \beta(\beta(a, b), c)$ for every $a, b, c \in A$ and such that there exists $1 \in A$ with $\beta(1, a) = a = \beta(a, 1)$ for every $a \in A$ (then $\phi(t) := t \cdot 1$ for every $t \in F$). For F-central algebras (A, β_A) and (B, β_B), there is a unique structure of F-central algebra on $A \otimes_F B$ such that the two F-linear maps

$$A \to A \otimes_F B, \quad a \mapsto a \otimes 1,$$

$$B \to A \otimes_F B, \quad b \mapsto 1 \otimes b,$$

are both morphisms of F-central algebras, namely,

$$\beta_{A \otimes_F B} : (A \otimes_F B) \times (A \otimes_F B) \mapsto A \otimes_F B, \quad (a \otimes b, a' \otimes b') \mapsto \beta_A(a, a') \otimes \beta_B(b, b').$$

This F-central algebra is the **tensor product** of the F-central algebras (A, β_A) and (B, β_B). The **opposite** F-central algebra is obtained from the opposite F-bilinear map,

$$\beta^{\text{opp}} : A \times A \to A, \beta^{\text{opp}}(a, b) = \beta(b, a).$$

A **homomorphism** between F-central algebras is a homomorphism of the underlying associative, unital rings that is also an F-linear transformation. The image of such a homomorphism is an F-central subalgebra of the target. An F-central algebra is **commutative** if $a \cdot b$ equals $b \cdot a$ for every $a, b \in A$. This is equivalent to the condition that the identity bijection $\text{Id}_A : A \to A^{\text{opp}}$ being a homomorphism of F-central algebras (in which case it is an isomorphism of F-central algebras).

Lemma 1.2. *For every F-central algebra A, the identity map on A is a homomorphism of F-central algebras. For homomorphisms of F-central algebras, $f : A \to B$ and $g : B \to C$, the composition $g \circ f : A \to C$ is a homomorphism of F-central algebras. For a homomorphism of F-central algebras that is a bijection, the inverse set map is also a homomorphism of F-central algebras, so that a homomorphism of F-central algebras is invertible if and only if it is bijective.*

Proof. Each of these is straightforward, and follows the pattern of the analogous result for group homomorphisms. □

Altogether, this lemma proves that there is a **category** whose objects are F-central algebras and whose morphisms are homomorphisms of F-central algebras.

Example 1.3. For every F-vector space V, the F-vector space $\mathrm{Hom}_F(V,V)$ is an F-central algebra under composition, where each $c \in F$ is mapped to $c\mathrm{Id}_V \in \mathrm{Hom}_F(V,V)$. This map is injective if and only if V is nonzero. Then the isomorphic image of F is precisely the center of $\mathrm{Hom}_F(V,V)$. If the dimension of V is > 1, then $\mathrm{Hom}_F(V,V)$ is not commutative. However, if V has positive finite dimension, so that there exists a (non-unique) F-linear isomorphism

$$q : V \to V^*, \quad v \mapsto q_v$$

then there is an induced isomorphism of F-central algebras

$$(-)_q^\dagger : \mathrm{Hom}_F(V,V) \to \mathrm{Hom}_F(V,V)^{\mathrm{opp}},$$

that sends each F-linear transformation $a : V \to V$ to the unique F-linear transformation $a^\dagger : V \to V$ such that $q_{a(v)}(w) = q_v(a^\dagger w)$ for every $v, w \in V$. The Skolem-Noether theorem guarantees that every homomorphism of F-central algebras from $\mathrm{Hom}_F(V,V)$ to its opposite algebra arises in this way for an F-linear isomorphism $q : V \to V^*$ that is unique up to nonzero scalar (this is not the usual formulation of the Skolem-Noether theorem).

Definition 1.4. An element a of an F-central algebra is a **unit** or (multiplicatively) **invertible** if there exists $b \in A$ such that $a \cdot b = b \cdot a = 1$, and otherwise a is a **nonunit**, i.e., it is **noninvertible**. The set of all invertible elements is a group under multiplication with identity element equal to 1 and with the inverse of a equal to b. This group is the **multiplicative group** of A, denoted $A^\times$. Multiplication on the left, resp. on the right, by elements of $A^\times$ defines a left action on A, resp. a right action on A, by $A^\times$. Elements in the same orbit of this action are **left associate**, resp. **right associate**. An element a is a **left zero divisor** if there exists nonzero b such that $a \cdot b = 0$. It is a **right zero divisor** if there exists nonzero b such that $b \cdot a = 0$. It is a **zero divisor** if it is both a left zero divisor and a right zero divisor, and it is a **regular element** if it is neither a left zero divisor nor a right zero divisor. If every nonzero element is a regular element, then the ring is a **domain**. An **integral domain** is a commutative algebra that is a domain. An element a is **nilpotent** if there exists a positive integer e such that $a^e = a \cdots a$ equals 0. The smallest such positive integer is the **nilpotence degree** or **index**. A commutative algebra is **reduced** if the only nilpotent element is zero. An element a is **idempotent** if $a \cdot a$ equals a, i.e., $a \cdot (1-a) = 0 = (1-a) \cdot a$. Thus $a = 1$ is the unique idempotent that is not a zero divisor. A subset $E \subset A$ whose elements are nonzero idempotents is a set of **orthogonal idempotents** if for every pair (a,b) of distinct elements of E, $a \cdot b = b \cdot a = 0$; in this case the sum of any finite collection of elements of E is again an idempotent. A finite set E of orthogonal idempotents is an **orthogonal idempotent decomposition** if the sum of all elements of E equals 1. Equivalently it is a finite subset of E whose elements sum to 1 and such that the product of any ordered pair of distinct elements in the set equals 0. Then the map from the product F-central algebra to A,

$$\prod_{e \in E} F \to A, \quad (c_e)_{e \in E} \mapsto \sum_{e \in E} c_e e,$$

is an injective morphism of F-central algebras. A nonzero idempotent is a **primitive idempotent** if it cannot be written as a sum of two nonzero orthogonal idempotents. An orthogonal idempotent decomposition is **primitive** if every idempotent in the decomposition is primitive.

Example 1.5. For every F-vector space V and for every direct sum decomposition $(V_i)_{i\in I}$ of V into nonzero subspaces V_i, i.e., a collection of subspaces such that the induced F-linear transformation $\bigoplus_{i\in I} V_i \to V$ is an isomorphism, every projection $e_i : V = \bigoplus_{i\in I} V_i \twoheadrightarrow V_i \hookrightarrow V$ is an idempotent with $\text{Image}(e_i) = V_i$ and with $\text{Ker}(e_i)$ equal to a complementary subspace $\sum_{j\neq i} V_j$. In particular, e_i is a primitive idempotent if and only if V_i is a one-dimensional F-vector space. The set $\{e_i | i \in I\}$ is a set of orthogonal idempotents. Every set of orthogonal idempotents in $\text{Hom}_F(V,V)$ is of this form for some direct sum decomposition. In particular, a set of orthogonal primitive idempotents is equivalent to a direct sum decomposition into one-dimensional subspaces, i.e., the direct sum decomposition $(F\cdot\vec{v}_i)_{i\in I}$ for a basis for V, $(\vec{v}_i)_{i\in I}$, unique up to scaling $(\lambda_i\vec{v}_i)_{i\in I}$, by nonzero elements $\lambda_i \in F\smallsetminus\{0\}$. If $(V_i)_{i\in I}$ is a finite direct sum decomposition, this set of orthogonal idempotents gives an orthogonal idempotent decomposition. Thus the primitive orthogonal idempotent decompositions are equivalent to finite bases of V up to scaling by nonzero elements of F as above. The corresponding commutative F-central subalgebra $\sum_{e\in E} F\cdot e$ is a maximal commutative F-central subalgebra of $\text{Hom}_F(V,V)$.

Example 1.6. An element a in $\text{Hom}_F(V,V)$ is nilpotent if and only if there exists a finite filtration by F-vector subspaces, $\{0\} = V^e \subsetneq \cdots \subsetneq V^0 = V$ such that $a(V^i) = V^{i+1}$ for every $i = 0,\dots,e-1$. In this case, e equals the nilpotence degree.

Example 1.7. An element $a \in \text{Hom}_F(V,V)$ is invertible if and only if a is an isomorphism from V to V, so the multiplicative group of $\text{Hom}_F(V,V)$ is the group $\text{Isom}_F(V,V)$ of F-linear isomorphisms of V under composition. For $V = F^{\oplus n}$, so that $\text{Hom}_F(V,V) = \text{Mat}_{n\times n}(F)$, the multiplicative group is $\mathbf{GL}_n(F)$. The right orbits for the action of $\mathbf{GL}_n(F)$ on $\text{Mat}_{n\times n}(F)$ are precisely the row equivalent matrices, and every right orbit contains a unique reduced row echelon form matrix. Similarly, the left orbits are the column equivalent matrices, and each left orbit contains a unique orbit that is the transpose of a reduced row echelon form matrix. (Transposition is an F-linear involution of $\text{Mat}_{n\times n}(F)$ that interchanges the order of multiplication and interchanges left orbits and right orbits.) If a is not invertible, then either $\text{Ker}(a)$ properly contains $\{0\}$ or $\text{Image}(a)$ is properly contained in V (or both). In the first case, for an idempotent e with image equal to $\text{Ker}(a)$, the product $a\cdot e$ equals 0, so a is a left zero divisor. In the second case, for an idempotent e whose kernel equals $\text{Image}(a)$, the product $e\cdot a$ equals 0, so a is a right zero divisor.

2 Modules

Definition 2.1. A pair (V,λ) of an F-vector space V and an F-bilinear map

$$\lambda : A\times V \to V,$$

respectively a pair (V,ρ) of an F-vector space V and an F-bilinear map

$$\rho : V\times A \to A,$$

is a **left A-module**, resp. a **right A-module**, if for every $a, b \in A$ and for every $v \in V$, $\lambda(1, v) = v$ and $\lambda(a \cdot b, v) = \lambda(a, \lambda(b, v))$, resp. $\rho(v, 1) = v$ and $\rho(v, a \cdot b) = \rho(\rho(v, a), b)$. Via adjointness of tensor product and Hom, this is equivalent to a homomorphism of F-central algebras,

$$A \to \mathrm{Hom}_F(V, V),$$

via the map sending a to $\lambda_{a,-}$, resp. sending a to $\rho_{-,a}$. For F-central algebras A and B, an $A - B$-**bimodule** is an F-trilinear map,

$$\gamma : A \times V \times B \to V,$$

such that both $\lambda(a, v) = \gamma(a, v, 1)$ and $\rho(v, b) = \gamma(1, v, b)$ are structures of left A-module and right B-module satisfying $\lambda(a, \rho(v, b)) = \gamma(a, v, b) = \rho(\lambda(a, v), b)$ for every $a \in A$, for every $v \in V$, and for every $b \in B$. A left or right A-module is **faithful** if the homomorphism from A to $\mathrm{Hom}_F(V, V)$ is injective, in which case A is identified with an F-central subalgebra of $\mathrm{Hom}_F(V, V)$. A **morphism** of left A-modules from (V, λ) to (W, μ) is an F-linear transformation $L : V \to W$ such that for every $a \in A$ and for every $v \in V$, $L(\lambda(a, v)) = \mu(a, L(V))$. Similarly for a morphism of right A-modules, and for a morphism of $A - B$-bimodules. For an $A - B$-modules V and for an $A - C$-module W, the set of morphisms of left A-modules, $\mathrm{Hom}_{A-\mathrm{mod}}(V, W)$, has a structure of $C - B$-bimodule by the rule that scales each left A-module homomorphism, $L : V \to W$, by $c \otimes b \in C \otimes_F B^{\mathrm{opp}}$ to get

$$c \cdot L \cdot b : V \to W, \quad v \mapsto L(v \cdot c) \cdot b.$$

Every F-central algebra is a bimodule over itself.

Definition 2.2. For every F-central algebra A, the F-bilinear multiplication map $A \times A \to A$ sending (a, b) to $a \cdot b$ is both a left A-module structure on A and a right A-module structure on A. This is faithful because A has a multiplicative identity. The associated morphism of F-central algebras, $A \to \mathrm{Hom}_F(A, A)$, is the **left regular representation**, resp. the **right regular representation**. In fact, because of associativity, altogether this is an $A - A$-bimodule structure on A, the **natural bimodule structure** of A on itself.

Left modules are equivalent to right modules for the opposite ring. For every left A-module (V, λ), define

$$\lambda^{\mathrm{opp}} : V \times A^{\mathrm{opp}} \to V, \quad \lambda^{\mathrm{opp}}(v, a) := \lambda(a, v).$$

For every right B-module, (W, ρ), define

$$\rho^{\mathrm{opp}} : B^{\mathrm{opp}} \times W \to W, \quad \rho^{\mathrm{opp}}(b, w) := \rho(w, b).$$

Lemma 2.3. *For every left A-module (V, λ), also $(V, \lambda^{opp}$ is a right A^{opp}-module, for every right A^{opp}-module (W, ρ), also (W, ρ^{opp}) is a left A-module, the opposite opposite left A-module $(V, (\lambda^{opp})^{opp})$ equals (V, λ), the opposite opposite right A^{opp}-module $(W, (\rho^{opp})^{opp})$ equals (W, ρ), and these operations define an equivalence between the categories of left A-modules and right A-modules. In particular, if A is commutative, then every left A-module naturally has a structure of $A - A$-bimodule, and this $A - A$-bimodule structure on the left A-module A agrees with the natural bimodule structure above.*

Proof. This is straightforward. □

Many modules are constructed as submodule of modules that have already been constructed.

Definition 2.4. A left A-**submodule** of a left A-module (V, λ) is an F-vector subspace U of V such that $\lambda(a, u)$ is in U for every $a \in A$ and every $u \in U$, so that the restriction $\lambda|_{A\times U}$ is a left A-module structure λ_U on U and the inclusion map from U to V is a morphism of left A-modules. Similarly for **right** B-**submodules** of a right B-module, and for $A-B$-**subbimodules** of an $A-B$-bimodule. The **zero submodule** is $\{0\}$. A **proper submodule** of a module is a submodule that does not equal the entire module. A **simple** left A-module is a nonzero left A-module such that the only left A-submodules are $\{0\}$ and all of A. Similarly for simple right B-modules, and similarly for simple $A-B$-bimodules. For a subset $\mathcal{F} \subseteq V$ of a left A-module, resp. of a right B-module, of a $A-B$-bimodule, the intersection of all left A-submodules, resp. right B-submodules, $A-B$-bimodules, that contain $\mathcal{F}$ is the left A-submodule, resp. right B-submodule, $A-B$-bimodule, that is **generated** by $\mathcal{F}$, denoted $A\cdot\mathcal{F}$, resp. $\mathcal{F}\cdot B$, $A\cdot\mathcal{F}\cdot B$. When $\mathcal{F}$ is a singleton set, resp. a finite set, the module is **cyclic**, resp. **finitely generated**.

Lemma 2.5. *For every subset $\mathcal{F} \subset V$ of a left A-module, resp. a right B-module, an $A-B$-bimodule, the submodule $A\mathcal{F}$, resp. $\mathcal{F}B$, $A\mathcal{F}B$, is the subset of V whose elements are 0 and all linear combinations $a_1f_1+\cdots+a_nf_n$, resp. $f_1b_1+\cdots+f_nb_n$, $a_1f_1b_1+\cdots+a_nf_nb_n$, for all integers $n \geq 0$, for all subsets $\{f_1,\ldots,f_n\} \subset \mathcal{F}$, for all $(a_1,\ldots,a_n) \in A^n$, and for all $(b_1,\ldots,b_n) \in B^n$.*

Proof. It is straightforward to check that this subset of V is a submodule. It contains $\mathcal{F}$ by construction. Moreover, every submodule of V that contains $\mathcal{F}$ must contain every such linear combination of elements of $\mathcal{F}$. Thus, this is the smallest submodule containing $\mathcal{F}$. □

Many submodules are constructed from homomorphisms between modules.

Lemma 2.6. *The image, resp. kernel, of any morphism of left A-modules is a left A-submodule. Similarly for morphisms of right B-modules and for morphisms of $A-B$-bimodules. The identity map of a module is a homomorphism of modules. The composition of a pair of composable homomorphisms of modules is again a homomorphism of modules.*

Proof. The proof works just as in the case of F-linear transformations of F-vector spaces. □

Lemma 2.7 (Schur's Lemma)**.** *Every nonzero homomorphism between left A-modules is injective, respectively surjective, an isomorphism, if the domain is simple, resp. if the target is simple, if both the domain and target are simple. The analogous result holds for homomorphisms between right B-modules, and for homomorphisms between $A-B$-bimodules. A nonzero module is simple if and only if every nonzero element is a cyclic generator of the entire module.*

Proof. This follows from the definition of simple and the fact that the kernel and image are left A-submodules. □

Every submodule also gives a quotient module.

Lemma 2.8. *For every left A-submodule U of a left A-module (V, λ), the quotient F-vector space $q_{V,U} : V \to V/U$ has a unique structure of left A-module, $\lambda_{V,U} : A \times (V/U) \to (V/U)$, such that $q_{V,U}$ is a morphism of left A-modules, and similarly for right B-submodules of a right B-module, and for $A-B$-submodule of an $A-B$-module.*

Proof. The proof is precisely the same as in the proof of the analogous result that the coset space of a subgroup in a group has a natural action by the group. □

Definition 2.9. The module structure in the previous lemma is the **quotient module structure**. For a morphism of modules, the **cokernel** is the quotient module of the target module by the image of the morphism considered as a submodule of the target module.

3 Limits and Colimits

The category of modules has limits and colimits. Let I be a small category, i.e., a set whose elements i are objects, together with an association to every ordered pair (i, j) of objects of I of a set $\mathrm{Hom}_I(i, j)$, and to every ordered triple (i, j, k) of objects of I a binary operation,

$$\circ_{i,j,k} : \mathrm{Hom}_I(j, k) \times \mathrm{Hom}_I(i, j) \to \mathrm{Hom}_I(i, k),$$

that has identity morphisms $\mathrm{Id}_i \in \mathrm{Hom}_I(i, i)$ and that satisfies associativity.

Definition 3.1. A small category I is **discrete** if the only morphisms are identity morphisms. A small category I is **almost filtered** if it satisfies both of the following. For every ordered pair (i, j) of objects of I, there is an object k of I and morphisms $\phi \in \mathrm{Hom}_I(i, k)$ and $\psi \in \mathrm{Hom}_I(j, k)$. Also, for every ordered pair (u, v) of elements of $\mathrm{Hom}_I(i, j)$, there exists an object k of I and an ordered pair (ϕ, ψ) of elements of $\mathrm{Hom}_I(j, k)$ such that $\phi \circ u$ equals $\psi \circ v$. If there always exists k and (ϕ, ψ) as above with ϕ equal to ψ, then the category is **filtered**.

Definition 3.2. An I-**compatible family** of sets, respectively left A-modules $M_\bullet$, right B-modules, $A-B$-bimodules, F-central algebras, is a rule (covariant functor) which for each object i of I associates M_i, a set, resp. left A-module, right B-module, $A-B$-bimodule, F-central algebra, and for each morphism $\phi : i \to j$ in I associates $M_\phi : M_i \to M_j$, a morphism of sets, resp. a morphism of left A-modules, right B-modules, $A-B$-bimodules, F-central algebras, such that M_{Id_i} equals the identity on M_i for every object i of I, and such that the composition $M_\psi \circ M_\phi$ equals $M_{\psi\circ\phi}$ for every ordered pair (ϕ, ψ) of composable morphisms in I. For I-compatible families $M_\bullet$ and $N_\bullet$, a **homomorphism** $a_\bullet$ of I-compatible families is a rule which to every object i of I associates $a_i : M_i \to N_i$, a morphism of sets, resp. left A-modules, right B-modules, $A-B$-bimodules, F-central algebras, such that for every morphism $\phi : i \to j$ in I, the composition $a_j \circ M_\phi$ equals $N_\phi \circ a_i$.

Lemma 3.3. *For every morphism $a_\bullet$ of I-compatible families of left A-modules, the rule associating to every object i of I the image of a_i, resp. the kernel of a_i, is an I-compatible family of*

left A-modules. Similarly, for every morphism of I-compatible families of sets, resp. F-central algebras, the rule associating to every object i of I the image of a_i is an I-compatible family of sets, resp. F-central algebras. For each I-compatible family $M_\bullet$, the identity maps $M_i \to M_i$ form a homomorphism of I-compatible families of left A-modules. For homomorphisms of I-compatible families $a_\bullet : M_\bullet N_\bullet$ and $b_\bullet : N_\bullet \to P_\bullet$, the composition $(b_i \circ a_i)_i$ is a homomorphism of I-compatible families of left A-modules.

Proof. This is straightforward. □

Altogether, these notions give a category whose objects are I-compatible families and whose morphisms are morphisms of I-compatible families.

Definition 3.4. For every M, a set, respectively a left A-module, right B-module, $A-B$-bimodule, F-central algebra, the **constant** I-compatible family is the I-compatible family $\mathrm{const}_{I,M,\bullet}$ such that every M_i equals M and every M_ϕ equals Id_M. For every $a : M \to N$ a morphism of sets, resp. left A-modules, right B-modules, $A-B$-bimodules, F-central algebras, the **constant** morphism of constant I-compatible families,

$$\mathrm{const}_{I,a,\bullet} : \mathrm{const}_{I,M,\bullet} \to \mathrm{const}_{I,N,\bullet},$$

associates to every object i of I the morphism $a : M \to N$. For an I-compatible family $M_\bullet$, an (inverse) **limit** of $M_\bullet$ is a pair $(L, p_\bullet)$ of L, a set, resp. left A-module, right B-module, $A-B$-bimodule, F-central algebras, and a morphism of I-compatible families,

$$p_\bullet : \mathrm{const}_{I,L,\bullet} \to M_\bullet,$$

such that for every such pair $(K, u_\bullet)$ there exists unique $v : K \to L$ a morphism of sets, resp. left A-modules, right B-modules, $A-B$-bimodules, with $u_\bullet$ equal to the composition $p_\bullet \circ \mathrm{const}_{v,\bullet}$. A limit is unique up to unique isomorphism, and it is denoted $L = \varprojlim M_\bullet$. If I is a discrete category, this is also called a **product** and is denoted $\prod M_\bullet$. Similarly, a **colimit** (or **direct limit**) of $M_\bullet$ is pair $(P, q_\bullet)$ of P, a set, resp. left A-module, right B-module, $A-B$-bimodule, F-central algebras, and a morphism of I-compatible families

$$q_\bullet : M_\bullet \to \mathrm{const}_{I,P,\bullet},$$

such that for every such pair $(Q, t_\bullet)$ there exists a unique $s : P \to Q$, a morphism of sets, resp. left A-modules, right B-modules, $A-B$-bimodules, F-central algebras, with $t_\bullet$ equal to the composition $\mathrm{const}_{f,\bullet} \circ q_\bullet$. A colimit is unique up to unique isomorphism, and it is denoted $P = \varinjlim M_\bullet$. If I is a discrete category, this is also called a **coproduct**. A coproduct of sets is denoted $\bigsqcup M_\bullet$. A coproduct of left A-modules, resp. right B-modules, $A-B$-bimodules is denoted $\bigoplus M_\bullet$.

Lemma 3.5. *Every I-compatible family $M_\bullet$ of sets has a limit $(\varprojlim M_\bullet, p_\bullet)$. For an I-compatible family $M_\bullet$ of left A-modules, respectively right B-modules, $A-B$-bimodules, F-central algebras, there is a unique structure of left A-module, resp. right B-module, $A-B$-bimodule, on $\varprojlim M_\bullet$ such that $p_\bullet$ is a morphism of I-compatible families of left A-modules, resp. right B-modules, $A-B$-bimodules. With this structure, also $(\varprojlim M_\bullet, p_\bullet)$ is a limit of the I-compatible family $M_\bullet$ of left A-modules, resp. right B-modules, $A-B$-bimodules, F-central algebras.*

Proof. By hypothesis, I has a set $\mathrm{Ob}I$ of objects. By the axioms of set theory, there is a Cartesian produt $\prod M_\bullet$ of all sets M_i indexed by i in $\mathrm{Ob}I$. Denote the coordinate projections from this Cartesian product as

$$\mathrm{pr}_{M_\bullet,i} : \prod M_\bullet \to M_i.$$

If $M_\bullet$ is an I-compatible family of left A-modules, respectively right B-modules, $A-B$-bimodules, then also $\prod M_\bullet$ has a unique structure of left A-module, resp. right B-module, $A-B$-bimodule, F-central algebras, such that every $\mathrm{pr}_{M_\bullet,i}$ is a morphism of left A-modules, resp. right B-modules, $A-B$-bimodules, F-central algebras. By the universal property of Cartesian products, a morphism from K to $\prod M_\bullet$ is equivalent to a family of morphisms $u_i : K \to M_i$ indexed by $i \in \mathrm{Ob}I$, and this also holds in the category of left A-modules, resp. right B-modules, $A-B$-bimodules, F-central algebras.

Define $\varprojlim M_\bullet$ to be those elements m of $\prod M_\bullet$ such that $M_\phi \circ \mathrm{pr}_i$ and pr_j map m to the same element in M_j for every morphism $\phi : i \to j$ in I. Inside $M_\bullet$, this is a subset, resp. a left A-submodule, right B-submodule, $A-B$-bisubmodule, F-central algebras. For every i in $\mathrm{Ob}I$, denote the restriction of $\mathrm{pr}_{M_\bullet,i}$ to $\varprojlim M_\bullet$ by

$$p_i : \varprojlim M_\bullet \to M_i.$$

By construction, this gives a pair $(\varprojlim M_\bullet, p_\bullet)$ as in the definition. The universal property for $(\prod M_\bullet, \mathrm{pr}_\bullet)$ implies the universal property for $(\varprojlim M_\bullet, p_\bullet)$. □

Corollary 3.6. *For every strictly small indexing category I, for every morphism of I-compatible families, $a_\bullet : M_\bullet \to N_\bullet$, if every $a_i : M_i \to N_i$ is injective, then also the map of colimits is injective, $\varprojlim a_\bullet : \varprojlim M_\bullet \hookrightarrow \varprojlim N_\bullet$. On the other hand, $\varprojlim a_\bullet$ is surjective if every a_i is surjective and the I-compatible system of kernels is* ***stationary****, i.e., for every object i there exists a morphism $\phi : j \to i$ such that for every morphism $\psi : k \to j$, the images of $Ker(a_k)$ and $Ker(a_j)$ are equal in $Ker(a_i)$ via the maps $M_{\phi\circ\psi}$ and M_ϕ.*

Proof. Since the limit is, by construction, a subset of the product, injectivity of a map of colimits reduces to injectivity of a map of coproducts, which is immediate. The result about surjectivity is more subtle; please search for the keyword "Mittag-Leffler condition" in a more advanced algebra textbook (such as Lang's textbook). □

Lemma 3.7. *Every I-compatible family $M_\bullet$ of sets has a colimit set. If I is a filtered category, then for an I-compatible family $M_\bullet$ of left A-modules, respectively right B-modules, $A-B$-bimodules, F-central algebras, there is a unique structure of left A-module, resp. right B-module, $A-B$-bimodule, F-central algebra, on the colimit set such that it is also a colimit of left A-modules, resp. right B-modules, $A-B$-bimodules, F-central algebras. If I is not necessarily prefiltered, then a colimit of $M_\bullet$ still exists in the category of left A-modules, resp. right B-modules, $A-B$-bimodules, but the induced map from the colimit set to the underlying set of the colimit module is not necessarily a bijection.*

Proof. The coproduct set is the subset $\sqcup M_\bullet$ of the Cartesian product $\mathrm{Ob}I \times (\cup M_\bullet)$ consisting of ordered pairs (i, m_i) such that m_i is an element of M_i. The inclusion maps are

$$\mathrm{incl}_i : M_i \to \sqcup M_\bullet, \quad m_i \mapsto (i, m_i).$$

The colimit set is the quotient by the smallest equivalence relation such that $\mathrm{incl}_j \circ M_\phi(m_i)$ is equivalent to $\mathrm{incl}_i(m_i)$ for every morphism $\phi : i \to j$ in I and for every $m_i \in M$. Note that the colimit set is the union of the images of the maps q_i, and elements $m_i \in M_i$ and $m_j \in M_j$ have equal images under q_i and q_j if and only if there exist morphisms $\phi : i \to k$ and $\psi : j \to k$ in I such that $M_\phi(m_i)$ equals $M_\psi(m_j)$.

Now assume that I is a filtered category, and let $M_\bullet$ be an I-compatible family of Abelian groups, e.g., the underlying additive group of a left A-module, a right B-module, or an $A-B$-bimodule. Then for all objects i, j in $\mathrm{Ob}I$, there exist morphisms $\phi : i \to k$ and $\psi : j \to k$ in I. Thus, $q_i(m_i) + q_j(m_j)$ can be defined as $q_k(M_\phi(m_i) + M_\psi(m_j))$. Is this well-defined? For every morphism $\phi' : i \to k$, there exists a morphism $\chi : k \to \ell$ in I such that $\chi \circ \phi$ equals $\chi \circ \phi'$. Thus, $M_\chi(M_\phi(m_i) + M_\psi(m_j))$ equals $M_\chi(M_{\phi'}(m_i) + M_\psi(m_j))$. Thus, the images in the colimit of $M_\phi(m_i) + M_\psi(m_j)$ and $M_{\phi'}(m_i) + M_\psi(m_j)$ are equal. Therefore addition is well-defined. The axioms for an Abelian group for the colimit set follow from the axioms for the Abelian groups M_i and the axioms for Abelian group homomorphisms M_ϕ. By construction, every q_i is a homomorphism of Abelian groups. Thus, the colimit set is a colimit of $M_\bullet$ in the category of Abelian groups. The argument is similar if $M_\bullet$ is an I-compatible family of left A-modules, resp. right B-modules, $A-B$-modules, F-central algebras.

Finally, assume that $M_\bullet$ is an I-compatible family of modules, but do not assume that I is a filtered category. Inside $\prod M_\bullet$, define $\bigoplus M_\bullet$ to be the submodule of elements $m = (m_i)_{i \in \mathrm{Ob}I}$ such that m_i is zero for all but finitely many i. Define q_i to be the morphism sending m_i to the unique element m such that $\mathrm{pr}_j(m) = 0$ for all $j \neq i$ and $\mathrm{pr}_i(m)$ equals m_i. This is a homomorphism to $\bigoplus M_\bullet$. It is straightforward to check that this is a coproduct in the category of modules. The colimit is constructed in the analogous manner as above: form the quotient by the submodule generated by the image of $q_j \circ M_\phi - q_i$ for every morphism $\phi : i \to j$ in I. □

[HERE]

Corollary 3.8. *For every strictly small category, for every morphism of I-compatible families $a_\bullet : M_\bullet \to N_\bullet$, if a_i is surjective for every object i in I, then also the induced map of colimits is surjective. For every strictly small, filtered category I, for every morphism of I-compatible families $a_\bullet : M_\bullet \to N_\bullet$, if a_i is injective for every object i in I, then also the induced map of colimits is surjective.*

Proof. For the first statement, since the colimit is a quotient of the direct sum, then it suffices to prove that the induced map of direct sums is surjective. Since the direct sum of $(N_i)_{i \in \mathrm{Ob}I}$ is generated by the images of N_i, and since every N_i is in the image of M_i, then the induced map of direct sums is surjective.

The second statement uses the fact that every element of $\varinjlim M_\bullet$ is the image of an element $m_i \in M_i$ for some object i of I. For $a_i(m_i)$, if the image in $\varinjlim N_\bullet$ is zero, then there exists a morphism $\phi : i \to j$ such that N_ϕ maps $a_i(m_i)$ to zero. Then a_j also maps $M_\phi(m_i)$ to zero. Since a_j is injective, it follows that $M_\phi(m_i)$ is zero. Since the image of m_i in the colimit also equals the image

of $M_\phi(m_i)$ in the colimit, it follows that the image of m_i in the colimit equals 0. Therefore the induced map of colimits is injective. □

The construction of colimit of F-central algebras requires the tensor product.

4 Exact Sequences of Modules

Definition 4.1. A ($\mathbb{Z}$-graded) **cochain complex** $V^\bullet$ of left A-modules, resp. right B-modules, $A-B$-bimodules, is an ordered pair $((V^n)_{n\in\mathbb{Z}}, (d_V^n)_{n\in\mathbb{Z}})$ of a sequence $(V_n)_{n\in\mathbb{Z}}$ of left A-modules, resp. right B-modules, $A-B$-bimodules, and a sequence $(d_V^n : V^n \to V^{n+1})_{n\in\mathbb{Z}}$ of homomorphisms of left A-modules, resp. right B-modules, $A-B$-bimodules, such that the composite $d^{n+1}\circ d^n$ is the zero homomorphism for every $n\in\mathbb{Z}$. (Please note that the superscript is an index, not a product or direct sum.) For cochain complexes $V^\bullet$ and $W^\bullet$ of left A-modules, resp. right B-modules, $A-B$-bimodules, a **cochain map** $f^\bullet$ of left A-modules, resp. right B-modules, $A-B$-bimodules from $V^\bullet$ to $W^\bullet$ is a sequence $(f^n : V^n \to W^n)_{n\in\mathbb{Z}}$ of homomorphisms of left A-modules, resp. right B-modules, $A-B$-bimodules, such that the composite $f^{n+1}\circ d_V^n$ equals $d_W^n \circ f^n$ for every $n\in\mathbb{Z}$. If every f^n is an inclusion of a submodule, then $V^\bullet$ is a **cochain subcomplex** of $W^\bullet$; note that then the differentials on the subcomplex are uniquely determined. For cochain complexes $V^\bullet$ and $W^\bullet$ of left A-modules, resp. right B-modules, $A-B$-bimodules, and for cochain maps, $f^\bullet, g^\bullet : V^\bullet \to W^\bullet$, of left A-modules, resp. right B-modules, $A-B$-bimodules, a **cochain homotopy** $s^\bullet$ from $f^\bullet$ to $g^\bullet$ of left A-modules, resp. right B-modules, $A-B$-bimodules, is a sequence $(s^n : V^n \to W^{n-1})_{n\in\mathbb{Z}}$ such that $f^n - g^n$ equals $d_W^{n-1}\circ s^n + s^{n+1}\circ d_V^n$ for every $n\in\mathbb{Z}$. If there exists such a cochain homotopy, then $f^\bullet$ is **homotopic** to $g^\bullet$. A cochain map is **nullhomotopic** if there exists a cochain homotopy from the chain map to the zero chain map. Thus, $f^\bullet$ is homotopic to $g^\bullet$ if and only if $f^\bullet - g^\bullet$ is nullhomotopic.

Lemma 4.2. *For every cochain complex $V^\bullet$, the sequence $(Id_{V^n})_{n\in\mathbb{Z}}$ is a cochain map. A composition of cochain maps of left A-modules, resp. right B-modules, $A-B$-bimodules, is again a cochain map of left A-modules, resp. right B-modules, $A-B$-bimodules. Thus, there is a category of cochain complexes of left A-modules, resp. right B-modules, $A-B$-bimodules. For a cochain map, the sequence of kernels, respectively images, forms a cochain subcomplex. Similarly, there is a unique structure of cochain complex on the sequence of cokernels such that the sequence of quotient homomorphisms is a cochain map. Finally, for every cochain homotopy $s^\bullet$ between cochain maps, $f^\bullet, g^\bullet : V^\bullet \to W^\bullet$, for every cochain map $e^\bullet : U^\bullet \to V^\bullet$ and for every cochain map $h^\bullet : W^\bullet \to Y^\bullet$, the sequence $(s^n\circ e^n)_{n\in\mathbb{Z}}$ is a cochain homotopy from $f^\bullet\circ e^\bullet$ to $g^\bullet\circ e^\bullet$, and the sequence $(h^{n-1}\circ s^n)_{n\in\mathbb{Z}}$ is a cochain homotopy from $h^\bullet\circ f^\bullet$ to $h^\bullet\circ g^\bullet$. Thus there is also a well-defined category in which cochain maps are replaced by cochain homotopy classes of cochain maps.*

Proof. This is straightforward. □

Definition 4.3. For every cochain complex $V^\bullet$, for every integer n, the **cocycle submodule** in degree n, $Z_V^n = Z^n(V^\bullet)$, is the kernel of d_V^n as a submodule of V^n. The sequence $(Z_V^n)_{n\in\mathbb{Z}}$ forms

a cochain subcomplex of $V^\bullet$ in which every differential is the zero homomorphism. This is the **cocycle subcomplex**, $Z_V^\bullet$. The **coboundary submodule** in degree n, $B_V^n = B^n(V^\bullet)$, is the image of d_V^{n-1}. Since $d_V^n \circ d_V^{n-1}$ is zero, B_V^n is a submodule of Z_V^n. The sequence $(B_V^n)_{n\in\mathbb{Z}}$ is the **coboundary subcomplex**, $B_V^\bullet$, of $Z_V^\bullet$. As with $Z_V^\bullet$, each differential is the zero homomorphism. Finally, the **cohomology complex** $H_V^\bullet$ is the quotient of the cochain complex $Z_V^\bullet$ by the cochain subcomplex $B_V^\bullet$, i.e., $H_V^n = H^n(V^\bullet)$ equals $Z^n(V^\bullet)/B^n(V^\bullet)$. As with $Z_V^\bullet$ and $B_V^\bullet$, each differential for $H_V^\bullet$ is the zero homomorphism.

Lemma 4.4. *For every cochain map $f^\bullet : V^\bullet \to W^\bullet$, each f^n maps $Z^n(V^\bullet)$ to $Z^n(W^\bullet)$ and maps $B^n(V^\bullet)$ to $B^n(W^\bullet)$. Thus, there are well-defined cochain maps $Z_f^\bullet : Z_V^\bullet \to Z_W^\bullet$ and $B_f^\bullet : B_V^\bullet \to B_W^\bullet$. The cocycle complex is functorial, i.e., $Z^n_{Id_V}$ equals the identity map on Z_V^n, and $Z_f^n \circ Z_e^n$ equals $Z^n_{f\circ e}$ for cochain maps $e^\bullet : U^\bullet \to V^\bullet$ and $f^\bullet : V^\bullet \to W^\bullet$. Similarly, the boundary complex is functorial. Thus, also the cohomology complex $H_V^\bullet$ is functorial.*

Proof. This is straightforward. □

Lemma 4.5. *For cochain complexes $V^\bullet$ and $W^\bullet$, for cochain maps $f^\bullet, g^\bullet : V^\bullet \to W^\bullet$, if there exists a cochain homotopy $s^\bullet$ from $f^\bullet$ to $g^\bullet$, then the maps $H_f^n, H_g^n : H^n(V^\bullet) \to H^n(W^\bullet)$ are equal.*

Proof. Since $f^n - g^n$ equals $d_W^{n-1} \circ s^n + s^{n+1} \circ d_V^n$, the restriction to Z_V^n satisfies $(f^n - g^n)|_Z$ equals $d_W^{n-1} \circ s^n$. Thus, the composite of $(f^n - g^n)|_Z$ with projection to the quotient W^n/B_W^n equals 0. Therefore the induced maps are equal,

$$f^n, g^n : Z_V^n \to W^n/B_W^n.$$

Therefore the induced maps from $H_V^n = Z_V^n/B_V^n$ to $H_W^n = Z_W^n/B_W^n$ are equal. □

Definition 4.6. A cochain map $f^\bullet : V^\bullet \to W^\bullet$ is a **quasi-isomorphism** if the induced map $H_f^n : H^n(V^\bullet) \to H^n(W^\bullet)$ is an isomorphism for every $n \in \mathbb{Z}$. A cochain complex $V^\bullet$ is **exact** (sometimes also called **acyclic**) if H_V^n is a zero module for every $n \in \mathbb{Z}$. An exact complex is also called a **long exact sequence**. A **short exact sequence** is an exact complex $V^\bullet$ so that there is an integer n with V^m equal to a zero module with the possible exceptions of $m = n$, $m = n+1$ and $m = n+2$, i.e., at most three nonzero modules, and they are all consecutive. Explicitly, a **three-term complex** is an ordered triple (V^n, V^{n+1}, V^{n+2}) of modules, and an ordered pair $(d_V^n : V^n \to V^{n+1}, d_V^{n+1} : V^{n+1} \to V^{n+2})$ of module homomorphisms such that $d_V^{n+1} \circ d_V^n$ equals the zero homomorphism. A three-term complex is **right exact**, respectively **left exact**, if d_V^{n+1} is surjective, resp. d_V^n is injective, and if the image of d_V^n equals the kernel of d_V^{n+1}. This is usually written as

$$V^n \xrightarrow{d^n} V^{n+1} \xrightarrow{d^{n+1}} V^{n+2} \to 0, \quad \textbf{resp.}$$

$$0 \to V^n \xrightarrow{d^n} V^{n+1} \xrightarrow{d^{n+1}} V^{n+2}.$$

A three-term complex is **exact** if it is both right exact and left exact. In this case, it is equivalent to a short exact sequence as above, where V^m is defined to be a zero module for every m different from n, $n+1$ and $n+2$. This is usually written as

$$0 \to V^n \xrightarrow{d^n} V^{n+1} \xrightarrow{d^{n+1}} V^{n+2} \to 0.$$

Definition 4.7. A functor to the category of Abelian groups from the category of left A-modules, resp. right B-modules, $A-B$-bimodules, is **additive** if it maps zero modules to zero Abelian groups and if it maps every product $M \times N$ of modules in the category to a product of the corresponding Abelian groups. For such a functor, the induced maps of Hom sets are automatically homomorphisms of Abelian groups. An additive functor is **right exact**, respectively **left exact**, if it maps every short exact sequence of modules to a three-term complex that is right exact, resp. left exact. An additive functor is **exact** if it is both left exact and right exact.

5 Tensor Products

Definition 5.1. For F-central algebras A, B, and C, for an $A-B$-bimodule U for a $B-C$-bimodule V, and for every $A-C$-bimodule W, a B-**balanced** $A-C$-**bilinear map** from $U \times V$ to W is an F-bilinear map $\beta : U \times V \to W$ such that for every $a \in A$, for every $b \in B$, for every $c \in C$, for every $u \in U$, and for every $v \in V$, $\beta(u \cdot b, v)$ equals $\beta(u, b \cdot v)$, $\beta(a \cdot u, v)$ equals $a \cdot \beta(u, v)$, and $\beta(u, v \cdot c)$ equals $\beta(u, v) \cdot c$. Such β is **universal** if for every $A-C$-bimodule Y and for every B-balanced $A-C$-bilinear map γ from $U \times V$ to Y, there exists a unique homomorphism of $A-C$-bimodules $W \to Y$ such that the composition of β with this homomorphism equals γ.

Lemma 5.2. *There exists a universal B-balanced $A-C$-bilinear map from $U \times V$ to an $A-C$-bimodule. One construction is the composition of the universal F-bilinear map $U \times V \to U \otimes_F V$ with the quotient of $U \otimes_F V$ by the F-subspace K generated by elements $(u \cdot b) \otimes v - u \otimes (b \cdot v)$ for all $b \in B$, for all $u \in U$, and for all $v \in V$; this subspace is an $A-C$-subbimodule.*

Proof. The $A-C$-bimodule structure on $U \otimes V$ is the unique structure such that $a \cdot (u \otimes v) = (a \cdot u) \otimes v$ and $(u \otimes v) \cdot c = u \otimes (v \cdot c)$ for every $a \in A$, for every $c \in C$, for every $u \in U$, and for every $v \in V$. Note that $a \cdot ((u \cdot b) \otimes v - u \otimes (b \cdot v))$ equals $((a \cdot u) \cdot b) \otimes v - (a \cdot u) \otimes (b \cdot v)$, and likewise for $((u \cdot b) \otimes v - u \otimes (b \cdot v)) \cdot c$. Thus, the F-subspace K is already an $A-C$-subbimodule of $U \otimes V$, and the quotient of $U \otimes_F V$ by K is a quotient $A-C$-bimodule.

A B-balanced F-bilinear map from $U \times V$ to an F-vector space W is equivalent to an F-bilinear map such that the induced F-linear transformation $U \otimes_F V \to W$ maps every $(u \cdot b) \otimes v - u \otimes (b \cdot v)$ to zero. This is precisely the same as an F-linear transformation to W from the quotient $(U \otimes_F V)/K$. □

Lemma 5.3. *For every I-compatible system $V_\bullet$ of right B-modules with colimit $q_\bullet : V_\bullet \to const_{I,V}$, for every left B-module U, the induced system $Id_U \otimes q_\bullet : U \otimes_B V_\bullet \to const_{I, U \otimes_B V}$ is a colimit of the I-compatible system $U \otimes_B V_\bullet$ of Abelian groups.*

Proof. For every Abelian group Q, a morphism of I-compatible systems of Abelian groups,

$$(t_i : U \otimes_B V_i \to Q)_{i \in \mathrm{Ob} I},$$

is equivalent to a sequence of B-balanced biadditive maps,

$$(\widetilde{t}_i : U \times V_i \to Q)_{i \in \mathrm{Ob} I},$$

such that for every morphism $\phi : i \to j$ in I, also $\widetilde{t}_j \circ (\mathrm{Id}_U \times V_\phi)$ equals $\widetilde{t}_i$. Then, for every $u \in U$, the sequence

$$((\widetilde{t}_i)_{u,\bullet} : V_i \to Q)_{i \in \mathrm{Ob} I},$$

is an I-compatible family of homomorphisms of Abelian groups. By the universal property of the colimit, there is a unique homomorphism of Abelian groups,

$$\widetilde{t}_{u,\bullet} : V \to Q,$$

such that for every object i of I, the composite $\widetilde{t}_{u,\bullet} \circ q_i$ equals $(\widetilde{t}_i)_{u,\bullet}$. This gives a well-defined binary operation,

$$\widetilde{t} : U \times V \to Q, \quad (u, v) \mapsto \widetilde{t}_{u,\bullet}(v).$$

Since eavery $\widetilde{t}_i$ is a biadditive B-balanced map, and since the images of the maps q_i generate V, it follows that also $\widetilde{t}$ is a biadditive B-balanced map. Thus, by the universal property of tensor products, there is a unique homomorphism of Abelian groups,

$$t : U \otimes_B V \to Q,$$

such that $t(u \otimes v)$ equals $\widetilde{t}(u, v)$ for every $u \in U$ and for every $v \in V$. In particular, for every object i of I, the composition $t \circ (\mathrm{Id}_U \otimes q_i)$ equals t_i. Therefore the system $(\mathrm{Id}_U \otimes q_i)_{i \in \mathrm{Ob} I}$ is a colimit of the I-compatible family $U \otimes_B V_\bullet$. □

Lemma 5.4. *For every left B-module V, the functor from the category of right B-modules to Abelian groups that sends each right B-module U to $U \otimes_B V$ is a right exact functor.*

Proof. It is straightforward to see that tensor product sends zero module to zero Abelian groups and preserves finite direct sums. Thus, it is an additive functor. For every short exact sequence of right B-modules,

$$0 \to U' \xrightarrow{q} U \xrightarrow{p} U'' \to 0,$$

every "pure tensor" $u'' \otimes v \in U'' \otimes_B V$ equals the image under $p \otimes \mathrm{Id}_V$ of the pure tensor $u \otimes v \in U \otimes_B V$ for an element $u \in U$ with $p(u) = u''$. Since the pure tensors generate $U'' \otimes_B V$ as an Abelian group, it follows that $p \otimes \mathrm{Id}_V$ is surjective.

Since $p \circ q$ is a zero homomorphism, also $(p \otimes \mathrm{Id}_V) \circ (q \otimes \mathrm{Id}_V)$ equals $(p \circ q) \otimes \mathrm{Id}_V$, and this is a zero homomorphism. Thus, we have a three-term complex. Finally, let $r : U \otimes_B V \to W$ be a homomorphism of Abelian groups such that $r \circ (q \otimes \mathrm{Id}_V)$ is the zero homomorphism. Then the induced B-balanced biadditive map,

$$\widetilde{r} : U \times V \to W, \quad (u, v) \mapsto r(u \otimes v),$$

restricts as zero on $q(U') \times V$. Thus, for every $u'' \in U$ and for every $v \in V$, the image $\widetilde{r}(u, v) \in W$ is independent of the choice of $u \in U$ with $p(u) = u''$. So there is an induced well-defined, B-balanced biadditive map,

$$\widetilde{s} : U'' \times V \to W, \quad (u'', v) \mapsto r(u \otimes v),$$

such that $\widetilde{r}$ equals $\widetilde{s} \circ (p \times \mathrm{Id}_V)$. In other words, there is an induced well-defined homomorphism of Abelian groups,

$$s : U'' \otimes_B V \to W,$$

such that r equals $s \circ (p \otimes \mathrm{Id}_V)$. In particular, the kernel of $p \otimes \mathrm{Id}_V$ is contained in the kernel of r. Taking r to be the quotient of $U \otimes_B V$ by the image of $q \otimes \mathrm{Id}_V$, it follows that the kernel of $p \otimes \mathrm{Id}_V$ equals the image of $q \otimes \mathrm{Id}_V$. □

Definition 5.5. A left B-module V is **flat** (as a left B-module) if for every injective homomorphism of right B-modules, $q : U' \to U$, the following homomorphism of Abelian group is injective,

$$q \otimes_B \mathrm{Id}_V : U' \otimes_B V \to U \otimes_B V, \quad u' \otimes v \mapsto q(u') \otimes v.$$

In other words, V is flat if and only if the right exact functor $- \otimes_B V$ is an exact functor. Similarly, a right B-module U is **flat** (as a right B-module) if tensor product with the module preserves injective homomorphisms of left B-modules; equivalently $U \otimes_B -$ is an exact functor. An $A - B$-bimodule is **flat** as an $A - B$-bimodule if it is both flat as a left A-module and flat as a right B-module.

Lemma 5.6. *Every direct summand of a flat module is flat. Every direct sum of flat modules is flat. Every free module is flat. Every colimit of flat modules over a filtered index category is a flat module.*

Proof. Since tensor product preserves direct sums, and since a summand of an injective homomorphism is also injective, it follows that direct summands of flat modules are flat. Since tensor product is compatible with colimits, in particular it is compatible with direct sums. A direct sum of injective homomorphisms is injective. Thus, a direct sum of flat modules is flat. In particular, the ring is flat with its natural bimodule structure, since tensor product of a module with the ring just returns the module. Thus, every direct sum of modules each isomorphic to the ring is flat, i.e., every free module is flat. Finally, a filtered colimit of injective morphisms is injective. Thus, a filtered colimit of flat modules is flat. □

The most basic examples arise from composition of homomorphisms of modules, considered as balanced bilinear maps on modules of homomorphisms (of modules).

Definition 5.7. For F-central algebras A, B, C, and D, for every $A - B$-bimodule U, for every $A - C$-bimodule V, and for every $A - D$-bimodule W, for every homomorphism of left A-modules, $L : U \to V$, for every $b \in A$, for every $c \in C$, the **scalar multiple** $b \cdot L \cdot c$ is the F-linear transformation $U \to V$ defined by $u \mapsto L(u \cdot b) \cdot c$. Also the **opposite composition** is the F-bilinear map

$$\mathrm{Hom}_{A\text{–mod}}(U, V) \times \mathrm{Hom}_{A\text{–mod}}(V, W) \to \mathrm{Hom}_{A\text{–mod}}(U, W), \quad (L, M) \mapsto M \circ L.$$

Lemma 5.8. *The scalar multiple above is a structure of $B - C$-bimodule on $Hom_{A\text{–}mod}(U, V)$, and the opposite composition is a C-balanced F-bilinear map. The induced F-linear map is a homomorphism of $B - D$-bimodules,*

$$Hom_{A\text{–}mod}(U, V) \otimes_C Hom_{A\text{–}mod}(V, W) \to Hom_{A\text{–}mod}(U, W), \quad L \otimes M \mapsto M \circ L.$$

Proof. Each of these is straightforward to prove. □

Definition 5.9. For every F-central algebra A, for every left A-module V, composition defines a structure of F-central algebra on $\mathrm{End}_{A\text{-mod}}(V) = \mathrm{Hom}_{A\text{-mod}}(V,V)$, the A-**endomorphism algebra** of V. In the usual way, this is a bimodule over itself. For every left A-module U, composition defines on $\mathrm{Hom}_{A\text{-mod}}(U,V)$ a structure of left $\mathrm{End}_{A\text{-mod}}(V)$-module and a structure of right $\mathrm{End}_{A\text{-mod}}(U)$-module, and together these form a bimodule structure, the **natural bimodule structure** on $\mathrm{Hom}_{A\text{-mod}}(U,V)$. For the natural bimodule structures, the opposite composition map above is balanced and induces a homomorphism of bimodules. The analogous definitions and results also hold for right modules in place of left modules.

Adjunction gives natural isomorphisms relating tensor and Hom.

Lemma 5.10. *For all F-central algebras A, B, and C, for every $A-B$-bimodule U, for every $B-C$-bimodule V, and for every $A-C$-bimodule W, the adjunction F-linear transformation,*

$$Hom_{A-C-bimod}(U \otimes_B V, W) = Bil^B_{A-C-bimod}(U \times V, W) \to Hom_{A-B-bimod}(U, Hom_{mod-C}(V,W)),$$

is an isomorphism. These isomorphisms are natural in U and W.

Proof. The proof is the same as in the case for F-vector spaces. □

Definition 5.11. For every F-central algebra R, for every $R-R$-bimodule M, a datum $(f : R \to A, L : M \to A)$ of a homomorphism of F-central algebras $f : R \to A$ algebra A and a homomorphism of $R-R$-bimodules, $L : V \to A$, is **universal** if for every such datum $(g : R \to B, K : M \to B)$, there exists a unique homomorphism of F-central algebras, $e_K : A \to B$, such that $e_K \circ f$ equals g and such that $K = e_K \circ L$. A universal datum is unique up to unique isomorphism. If it exists, it is the **tensor R-algebra** generated by M. It is denoted by $A = T^\bullet_R(M) = R \oplus M \oplus T^2_R(M) \oplus \cdots \oplus T^n_R(M) \oplus \ldots$, where R is the (isomorphic) image of R in A, where M is the (isomorphic) image of M in A, and where $T^n_F(V)$ is the $R-R$-submodule of A generated by the image of the n-fold multiplication map $M \times \cdots \times M \to A$, so that the multiplication gives an isomorphism of $R-R$-bimodules,

$$T^m_R(M) \otimes_R T^n_R(M) \xrightarrow{\cong} T^{m+n}_R(M),$$

for all integers $m, n \geq 0$. Thus, sometimes $T^n_R(M)$ is also denoted $M^{\otimes n}$ or $\bigotimes^n_R M$.

Here is a variant of this universal property: for every $R-R$-bimodule N, for every $R-R$-bimodule homomorphism $\beta : M \otimes_R N \to N$, there exists a unique structure of (left) $T^\bullet_R(M)$-module on N whose restriction to $T^1_F(M) = M$ is β.

Example 5.12. For every nonnegative integer n, when M is the free $R-R$-bimodule $R^{\oplus n}$ with ordered basis $(\mathbf{e}_1, \ldots, \mathbf{e}_n)$, the associated tensor R-algebra $T^\bullet_R(R^{\oplus n})$ is the free, associative, unital R-algebra $R\langle x_1, \ldots, x_n\rangle$ in noncommuting variables $(x_1, \ldots, x_n)$, where each x_i is the image of $\mathbf{e}_i$ in $T^\bullet_F(F^{\oplus n})$. In this case, the universal property is the following: for every R-algebra B, for

every ordered n-tuple $\underline{b} = (b_1, \dots, b_n)$ of elements of B, there exists a unique homomorphism of R-algebras, $e_{\underline{b}} : R\langle x_1, \dots, x_n\rangle \to B$, sending every x_i to b_i. The image of $e_{\underline{b}}$ is the smallest R-subalgebra of B that contains $b_1, \dots, b_n$. The image is denoted by $R\langle b_1, \dots, b_n\rangle \subseteq B$. Alternatively, for every $R-R$-bimodule N, a (left) $R\langle x_1, \dots, x_n\rangle$-module structure on N is equivalent to an ordered n-tuple $(b_1, \dots, b_n)$ of $R-R$-bimodule endomorphisms of N, namely b_i is the linear operator of multiplication by x_i. For nonzero M and $(b_1, \dots, b_n)$ as above, a left submodule is an $R-R$-bisubmodule of N that is mapped back to itself by each of $b_1, \dots, b_n$. For an $R-R$-bimodule P and an ordered n-tuple $(c_1, \dots, c_n)$ of $R-R$-bimodule endomorphisms of P, a morphism of (left) $R\langle x_1, \dots, x_n\rangle$-modules from $(N, (b_1, \dots, b_n))$ to $(P, (c_1, \dots, c_n))$ is an $R-R$-bimodule homomorphism $K : W \to V$ that **intertwines** a_i and b_i, i.e., $K \circ a_i$ equals $b_i \circ K$ for every $i = 1, \dots, n$.

Tensor algebras give coproducts of commutative F-algebras. Let A be a commutative F-algebra, and let $f' : A \to A'$ and $f'' : A \to A''$ be A-**central algebras**, i.e., morphisms of F-central algebras whose image is contained in the center. Then both A' and A'' have a natural structure of $A-A$-bimodule. Thus, the tensor product $A' \otimes_A A''$ is naturally an $A-A$-bimodule. Denote by g', respectively g'', the induced morphism of left A-module, resp. right A-module,

$$g' : A' \to A' \otimes_A A'', \quad a' \mapsto a' \otimes 1,$$

$$g'' : A'' \to A' \otimes_A A'', \quad a'' \mapsto 1 \otimes a''.$$

By construction, $g' \circ f'$ equals $g'' \circ f''$, i.e., the pair (g', g'') **equalizes** the pair (f', f'').

Lemma 5.13. *There is a unique structure of F-central algebra on $A' \otimes_A A''$ such that g' and g'' are homomorphisms of F-central algebras whose images commute. This is the universal pair of morphisms from (A', A'') to an A-central algebra that equalizes (f', f'') with commuting images. In particular, if A' and A'' are also commutative, then (g', g'') is a coproduct of (f', f'') in the category of commutative A-algebras.*

Proof. Consider the multiadditive map to the Abelian group $A' \otimes_A A''$,

$$(A' \times A'') \times (A' \times A'') \to A' \otimes_A A'', \quad ((a', a''), (b', b'')) \mapsto (a'b') \otimes (a''b'').$$

Because A is commutative, this is simultaneously A-balanced in the first two arguments and in the last two arguments. Thus there is a well-defined biadditive map,

$$(A' \otimes_A A'') \times (A' \otimes_A A'') \to A' \otimes_A A''.$$

This defines the multiplication law. By construction, $g'(a')g''(a'') = a' \otimes a'' = g''(a'')g'(a')$ for all $a' \in A'$ and all $a'' \in A''$. Thus, the images of g' and g'' commute with one another. For any pair (h', h'') of morphisms of F-central algebras,

$$h' : A' \to B, \quad h'' : A'' \to B,$$

there is an F-balanced pairing,

$$\widetilde{h} : A' \times A'' \to B, \quad (a', a'') \mapsto h'(a')h''(a'').$$

If $h' \circ f'$ equals $h'' \circ f''$, then this pairing is A-balanced,

$$h'(a'f'(a))h''(a'') = h'(a')(h' \circ f')(a)h''(a'') = h'(a')(h'' \circ f'')(a)h''(a'') = h'(a') \circ h''(f''(a)a''),$$

for all $a \in A$, for all $a' \in A'$, and for all $a'' \in A''$. Thus there is a unique $A - A$-bimodule homomorphism,

$$h : A' \otimes_A A'' \to B, a' \otimes a'' \mapsto h'(a')h''(a''),$$

extending the A-balanced pairing. Finally, if the images of h' and h'' commute, then this is a morphism of A-central algebras,

$$h((a' \otimes a'') \cdot (b' \otimes b'')) = h((a'b') \otimes (a''b'')) = h'(a'b')h''(a''b'') = h'(a')h'(b')h''(a'')h''(b'') = h'(a')h''(a'')h'(b')h''(b'$$

Thus, (g', g'') is the universal pair of morphisms from (A', A'') to an A-central algebra equalizing (f', f'') and with commuting images. □

As usual, there is a reinterpretation of this A-algebra in terms of modules.

Lemma 5.14. *For every commutative F-algebra A and for every left A-module with its induced natural structure of $A-A$-bimodule, an A-algebra homomorphism from $A' \otimes_A A''$ to $Hom_{A-mod}(V, V)$ is equivalent both to a structure of left $A' \otimes_A A''$-module structure on V extending the left A-module structure and an $A' - (A'')^{opp}$-bimodule structure on V extending the natural $A - A$-bimodule structure.*

Proof. Since A is commutative and the $A - A$-bimodule structure on V is the induced natural bimodule structure, the following natural inclusion is surjective,

$$\mathrm{Hom}_{A-A\text{-bimod}}(V, V) \to \mathrm{Hom}_{A-\mathrm{mod}}(V, V).$$

Thus, $\mathrm{Hom}_{A-\mathrm{mod}}(V, V)$ is naturally an A-algebra (with composition giving the multiplication, as usual). Also homomorphisms from $A' \otimes_A A''$ to $\mathrm{Hom}_{A-A\text{-bimod}}(V, V)$ have both interpretations in terms of left module and bimodule structures. □

This implies a universal property for a tensor product of tensor algebras.

Corollary 5.15. *For every commutative F-algebra A, for left A-modules U, V, and W with their induced natural $A - A$-bimodule structures, a pair (f, g) of an A-module homomorphism $f : U \to Hom_{A-mod}(V, V) = Hom_{A-A-bimod}(V, V)$ and an A-module homomorphism $g : W \to Hom_{mod-A}(V, V) = Hom_{A-A-bimod}(V, V)$ whose images commute, is equivalent to an A-algebra homomorphism $T_A^\bullet(U) \otimes_A T_A^\bullet(W)^{opp} \to Hom_{A-mod}(V, V)$.*

This should be compared to the following.

Lemma 5.16. *For every commutative F-algebra A, for left A-modules U, V, and W with their induced natural $A-A$-bimodule structures, a pair (f,g) of an A-module homomorphism $f: U \to Hom_{A-A-bimod}(V,V)$ and an A-module homomorphism $g: W \to Hom_{A-A-bimod}(V,V)$, is equivalent to an A-algebra homomorphism $T_A^\bullet(U \oplus W) \to Hom_{A-mod}(V,V)$. Thus, $T_A^\bullet(U \oplus W)$ is a coproduct of $T_A^\bullet(U)$ and $T_A^\bullet(W)$ in the category of A-central algebras*

The construction of more general coproducts and colimits in the category of associative algebras will require quotient algebras, but this does already give coproducts in the category of commutative algebras.

Proposition 5.17. *For a commutative F-algebra A, coproducts exist in the category of commutative A-algebras.*

Proof. The argument above gives finite coproducts. Let S be any set. Denote by I the category whose objects are finite subsets of S, and whose morphisms are set inclusions among these finite subsets. This is a filtered category. For every family $(A_s)_{s\in S}$ of commutative A-algebras, for every finite subset i of S, define A_i to be the coproduct of A_s for the finitely many elements s in i. For every set inclusion $i \hookrightarrow j$ in I, define $A_i \to A_j$ to be the induced morphism of finite coproducts. This is an I-compatible family of commutative A-algebras. Thus, the colimit set of this I-compatible family is a commutative A-algebra. Thus, this colimit set is the colimit in the category of commutative A-algebras, i.e., it is the coproduct of $(A_s)_{s\in S}$. □

6 Ideals

Let A be an F-central algebra (not necessarily commutative). For the natural (bi)module structure of A on itself, the submodules are ideals.

Definition 6.1. Let A be an F-central algebra with its natural structure of $A-A$-bimodule. A **left ideal** in A, respectively a **right ideal**, is a left A-submodule of the A-module A, resp. a right A-submodule of the A-module A. A **left and right ideal** is an $A-A$-subbimodule of A, i.e., a left ideal that is also a right ideal. The entire module, A, is the **unit ideal**, and all other ideals are **proper ideals**. A proper left ideal is a **maximal left ideal** if the quotient left A-module A/I is a simple left A-module, and similarly for a **maximal right ideal** and a **maximal left and right ideal**.

All of the earlier submodule operations also apply to ideals. In particular, for a subset $\mathcal{F}$ of A, there is the left ideal $A\mathcal{F}$ generated by $\mathcal{F}$, there is the right ideal $\mathcal{F}A$ generated by $\mathcal{F}$, and there is the left and right ideal generated by $\mathcal{F}$, $A\mathcal{F}A$. As discussed earlier, for a commutative F-algebra A, because the identity map $A \to A^{opp}$ is an isomorphism of F-central algebras, every left A-module is

naturally also a right A-module, and vice versa. Then every left A-module is naturally an $A-A$-bimodule. In particular, every left ideal in A is a right ideal in A, and thus a left and right ideal. Because of this, the ideal in a commutative F-algebra A generated by a subset $\mathcal{F}$ is often denoted by $\langle \mathcal{F} \rangle$ – a notation that equally denotes left ideal and right ideals.

Definition 6.2. A nonzero algebra A is a **division algebra** if the only proper left ideal is $\{0\}$ and the only proper right ideal is $\{0\}$ (if the F-dimension is finite, these are equivalent). Equivalently, every nonzero element is invertible. A nonzero algebra A is **simple** if the only left and right ideals are $\{0\}$ and all of A; equivalently, the left and right ideal generated by any nonzero element is the unit ideal. Thus, division algebras are simple, but not every simple algebra is a division algebra. In particular, a commutative division algebra over F is precisely a field together with a field homomorphism (automatically injective) from F to this field; this is called a **field extension** of F. A **central simple algebra** over F is an F-central algebra that is simple and whose center equals the isomorphic image of F. Please note, that there are many simple F-central algebras whose center is strictly bigger than F, e.g., the commutative examples are precisely the nontrivial field extensions of F.

Lemma 6.3. *For every collection of left ideals, respectively right ideals, left and right ideals, the intersection is again a left ideal, resp. right ideal, left and right ideal. Similarly, the sum as an Abelian group is again a left ideal, resp. right ideal, left and right ideal. For every homomorphism of F-central algebras, the preimage of every left ideal, resp. right ideal, left and right ideal, is again a left ideal, resp. right ideal, left and right ideal.*

Proof. Each of these is straightforward and follows by the same method to prove the analogous result for subgroups of a group. □

Proposition 6.4. *Every increasing union of ideals is an ideal, and if each ideal is proper, so is the union. Every proper left ideal, resp. right ideal, left and right ideal is contained in a left ideal, resp. right ideal, left and right ideal, that is maximal.*

Proof. For a totally ordered collection of ideals, for every pair of elements of the union, there exists an ideal in the collection that contains both elements. Thus, the sum of the elements is in that ideal, hence also in the union. Therefore the union is an ideal. Note that if each ideal in the collection is proper, so that 1 is in none of these ideals, then also the union does not contain 1. Thus the union is also proper.

Now let J in A be a left ideal, respectively right ideal, left and right ideal. Let $\mathcal{C}$ be the subset of the power set of A whose elements are left ideals, resp. right ideals, left and right ideals, that are proper and that contain I. By the previous paragraph, every totally ordered subset of $\mathcal{C}$ has a least upper bound in $\mathcal{C}$. Thus, there exists a maximal element in $\mathcal{C}$ by Zorn's lemma, i.e., J is contained in a left ideal, resp. right ideal, left and right ideal, that is maximal. □

Lemma 6.5. *For a left ideal I in A, the induced left A-module structure on A/I, factors through the quotient $A \times (A/I) \xrightarrow{q_{A,I} \times Id_{A/I}} (A/I) \times (A/I)$ if and only if I is also a right ideal. In this case, the*

induced F-bilinear map from $(A/I)\times(A/I)$ to A/I is a structure of F-central algebra. This is the unique structure of F-central algebra on A/I such that $q_{A,I}: A \to A/I$ is a morphism of F-central algebras. In particular, a left and right ideal I is a maximal left and right ideal if and only if A/I is a simple F-central algebra.

Proof. The proof is very similar to the proof of the analogous result that the left G-action on the coset space G/H of a subgroup H factors through a group law on G/H if and only if H is a normal subgroup. □

Definition 6.6. For a left and right ideal $I \subset A$, the **quotient F-central algebra** associated to I is the unique structure of F-central algebra on A/I such that the quotient map, $q_{A,I}: A \to A/I$, is a morphism of F-central algebras. Note that a proper left and right ideal I is maximal if and only if the algebra A/I is simple.

Example 6.7. Let V be a nonzero, finite-dimensional vector space over a field F. The natural F-bilinear map $\mathrm{Hom}_F(V,V)\times V \to V$ by $(L,\vec{v}) \mapsto L(\vec{v})$ is a structure of left F-module on V that is a simple module. Similarly, the natural F-bilinear map $V^*\times \mathrm{Hom}_F(V,V) \to V^*$ by $(\chi, L) \mapsto \chi\circ L$ is a simple right module structure. The left ideals in $\mathrm{Hom}_F(V,V)$ are precisely the subsets $\mathrm{Ann}(U) \cong \mathrm{Hom}_F(V, V/U)$ as U ranges over all F-vector subspaces of V. The maximal left ideals are those ideals such that U is one-dimensional, and then the simple quotient left module is isomorphic to the simple left module V. The right ideals are precisely the subsets $\mathrm{Hom}_F(U,V) \subseteq \mathrm{Hom}_F(V,V)$ as U ranges over all F-vector subspaces of V. The maximal right ideals are those ideals such that V/U is one-dimensional, and then the simple quotient right module is isomorphic to the simple right module V^*. The only left and right ideals are the zero ideal, $\mathrm{Hom}_F(\{0\},V) = \mathrm{Ann}(V)$, and all of $\mathrm{Hom}_F(V,V) = \mathrm{Ann}(\{0\})$. Thus, when V is nonzero, the F-central algebra $\mathrm{Hom}_F(V,V)$ is a central simple algebra over F. Of course for many fields, there are central simple algebras over F with finite dimension that are not isomorphic to one of these, e.g., the quaternion algebra over $F = \mathbb{R}$ is even a central simple F-algebra that is a division algebra over $\mathbb{R}$. Wedderburn's Theorem, which we will discuss, is that when F is a finite field, every finite-dimensional, central simple algebra over F is isomorphic as an F-central algebra to $\mathrm{Hom}_F(V,V)$ for some finite-dimensional F-vector space V.

Quotient algebras complete the construction of coproducts and colimits for associative algebras. Let A be a commutative F-algebra.

Proposition 6.8. *Coproducts and colimits exist in the category of A-central associative unital algebras.*

Proposition 6.9. *Let A' and A'' be A-central, associative, unital algebras. The left regular representation of A' on itself, respectively of A'' on itself, is equivalent to surjections of A-central algebras,*

$$q' : T_A^\bullet(A') \to A', \quad q'' : T_A^\bullet(A'') \to A''.$$

Denote the kernel ideals by I' and I''. The inclusion maps of $A-A$-bimodules into the direct sum,

$$e' : A' \to A' \oplus A'', \quad e'' : A'' \to A' \oplus A'',$$

induce A-algebra homomorphisms of tensor algebras,

$$j' = T_A^\bullet(e') : T_A^\bullet(A') \to T_A^\bullet(A' \oplus A''), \quad j'' = T_A^\bullet(e'') : T_A^\bullet(A'') \to T_A^\bullet(A' \oplus A'').$$

Define A'' to be the quotient A-central algebra of $T_A^\bullet(A' \oplus A'')$ by the left and right ideal generated by $j'(I')$ and $j''(I'')$. Chasing universal properties, for every left A-module V with its natural $A-A$-bimodule structure, an A-algebra homomorphism from A'' to $Hom_{A-A-bimod}(V,V)$ is equivalent to simultaneous extensions of the A-module structure to both a left A'-module structure and a left A''-module structure, but with no requirement that those actions should commute (as arises from homomorphisms from $A' \otimes_A A''$). Rewritten in terms of A-algebras, this implies that A'' is a coproduct of A' and A'' in the category of A-central associative unital algebras.

Together with induction, this gives finite coproducts. Arbitrary coproducts follow by the same technique as in the proof of Proposition 5.17. Finally, let $B_\bullet$ be an I-compatible family of A-central associative unital algebras, where I is a strictly small indexing category. Denote by B the coproduct over all objects i of I of B_i with its natural A-algebra homomorphisms $u_i : B_i \to B$. Thus, simultaneously B is a $B_i - B_i$-bimodule for every object i of I. For every morphism $\phi : i \to j$ of I, there are $B_i - B_i$-module homomorphisms, $u_i : B_i \to B$ and $u_j \circ B_\phi : B_i \to B$, thus there is a difference $B_i - B_i$-module homomorphism, $u_j \circ B_\phi - u_i$. Define J to be the left and right ideal in B generated by the image of $u_j \circ B_\phi - u_i$ for every morphism $\phi : i \to j$ in I. The colimit is the quotient A-central algebra B/J.

Note, this same quotient construction also produces colimits of commutative F-algebra homomorphisms beginning with the coproduct in the category of commutative F-algebras, proved in Proposition 5.17. Of course coproducts and colimits in the category of commutative F-algebras also follow from coproducts and colimits in the category of F-central algebras by taking the associated commutative F-algebra.

Definition 6.10. For every F-central algebra A, the **associated commutative F-algebra** is the quotient F-central algebra $q_A : A \twoheadrightarrow A^{\text{comm}}$ that is universal among homomorphisms of F-central algebras from A to commutative F-algebras. In other words, a homomorphism of F-central algebras from A to B factors through q_A if and only if the image of the homomorphism is a commutative subalgebra of B. The kernel of q_A is the **commutator ideal** denoted $[A, A]$: the left and right ideal in A generated by the set of all commutators $a \cdot b - b \cdot a$ for $a, b \in A$ (the left ideal generated by all commutators is automatically also a right ideal).

Example 6.11. For $\text{Hom}_F(V,V)$, if $\dim_F(V)$ equals 1, then the commutator ideal is the zero ideal, and q_A is the identity. In all other cases, the commutator ideal equals all of $\text{Hom}_F(V,V)$, and the associated commutative F-algebra is just the zero F-vector space.

Definition 6.12. For every commutative F-algebra A, for every A-module M with its natural A–A-bimodule structure, the **symmetric A-algebra** generated by M is the associated commutative F-algebra of the tensor A-algebra of M, $q : T_A^\bullet(M) \twoheadrightarrow S_A^\bullet(M)$. The direct summand $S_A^n(M) = q(T_A^n(M))$ is the n^{th} **symmetric power** of M (relative to A). Thus, the composite A-module homomorphism,

$$L : M \xrightarrow{cong} T_R^1(M) \xrightarrow{cong} S_A^1(M) \hookrightarrow S_A^\bullet(M),$$

is universal among A-module homomorphisms from M to commutative A-algebras. Alternatively, the universal property is as follows: for every A-central associative algebra B and for every A-module homomorphism $K : M \to B$ such that the smallest A-subalgebra generated by Image(K) is commutative (this is automatic if B is commutative), there exists a unique homomorphism of A-algebras, $e_K : S_A^\bullet(M) \to B$ such that K equals $e_K \circ L$. Alternatively, the universal property is as follows: for every left A-module N, for every A-module homomorphism $\beta : M \otimes_A N \to N$ that is commutative in M, i.e., such that $\beta_{v,-} \circ \beta_{u,-} = \beta_{u,-} \circ \beta_{v,-}$ for all $u, v \in M$, there exists a unique structure of (left) $S_A^\bullet(M)$-module on N whose restriction to $S_A^1(M) = M$ is β.

Example 6.13. For V equal to the free A-module $A^{\oplus n}$ with basis $(\mathbf{e}_1, \ldots, \mathbf{e}_n)$, the corresponding symmetric A-algebra is the **polynomial A-algebra** in n variables $x_1, \ldots, x_n$, where x_i is the image of $\mathbf{e}_i$ in the symmetric F-algebra. This symmetric A-algebra is usually denoted $A[x_1, \ldots, x_n]$. In particular, for n equal to 1, this symmetric F-algebra is usually denoted $A[x]$. For every A-central algebra B, for every ordered n-tuple $\underline{b} = (b_1, \ldots, b_n)$ of pairwise commuting elements of B, there exists a unique homomorphism of A-central algebras, $e_{\underline{b}} : A[x_1, \ldots, x_n] \to B$, mapping every x_i to b_i. The image is the smallest A-central subalgebra of B that contains $b_1, \ldots, b_n$, and this A-central subalgebra is commutative. It is denoted by $A[b_1, \ldots, b_n] \subseteq B$. Alternatively, for every A-module W, a (left) $A[x_1, \ldots, x_n]$-module structure on W is equivalent to an ordered n-tuple $\underline{b} = (b_1, \ldots, b_n)$ of pairwise commutating A-module endomorphisms of W, namely b_i is the A-module endomorphism of multiplication by x_i. For an A-module U and an ordered n-tuple $\underline{c} = (c_1, \ldots, c_n)$ of pairwise commuting A-module endomorphisms of U, a morphism of (left) $A[x_1, \ldots, x_n]$-modules from $(W, (b_1, \ldots, b_n))$ to $(U, (c_1, \ldots, c_n))$ is an A-module homomorphism $L : W \to V$ that **intertwines** b_i and c_i, i.e., $L \circ b_i$ equals $c_i \circ L$ for every i.

7 Fractions

Let A be a nonzero F-central associative unital algebra.

Definition 7.1. A subset $S \subset Z(A)$ is a **multiplicative subset** if 1 is in S and $\Sigma \times \Sigma$ maps to Σ under multiplication. A multiplicative subset is **regular** if every element in the multiplicative subset is a regular element. For a multiplicative subset S, the **saturation** of S is the set of all elements $u \in Z(A)$ such that there exist $s, t \in S$ with $su = t$.

Lemma 7.2. *The subset of $Z(A)$ consisting of all regular elements is a regular multiplicative subset. The saturation of a multiplicative subset, respectively a regular multiplicative subset, is a multiplicative subset, resp. a regular multiplicative subset.*

Proof. The element 1 is a regular element in $Z(A)$. Let s and t be regular elements in $Z(A)$. For every nonzero $a \in A$, since s is regular, as is nonzero. Since t is regular, also $(as)t$ is nonzero. By associativity, also $a(st)$ is nonzero. Thus the element $st \in Z(A)$ is again a regular element.

Let s, t, s', t' be elements of S, and let u, u' be elements of $Z(A)$ such that $su = t$ and $s'u' = t'$. Then $(ss')(uu') = (su)(s'u') = tt'$. Since S is a multiplicative subset, both ss' and tt' are in S. Thus uu' is in the saturation of S. If s and t are regular, then for every nonzero a, also $ta = s(ua)$ is nonzero. Thus also ua is nonzero. So every element in the saturation of a regular multiplicative subset is a regular element. □

Definition 7.3. For a left A-module M, for every $m \in M$, the **annihilator** of m in M is the subset $\mathrm{Ann}_M(m) := \{a \in A : am = 0\}$ of A. For a subset S of M, the **annihilator** $\mathrm{Ann}_M(S)$ of S in M is the intersection in A of $\mathrm{Ann}_M(m)$ for every m in S. An element $a \in A$ is M-**regular** if a is contained in $\mathrm{Ann}_M(m)$ only for the zero element $m = 0$, otherwise a is M-**nonregular**. In other words, a is M-regular if multiplication by a is injective on M. More generally, for a subset T of M, an element $a \in A$ is (M, T)-**regular** if for every $t \in T$, the element a is not in $\mathrm{Ann}_M(t)$, and otherwise a is (M, T)-**nonregular**. In particular, $(M, M \smallsetminus \{0\})$-regular is the same as M-regular. An element a is M-**invertible** if multiplication by a is a bijection on M. For a multiplicative subset S of $Z(A)$, the left A-modules is S-**inverting** if s is M-invertible for every $s \in S$. For a right A-module, respectively $A - A$-bimodule, these notions are defined in an analogous way. For every $A - A$-bimodule M, the **center** of M, $Z(M)$, is the set of all elements $m \in M$ such that for every $a \in A$, am equals ma.

Lemma 7.4. *For every left A-module M, respectively for every right A-module M, for every $m \in M$, the annihilator $Ann_M(m)$ in A is a left ideal, resp. a right ideal. For every $A - A$-bimodule M and for every element m in the center of M, this ideal is a left and right ideal.*

Proof. If am equals 0, then $(ba)m = b(am)$ also equals 0 for every $b \in A$. If m is in the center of an $A - A$-bimodule, and if am equals 0, then $(ab)m = a(bm) = a(mb) = (am)b$ is also 0. Thus, the annihilator is a left and right ideal. □

Lemma 7.5. *For an F-central algebra A, for every multiplicative subset S of $Z(A)$, the set I of (A, S)-nonregular elements in A is a left and right ideal in A. The image of S in the quotient ring A/I is a regular multiplicative subset.*

Proof. Clearly the set of (M, S)-nonregular elements is nonempty, since it contains 0, and it is stable for multiplication on the right and on the left by elements of A. It remains to prove that it is stable under addition.

Let s, t be elements of S. Let a, b be elements of A such that as and bt equal 0. Since S is a multiplicative subset, also st is in S. Since s and t are in the center, both $a(st) = (as)t$ and $b(st) = s(bt)$ are zero. Thus, also $(a + b)(st)$ equals 0. So also $a + b$ is (M, S)-nonregular. Therefore I is a left and right ideal.

For $s \in S$ and $a \in A$, if as is in I, then there exists $t \in S$ with $(as)t$ equal to 0. Since S is multiplicatively closed, also st is in S. Therefore a is already in I. Therefore the image of S in A/I is a regular multiplicatively closed subset. □

Definition 7.6. Let A be an F-central algebra, let S be a multiplicative subset of $Z(A)$, and let M be a left A-module. A homomorphism of left A-modules, $f : M \to N$, is S-**inverting** if N is S-inverting. An S-inverting homomorphism $f : M \to N$ is **universal** if for every S-inverting homomorphism $h : M \to P$, there exists a unique homomorphism of left A-modules, $g : N \to P$, such that $g \circ f$ equals h. For a right A-module, respectively, an $A - A$-bimodule, these notions are defined in the analogous way.

Lemma 7.7. *For every S-inverting left A-module, the action of A factors through the quotient A/I by the ideal I of (A, S)-nonregular elements. Every S-inverting homomorphism also inverts the saturation of S. Thus, a universal S-inverting homomorphism out of M as a left A-module exists if and only if there exists a universal inverting homomorphism out of M/IM as a left A/I-module, and where S is replaced by the saturation of the image of S in A/I, which is a saturated, regular multiplicative system in A/I. The analogous result holds for right A-modules and for $A - A$-bimodules.*

Proof. Let N be an S-inverting left A-module. Let s be an element of S, and let a be an element of A such that as equals 0. Then multiplication by as on N is the constant map with image 0. Since multiplication by s on N is a bijection, multiplication by a on M is the constant map with image 0. Thus, for every $a \in I$, the action of a on M is zero. Therefore the action of A on N factors uniquely through an action of A/I on N.

Let u be an element of $Z(A)$ such that su equals t for elements s, t in S. Since multiplication by t on N is a bijection, multiplication by su on N is a bijection. Since also multiplication by s on N is a bijection, multiplication by u on N is a bijection. Thus, N inverts the saturations of S. □

By the lemma, to construct a universal S-inverting homomorphism out of M as a left A-module, it suffices to construct a universal inverting homomorphism out of M/IM as a left A/I-module for the saturation of the image of S in A/I.

Definition 7.8. For an F-central algebra A, for a multiplicative system $S \subset Z(A)$, for a left A-module M, the set of S-**fractions**, $M[S^{-1}]$, is the set of equivalence classes of ordered pairs $(m, s) \in M \times S$ for the equivalence relation $\sim$ on $M \times S$ defined by $(m, s) \sim (n, t)$ if and only if there exists $u \in S$ with utm equal to usn. The equivalence class of (m, s) is denoted m/s. For every $a \in A$, the **fraction product** of a on m/s is defined to be $(am)/s$.

Proposition 7.9. *The fraction product is well-defined, and product by any element $t \in S$ is a bijection on $M[S^{-1}]$. For the natural function $f : M \to M[S^{-1}]$ by $m \mapsto m/1$, there is a unique addition law on $M[S^{-1}]$ such that, together with the fraction product, $M[S^{-1}]$ is a left A-module and f is a homomorphism of left A-modules. The homomorphism f is a universal S-inverting homomorphism.*

Proof. For (m, s) and (m', s') in $M \times S$, if (m, s) is equivalent to (m', s'), then there exists u with $us'm$ equal to usm'. Thus, for a in A, also $us'(am) = a(us'm)$ equals $us(am') = a(usm')$, i.e., (am, s) is equivalent to (am', s'). Therefore the fraction product is well-defined. For every t in

S, if $(ta, s) \sim (ta', s')$, then there exists u in S with $us'ta$ equal to $usta'$. Since ut is in S, also $(a, s) \sim (a', s')$. Thus multiplication by t is injective. Also, $t \cdot a/(st)$ equals a/s, so that multiplication by t is surjective.

For any addition law on $M[S^{-1}]$ that, together with fraction product, makes $M[S^{-1}]$ into a left A-module and makes f into a homomorphism of left A-modules,

$$st \cdot ((a/s) + (b/t)) = h(ta + sb).$$

Thus, $(a/s) + (b/t)$ must be the inverse image of $h(ta + sb)$ under multiplication by st, i.e., $h(ta + sb)/(st) = (ta + sb)/(st)$. It is straightforward to check that this is a well-defined addition law that, together with fraction product, makes $M[S^{-1}]$ into a left A-module and makes f into a homomorphism of left A-modules. Since multiplication by t is a bijection on $M[S^{-1}]$ for every t in S, this homomorphism of left A-modules is S-inverting.

Let $h : M \to P$ be any S-inverting homomorphism. Then the function,

$$g : M \times S \to C, \quad (m, s) \mapsto s^{-1}h(m),$$

factors through the equivalence relation: if $us'm$ equals usm', then $s^{-1}h(m) = u^{-1}(s')^{-1}s^{-1}h(us'm)$, which in turn equals $u^{-1}(s')^{-1}s^{-1}h(usm') = (s')^{-1}h(m')$. Thus, there is a unique set map,

$$g : A[S^{-1}] \to C,$$

such that g maps fraction products in $A[S^{-1}]$ to products in C and such that $g \circ f$ equals h. Then also $g((m/s) + (m'/s')) = g((s'm + sm')/(ss'))$ equals $(ss')^{-1}h(s'm + sm')$. By distributivity, this equals $s^{-1}h(m) + (s')^{-1}h(m') = g(m/s) + g(m'/s')$. Thus g respects addition as well. Therefore g is the unique homomorphism of left A-modules such that $g \circ f$ equals h. □

The analogous result holds for right A-modules, and for $A - A$-bimodules.

Proposition 7.10. *For every $A-A$-bimodule M with (associating) left and right module structures, $\lambda : A \times M \to M$ and $\rho : M \times A \to A$, there is a universal S-inverting $A - A$-bimodule homomorphism $M \to M[S^{-1}]$, and this is also the universal S-inverting left A-module homomorphism and the universal S-inverting right A-module structure. The induced $A - A$-bimodule structures on $Hom_{A-mod}(M[S^{-1}], M[S^{-1}])$ and on $Hom_{mod-A}(M[S^{-1}], M[S^{-1}])$ are both S-inverting. Both the left A-module homomorphism of left multiplication and the right A-module homomorphism of right multiplication are S-inverting homomorphisms,*

$$\widetilde{\lambda} : A \to Hom_{mod-A}(M[S^{-1}], M[S^{-1}]), \quad a \mapsto \lambda_{a,\bullet},$$

$$\widetilde{\rho} : A \to Hom_{A-mod}(M[S^{-1}], M[S^{-1}]), \quad a \mapsto \rho_{\bullet,a},$$

factor through $A \to A[S^{-1}]$, and the induced A-balanced biadditive maps,

$$\lambda[S^{-1}] : A[S^{-1}] \times M[S^{-1}] \to M[S^{-1}],$$

$$\rho[S^{-1}] : M[S^{-1}] \times A[S^{-1}] \to M[S^{-1}],$$

define a unique structure of $A[S^{-1}] - A[S^{-1}]$-bimodule structure on $M[S^{-1}]$ compatible with the given $A - A$-bimodule structure. In particular, there is a unique structure of F-central algebra on $A[S^{-1}]$ compatible with the $A - A$-bimodule structure and such that $A \to A[S^{-1}]$ is a homomorphism of F-central algebras.

Proof. The statement of the proposition contains its own proof. The construction of the fraction set $M[S^{-1}]$ is independent of whether we use the left module structure or the right module structure, since every denominator s is in the center of A. Thus, the map $M \to M[S^{-1}]$ is simultaneously the universal S-inverting left A-module homomorphism and the universal S-inverting right A-module homomorphism. Therefore it is the universal S-inverting $A - A$-bimodule homomorphism.

Since the $A - A$-bimodule $M[S^{-1}]$ is S-inverting, also the Hom $A - A$-bimodules are S-inverting. Therefore the homomorphisms $\widetilde{\lambda}$ and $\widetilde{\rho}$ factor through $A \to A[S^{-1}]$. This defines biadditive maps $\lambda[S^{-1}]$ and $\rho[S^{-1}]$. In particular, when M equals A with its natural $A - A$-bimodule structure, these biadditive maps agree as an A-balanced biadditive map on $A[S^{-1}] \times A[S^{-1}] \to A[S^{-1}]$. Of course this is the fraction product defined earlier. Biadditivity gives distributivity, so this defines a ring structure on $A[S^{-1}]$, the unique ring structure compatible with the $A - A$-bimodule structure and such that $A \to A[S^{-1}]$ is a ring homomorphism. Finally, for an arbitrary $A - A$-bimodule M, it then follows that the biadditive maps above give an $A[S^{-1}] - A[S^{-1}]$-bimodule structure on $M[S^{-1}]$. □

There is another construction of the fraction module that implies a flatness result.

Definition 7.11. For every F-central algebra A and for every saturated multiplicative subset S of $Z(A)$, the **associated category** is the category I whose objects are elements s of S, whose Hom set from s to t for each ordered pair $(s, t) \in S \times S$ is the set of elements $u \in S$ such that us equals t, and whose composition of $v : r \to s$ and $u : s \to t$ is $uv : r \to t$.

Lemma 7.12. *This is a category, i.e., composition is associative and identity morphisms exist. Moreover, it is a filtered category.*

Proof. Let $w : q \to r$, $v : r \to s$, and $u : s \to t$ be morphisms in I. The product $(uv)w$ equals $u(vw)$ since multiplication in A is associative. Thus, the composition of these three morphisms is associative. Also, for every s in S, the morphism $1 : s \to s$ is an identity morphism for s as an object of I.

For every pair of elements s and t of S, there are morphisms, $t : s \to st$ and $s : t \to st$ to a common object st of S. Finally, for every pair of morphisms $u, v : s \to t$ with common source and target, the compositions of these morphisms with $s : t \to st$ both equal the morphism $t : s \to st$. Therefore the category I is a filtered category. □

Definition 7.13. Let S be a saturated multiplicative subset in $Z(A)$ for an F-central algebra A. For every left A-module M, define the **fraction I-compatible family** $M_\bullet$ associated to I to be $M_s = M$ for every s, and $M_u : M_s \to M_t$ to be $u \cdot - : M \to M$ for every morphism $u : s \to t$ in I. For every s in S, the **fraction homomorphism** is

$$c_s : M \to M[S^{-1}], \quad c_s(m) = m/s.$$

Proposition 7.14. *The fraction I-compatible family $M_\bullet$ of a left A-module is an I-compatible family of left A-modules. The collection $(c_s)_{s\in S}$ defines a homomorphism of left A-modules, $\varinjlim M_\bullet \to M[S^{-1}]$. This is an isomorphism of left A-modules.*

Proof. It is straightforward to check that this is an I-compatible family of left A-modules, and that $(c_s)_{s\in S}$ is a homomorphism of I-compatible families. Let s be an element of S, and let m be an element of M such that m/s equals $0/1$. Then there exists $u \in S$ with um equal to 0. Thus, the image of $m \in M_s$ under M_u is zero in M_{us}. It follows that the homomorphism $\varinjlim M_\bullet \to M[S^{-1}]$ is injective. It is also surjective, since every element m/s of $M[S^{-1}]$ is in the image of c_s. Thus, the homomorphism is an isomorphism. □

Corollary 7.15. *With notations as above, the following natural homomorphism of left $A[S^{-1}]$-modules is an isomorphism,*

$$A[S^{-1}] \otimes_A M \to M[S^{-1}].$$

The $A-A$-bimodule $A[S^{-1}]$ is flat both as a left A-module and as a right A-module. For every left A-module M that is flat, also $M[S^{-1}]$ is flat as a left A-module, and similarly for right A-modules.

Proof. If M is flat, then every module in the I-compatible family $M_\bullet$ is flat, since M_s just equals M. Since tensor product preserves colimits, and since filtered colimits preserve injections, it follows that the filtered colimit of the flat left A-modules $M_\bullet$ is also a flat left A-module. The analogous result holds for right A-modules. In particular, when M equals A with its natural $A-A$-bimodule structure, the fraction ring $A[S^{-1}]$ is flat as both a left A-module and as a right A-module. Finally, the natural map of I-compatible families, $A_\bullet \otimes_A M \to M_\bullet$ is an isomorphism, term-by-term. Thus, the induced map of colimits is an isomorphism, $A[S^{-1}] \otimes_A M \to M[S^{-1}]$. □

8 Polynomial division

Definition 8.1. For a nonzero element of $S_F^\bullet(V)$, the **degree** of the element is the minimal integer d such that the element is contained in the F-vector subspace $S_F^0(V) \oplus S_F^1(V) \oplus \cdots \oplus S_F^d(V)$. For every integer $e = 0, \ldots, d$, the **homogeneous part** of the element of degree e is the summand of the element in $S_F^e(V)$.

Lemma 8.2. *For V a nonzero F-vector space, the commutative F-algebra $S_F^\bullet(V)$ is an integral domain. Moreover, the product of two nonzero elements of degrees d and e is a nonzero element of degree $d+e$. If the two factors are homogeneous, so is the product.*

Proof. Any element of $S_F^\bullet(V)$, and thus any finite collection of such elements, is contained in the commutative F-subalgebra $S_F^\bullet(U)$ for a finite dimensional F-subspace U of V. Thus, this lemma reduces to the case of the polynomial ring $F[x_1, \ldots, x_n]$, where it is straightforward by multiplying together pairs of elements of the F-basis $(x_1^{d_1} \cdots x_n^{d_n}) \cdot (x_1^{e_1} \cdots x_n^{e_n}) = x_1^{d_1+e_1} \cdots x_n^{d_n+e_n}$ and using F-bilinearity of multiplication. □

For multiplication of polynomials in a single variable, much more is true.

Proposition 8.3 (Polynomial Division). *For every nonzero element $g \in F[x]$, for every element f in $F[x]$, there exists a unique pair (q,r) of elements of $F[x]$ such that $f = g \cdot q + r$ and either r is zero or the degree of r is strictly less than the degree of g.*

Proof. Every nonzero multiple of g has degree $\geq \deg(g)$, by the lemma. Since the ring is an integral domain, it follows that (q,r) is unique, when they exist.

If f is a multiple of g, say $f = qg$, then the pair $(q,0)$ satisfies the proposition. Thus, assume that f is not a multiple of g, i.e., for every $q \in F[X]$ the difference $f - qg$ is nonzero.

Consider an element r of $F[x]$ of the form $f - qg$ that has minimal degree among all choices of q in $F[x]$. If the degree of r is at least $\deg(g)$, then some multiple of g has the same degree and leading coefficient as r, say $cx^m g$ for some nonzero $c \in F$ and some integer $m \geq 0$. But then $r - cx^m g = f - (q + cx^m)g$ has strictly smaller degree than r, contradicting the hypothesis on r. Thus, the degree of r is strictly smaller than the degree of g, so (q,r) satisfies the proposition. □

Theorem 8.4 (Division Algorithm). *For every pair (f,g) of elements of $F[x]$ that is not $(0,0)$, there exists (s,t) in $F[x] \times F[x]$ such that both f and g are multiples of $h = sf + tg$, i.e., the ideal $\langle f,g\rangle$ generated by f and g equals the ideal $\langle h\rangle$ generated by h.*

Proof. Consider the subset $I = \langle f,g\rangle := \{sf + tg \in F[x] | s,t \in F[x]\}$. This contains both $f = 1f + 0g$ and $g = 0f + 1g$, thus I contains nonzero elements by hypothesis. Let $h = sf + tg$ be a nonzero element in I that has minimal degree among all nonzero elements.

By the proposition, there exists (q,r) such that $f = qh + r$ and either r equals 0 or the degree of r is strictly less than the degree of h. In the second case, $r = (1 - qs)f + (-qt)g$ is a nonzero element of I that has strictly smaller degree than h, contradicting the hypothesis on h. Thus r equals 0, i.e., h divides f. By the same argument, also h divides g. □

Corollary 8.5 (Principal Ideal Domain Property). *For every nonempty subset $\mathcal{F} \subset F[x]$ and the ideal $I = \langle \mathcal{F}\rangle$ it generates, there exists $h \in I$ that generates I, i.e., $\langle \mathcal{F}\rangle$ equals $\langle h\rangle$ for some h in $\langle \mathcal{F}\rangle$. If $\langle \mathcal{F}\rangle$ is nonzero, then this holds for any nonzero element h of minimal degree in $\langle \mathcal{F}\rangle$.*

Proof. If $\mathcal{F}$ equals $\{h\}$, this is tautological. If $\mathcal{F}$ has two elements, it is the previous result. For every finite, nonempty subset of $F[x]$ this follows from the previous result and induction on the size of $\mathcal{F}$.

For an infinite subset $\mathcal{F}$, let h be a nonzero element of I that has minimal degree. In other words, h is a nonzero element of minimal degree of the form $s_1 f_1 + \cdots + s_n f_n$ for some positive integer n, for a finite subset $\{f_1, \ldots, f_n\}$ of $\mathcal{F}$, and for elements $s_1, \ldots, s_n$ of $F[x]$. By the result for finite subsets, h is the greatest common divisor of all elements $f_1, \ldots, f_n$. Now, for every $f \in \mathcal{F} \smallsetminus \{f_1, \ldots, f_n\}$, setting $f_{n+1} = f$ and setting $s_{n+1} = 0$, also $h = s_1 f_1 + \cdots + s_n f_n + s_{n+1} f_{n+1}$. So the same argument again implies that also h is a divisor of $f_{n+1} = f$. Therefore h is a common divisor of all elements of $\mathcal{F}$. Thus every element f of $\mathcal{F}$ is contained in $\langle h\rangle$. So the ideal $\langle \mathcal{F}\rangle$ is a subset of $\langle h\rangle$. Since h is an element of $\langle \mathcal{F}\rangle$, also $\langle h\rangle$ is a subset of $\langle \mathcal{F}\rangle$, i.e., $\langle h\rangle$ equals $\langle \mathcal{F}\rangle$. □

Corollary 8.6 (Irreducibles are prime). *For every nonzero, noninvertible element $f \in F[x]$ that is irreducible and for every element $g \in F[x]$ that is not in $\langle f \rangle$, the ideal $\langle f, g \rangle$ equals all of $F[x]$. More generally, for every pair of positive integers e and d, also $\langle f^e, g^d \rangle$ equals all of $F[x]$. Thus $\langle f \rangle$ is a maximal ideal in $F[x]$. Also, for $q \in F[x]$, the product gq is in $\langle f \rangle$ if and only if q is in $\langle f \rangle$.*

Proof. By the previous result, $\langle f, g \rangle$ equals $\langle h \rangle$ for some h that divides both f and g. Since f is irreducible and h divides f, either h is associate to f or h is invertible, i.e., either $\langle f, g \rangle$ equals $\langle f \rangle$ or it equals all of $F[x]$. By hypothesis, g is not in $\langle f \rangle$, so $\langle f, g \rangle$ is not even contained in $\langle f \rangle$, much less equal. Therefore $\langle f, g \rangle$ equals $F[x]$. In particular, there exists $s, t \in F[X]$ such that $1 = sf + tg$. Therefore also $1 = 1^{d+e-1} = (sf + tg)^{d+e-1}$. Using the Binomial Theorem, this equals $s'f^d + t'g^e$ for elements $s', t' \in F[x]$. Thus, $\langle f^d, g^e \rangle$ equals all of $F[x]$.

In particular, every ideal I that strictly contains $\langle f \rangle$ contains some element g that is not in $\langle f \rangle$. Since I contains the minimal ideal $\langle f, g \rangle$ containing f and g, and since $\langle f, g \rangle$ equals all of $F[x]$, it follows that I equals all of $F[x]$. Thus $\langle f \rangle$ is a maximal ideal.

Since $\langle f \rangle$ is a maximal ideal, the quotient commutative F-algebra $F[x]/\langle f \rangle$ is a field. Since g is not in $\langle f \rangle$, the image element $\overline{g}$ in $F[x]/\langle f \rangle$ is nonzero, and hence invertible. Thus, if $\overline{gq}$ is zero in this field, then (multiplying by the inverse of $\overline{g}$), also $\overline{q}$ is zero in this field, i.e., q is in $\langle f \rangle$. □

Corollary 8.7 (Noetherian Property). *Every nonempty collection of ideals in $F[x]$ that is totally ordered for set inclusion has a maximal element under set inclusion. In particular, every nonzero, noninvertible element of $F[x]$ is divisible by at least one irreducible element, the number of irreducible divisors (up to associates) is finite, and for each irreducible divisor there is a maximal exponent such that the corresponding power of the divisor divides the nonzero, noninvertible element.*

Proof. For a nonempty collection of ideals in $F[x]$ that is totally ordered for set inclusion, the union of all the ideals is again an ideal. By the Principal Ideal Property, this union ideal is principal. The generator is contained in one of the ideals in the collection. Thus that ideal in the collection is already a maximal element of the collection of ideals.

Since every nonempty totally ordered collection of ideals has a maximal element, every nonempty collection of ideals has a maximal element by Zorn's Lemma. In particular, for every nonzero, noninvertible element f of $F[x]$, the collection of ideals containing $\langle f \rangle$ that are not equal to all of $F[x]$ is such a nonempty collection. Thus there exists a maximal element $\langle f_1 \rangle$ in this collection. Since $\langle f_1 \rangle$ is not all of $F[x]$, the element f_1 is noninvertible. Since the nonzero element f is in $\langle f_1 \rangle$, also f_1 is nonzero. Finally, if f_1 is reducible, say $f_1 = gq$ for nonzero, noninvertible elements g and q, then $\langle f_1 \rangle$ is strictly contained in $\langle g \rangle$, and $\langle g \rangle$ is also in the collection of ideals containing $\langle f \rangle$ and strictly contained in $F[x]$. This contradicts the hypothesis that $\langle f_1 \rangle$ was maximal among such ideals. Therefore f_1 is irreducible, and f is a multiple of f_1.

By way of contradiction, assume that f is divisible by each of f_1^ℓ for every positive integer ℓ. Then the collection of ideals $(\langle f/f_1^\ell \rangle)_{\ell=1,2,\dots}$ is an ascending chain of ideals. By the argument above, it

has a maximal element $\langle f/f_1^{\ell}\rangle$. But $\langle f/f_1^{\ell+1}\rangle$ is a bigger element of this collection, contradicting maximality. Thus, there exists a largest positive integer e_1 such that f is divisible by $f_1^{e_1}$.

Finally, by way of contradiction, assume that f is divisible by some countably infinite collection of pairwise nonassociate irreducible elements $(f_1, f_2, \dots, f_\ell, \dots)$. Since irreducibles are prime, also f is divisible by every product $f_1 \cdots f_\ell$. Then the collection of ideals $(f/(f_1 \cdots f_\ell))_{\ell=1,2,\dots}$ is a totally ordered collection of ideals. By the argument above, it has a maximal element $f/(f_1 \cdots f_\ell)$. But $f/(f_1 \cdots f_\ell \cdot f_{\ell+1})$ is a bigger element in this collection. This contradiction proves that f can be divisible by only finitely many □

Corollary 8.8 (Unique Factorization of Polynomials)**.** *Every nonzero, noninvertible element f in $F[x]$ has a factorization $cf_1^{e_1} \cdots f_\ell^{e_\ell}$, where c is a nonzero invertible element of F (i.e., a constant) where $(f_1, \dots, f_\ell)$ is a finite collection of pairwise non-associate, irreducible elements of $F[x]$ (we can normalize these so that they are monic), and where every e_i is a positive integer. This factorization is unique up to permuting the factors $f_i^{e_i}$ and multiplying through by nonzero invertible elements of $F[x]$ (i.e., nonzero scalars in F).*

Proof. First of all, for an irreducible f_2, and for a nonzero, noninvertible element g_1 that is not in $\langle f_2\rangle$, for a positive integer e_2, using that irreducibles are primes, there exist $s_1, s_2 \in F[x]$ such that $1 = s_1 g_1 + s_2 f_2^{e_2}$. Let f be an element that is simultaneously divisible by g_1 and by $f_2^{e_2}$. Then $f = f \cdot 1 = s_2(g_1 f) + s_2(f_2^{e_2} f)$. Since f is divisible by g_1, also $s_2(f_2^{e_2} f)$ is divisible by $g_1 f_2^{e_2}$. Since f is divisible by $f_2^{e_1}$, also $s_1(g_1 f)$ is divisible by $g_1 f_2^{e_2}$. As a sum of two multiples of $g_1 f_2^{e_2}$, also f is divisible by $g_1 f_2^{e_2}$. Combined with a straightforward induction argument, for a list $(f_1, \dots, f_\ell)$ of pairwise nonassociate irreducible factors and for positive integers $(e_1, \dots, e_\ell)$, if f is divisible by each $f_i^{e_i}$, then f is divisible by the product $f_1^{e_1} \cdots f_\ell^{e_\ell}$. By the previous result, there is a finite, nonempty list $(f_1, \dots, f_\ell)$ of irreducible divisors of f that are pairwise nonassociate, and for every i there is a maximal positive integer e_i such that f is divisible by $f_i^{e_i}$. By this induction proof, f is divisible by $f_1^{e_1} \cdots f_\ell^{e_\ell}$. Then the factor $c = f/(f_1^{e_1} \cdots f_\ell^{e_\ell})$ is nonzero and divisible by no irreducible factor. By the previous result, c is invertible. Therefore f has an irreducible factorization $f = cf_1^{e_1} \cdots f_\ell^{e_\ell}$.

Because irreducible elements are prime, for any irreducible factorization of f, the irreducible polynomials that divide f are precisely those associate to one of the irreducible factors in the factorization. So the list of factors occuring in any irreducible factorization is precisely the list $(f_1, \dots, f_\ell)$ of pairwise nonassociate irreducible factors of f (up to associates and permutation). Similarly, the exponent of f_i in any irreducible factorization with these pairwise nonassociate factors is the maximal power of f_i that divides f, since by primeness of irreducibles, a positive integer power of f_i cannot divisor a product of positive integer powers of irreducibles that are not associate to f_i. So also the exponent of f_i in every irreducible factorization of f is precisely the largest positive integer e_i such that $f_i^{e_i}$ divides f. Therefore the irreducible factorization of f is unique up to associates and permutation. □

Corollary 8.9. *For every nonzero F-central algebra A, for every element a of A (possibly 0), the kernel of the homomorphism of F-central algebras $e_a : F[x] \to A$ equals $\langle f\rangle$ for some noninvertible $f \in F[x]$, typically normalized to be monic if it is nonzero, and called the **minimal polynomial** of a*

in the F-central algebra A. The minimal polynomial is nonzero if and only if the subalgebra $F[a] \subset A$ has finite dimension as an F-vector space, and then the degree of f equals the dimension of $F[a]$ as an F-vector space. In this case, for an irreducible factorization of f, say $f = cf_1^{e_1} \cdots f_\ell^{e_\ell}$, there exists an orthogonal idempotent decomposition in $F[a]$, $(\epsilon_1, \ldots, \epsilon_\ell)$, such that the minimal polynomial of each $a_i := a \cdot \epsilon_i$ equals $f_i^{e_i}$. Each $F[a] \cdot \epsilon_i$ equals $F[a_i]$, and the subspaces $(F[a_1], \ldots, F[a_\ell])$ give a direct sum decomposition of $F[a]$ into $F[x]$-submodules that are also quotient algebras of $F[x]$, i.e., $F[a]$ is isomorphic to the direct product commutative F-algebra $F[a_1] \times \cdots \times F[a_\ell]$. The elements a_i satisfy $a_i \cdot a_j = \delta_{i,j} a_i = \delta_{i,j} a_j = a_j \cdot a_i$ for all $1 \le i, j \le \ell$ and $a = a_1 + \cdots + a_\ell$.

Proof. This is a collection of straightforward consequences of the previous results. When $F[a]$ has finite dimension and $\ell \ge 2$, then the greatest common divisor of $(f/f_1^{e_1}, \ldots, f/f_\ell^{e_\ell})$ is 1. Thus, there exist elements $(s_1, \ldots, s_\ell)$ in $F[x]$ such that $1 = s_1 f/f_1^{e_1} + \cdots + s_\ell f/f_\ell^{e_\ell}$. The image ϵ_i of $s_i f/f_i^{e_i}$ satisfies the conditions. □

Definition 8.10. An element a in a nonzero F-central algebra A is **integral** if the subalgebra $F[a] \subset A$ has finite dimension as an F-vector space. For an irreducible monic polynomial f_i in $F[x]$, an integral element a is f_i-**primary** if the minimal polynomial of a equals $f_i^{e_i}$ for some positive integer e_i. Thus, every integral element a equals $a_1 + \cdots + a_\ell$ for integral elements $a_i \in F[a]$ such that $a_i \cdot a_j = \delta_{i,j} a_i = \delta_{i,j} a_j = a_j \cdot a_i$ and such that every a_i is f_i-primary for the distinct irreducible monic polynomials $(f_1, \ldots, f_\ell)$ that are divisors of the minimal polynomial of a.

9 Decomposition into primary subspaces

Let V be a nonzero, finite dimensional F-vector space, and let a be an element in $\mathrm{Hom}_F(V, V)$.

Definition 9.1. An a-**stable subspace** of V is an F-vector subspace U of V such that $a(U)$ is contained in U, i.e., U is an $F[a]$-submodule of V. If $a|_U \in \mathrm{Hom}_F(U, U)$ is f_i-primary for a monic irreducible $f_i \in F[x]$, then U is an f_i-**primary** a-stable subspace.

Corollary 9.2. *There exists a direct sum decomposition of V by a-stable subspaces $(E_1, \ldots, E_\ell)$ such that each E_i is f_i-primary, where $(f_1, \ldots, f_\ell)$ are the monic irreducible factors of the minimal polynomial f of a.*

Proof. If f equals $f_1^{e_1}$, then already $E_1 = V$ is f_1-primary. Thus, assume that the number ℓ of monic irreducible factors of f is > 1. Then by the previous corollary, there exist orthogonal idempotents $(\epsilon_1, \ldots, \epsilon_\ell) \in F[a]$ with $1 = \epsilon_1 + \cdots + \epsilon_\ell$ such that each $a_i := a \cdot \epsilon_i$ has minimal polynomial $f_i^{e_i}$. Define E_i to be the image of ϵ_i. Thus, $\epsilon_j|_{E_i}$ is the identity on E_i for $j = i$, and equals 0 for $j \ne i$. For every $v \in V$, there is a unique decomposition $v = v_1 + \cdots + v_\ell$ with each $v_i \in E_i$, namely $v_i = \epsilon_i(v)$ so that $v = \mathrm{Id}_V(v) = (\epsilon_1 + \cdots + \epsilon_\ell)(v) = v_1 + \cdots + v_\ell$. Therefore the subspaces $(E_1, \ldots, E_\ell)$ give a direct sum decomposition.

Moreover, the image of $a|_{E_i}$ equals the image of $a \cdot \epsilon_i = \epsilon_i \cdot a$ (since ϵ_i is in $F[a]$ thus commutes with a). Thus the image of $a|_{E_i}$ is contained in $E_i = \mathrm{Image}(\epsilon_i)$. Therefore each E_i is an a-stable subspace.

Finally, since $a|_{E_i}$ equals the restriction of $a_i = a \cdot \epsilon_i$, the minimal polynomial of $a|_{E_i}$ equals the minimal polynomial of a_i, namely $f_i^{e_i}$. Therefore each E_i is f_i-primary. □

10 Decomposition into cyclic primary subspaces

Definition 10.1. For an a-stable subspace U of V, an element $u \in U$ is a **cyclic generator** if the smallest a-stable subspace of U containing u is all of U. If there exists a cyclic generator, then U is a **cyclic** a-stable subspace.

For every nonzero u in V, the cyclic a-stable subspace $U = F[a]u$ of V generated by u equals the span of all elements $(a^i u)_{i \geq 0}$. Since V has finite dimension, so does U. The minimal polynomial of $a|_U$ has some finite degree m. Then a basis of U consists of $(a^i u)_{0 \leq i < m}$ since $c_0 a^0 u + \cdots + c_n a^n u$ equals 0 if and only if $(c_0 a^0 + \cdots + c_n a^n)(a^r u)$ equals 0 for every $r \geq 0$ if and only if $c_0 a^0 + \cdots + c_n a^n$ restricts to 0 on U. Thus the dimension of U equals the degree of the minimal polynomial of $a|_U$.

Proposition 10.2. *A nonzero a-stable subspace U is cyclic if and only if the dimension m of U equals the degree of the minimal polynomial of $a|_U$. In this case, for every cyclic generator u, one basis for U consists of $(a^i u)_{0 \leq i < m}$.*

Proof. If U is cyclic, this follows from the previous paragraph. For the other direction, let U be an a-stable subspace whose dimension equals the degree of the minimal polynomial $f = f_1^{e_1} \cdots f_\ell^{e_\ell}$ of $a|_U$. By the previous corollary, there exists a direct sum decomposition of U into a-stable subspaces $(E_1, \ldots, E_\ell)$ such that the minimal polynomial of $a|_{E_i}$ equals $f_i^{e_i}$. In particular, the dimension of E_i is at least the degree of $f_i^{e_i}$. Since the sum of the dimensions of E_i equals the dimension of U, since the sum of the degrees of $f_i^{e_i}$ equals the degree of f, and since the dimension of U equals the degree of f, the dimension of every E_i equals the degree of $f_i^{e_i}$.

For every $u \in E_i$, the minimal polynomial of the restriction of a to the cyclic a-stable subspace $F[a]u$ divides the minimal polynomial $f_i^{e_i}$ of the restriction of a to E_i. Thus, the minimal polynomial of the restriction to $F[a]u$ of a equals f_i^e for some integer $0 \leq e \leq e_i$. Thus, for the maximum value of e that occurs for all elements $u \in E_i$, the operator $f_i(a)^e$ annihilates every element $u \in E_i$. Thus f_i^e is divisible by the minimal polynomial $f_i^{e_i}$, i.e., $e \geq e_i$. Since also $e \leq e_i$, it follows that e equals e_i. Thus, there exists an element $u_i \in E_i$ such that the minimal polynomial of the restriction of a to $F[a]u_i$ equals $f_i^{e_i}$. Then the dimension of $F[a]u_i$ is at least as large as the degree of $f_i^{e_i}$. Since this degree equals the dimension of E_i, it follows that $F[a]u_i$ equals E_i, i.e., E_i is cyclic.

Finally, take u to equal $u_1 + \cdots + u_\ell$ where each u_i is a cyclic generator of E_i. Then $F[a]u$ contains $\epsilon_i(u) = u_i$, hence it contains $F[a]u_i = E_i$. Since the subspaces $(E_1, \ldots, E_\ell)$ give a direct sum decomposition of U, it follows that $F[a]u$ equals U, i.e., U is cyclic. □

Proposition 10.3. *Every nonzero, a-stable, f_i-primary subspace U is a direct sum of a-stable, f_i-primary subspaces that are cyclic.*

Proof. The result is proved by induction on the dimension of U. If the dimension of U is at most the degree of f_i, then the dimension equals the degree of f_i since the minimal polynomial is f_i^e for some positive integer e, so that the dimension of U is at least $e\text{degree}(f_i) \geq \text{degree}(f_i)$. Since the dimension of U equals the degree of the minimal polynomial $f_i^e = f_i$, the previous proposition implies that U is cyclic. Thus, by way of induction, assume that the dimension of U is strictly larger than the degree of f_i, and assume that the result is proved for all nonzero, a-stable, f_i-primary spaces that have strictly smaller dimension.

If U is cyclic, we are done. Thus assume that U is not cyclic. As above, the minimal polynomial of the restriction of a to U equals f_i^e, where e is the maximum of the exponents that occur for the minimal polynomial of a on a cyclic a-stable subspace $F[a]u \subset U$. Thus, there exists u in U such that the minimal polynomial of a on $F[a]u$ equals f_i^e (in particular, u is nonzero). Denote by a_u the restriction of a to $F[a]u$. Denote the quotient F-vector space by

$$q : U \twoheadrightarrow U/F[a]u = \overline{U}$$

Since $F[a]u$ is a-stable, there exists a unique F-linear transformation $\overline{a} : \overline{U} \to \overline{U}$ such that $\overline{a} \circ q$ equals $q \circ a|_U$. The minimal polynomial of $\overline{a}$ on $\overline{U}$ divides the minimal polynomial of $a|_U$, i.e., it is of the form f_i^d for some integer $1 \leq d \leq e$, i.e., $\overline{U}$ is f_i-primary. Since the dimension of $\overline{U}$ is strictly smaller than the dimension of U, by the induction hypothesis, $\overline{U}$ is a direct sum of cyclic subspace $F[a]\overline{u}_j$.

Denote the minimal polynomial of $\overline{a}$ on $F[a]\overline{u}_j$ by $f_i^{d_j}$ for an integer $1 \leq d_j \leq d$. Thus, for every element $u_j \in U$ with $q(u_j) = \overline{u}_j$, the minimal polynomial of a on $F[a]u_j$ equals $f_i^{b_j}$ for an integer b_j with $d_j \leq b_j \leq e$. To complete the proof, it suffices to show that there exists a choice of u_j in the q-fiber over $\overline{u}_j$ such that b_j equals d_j, i.e., such that $f_i(a)^{d_j}u_j$ equals 0. For then $F[a]u_j$ maps isomorphically to $F[a]\overline{u}_j$ under q, i.e., we lift the direct summand $F[a]\overline{u}_j$ from $\overline{U}$ to U. These cyclic subspaces, together with $F[a]\overline{u}$, then give a direct sum decomposition of U.

Let u_j be an element in the q-fiber over $\overline{u}_j$. Since $\overline{u}_j$ is annihilated by $f_i(\overline{a})^{d_j}$, it follows that $f_i(a)^{d_j}u_j$ is an element in $F[a]u$. Moreover, $f_i(a)^{e-d_j}$ applied to this element in $F[a]u$ is zero, since the minimal polynomial of a on U equals f_i^e. Since the minimal polynomial of a_u on $F[a]u$ also equals f_i^e, the kernel of $f_i(a_u)^{e-d_j}$ equals the image of $f_i(a_u)^{d_j}$. Thus, $f_i(a)^{d_j}u_j$ equals $f_i(a_u)^{d_j}v_j$ for some $v_j \in F[a]u$. Thus the difference $u_j - v_j$ is an element in the q-fiber over $\overline{u}_j$ such that $f_i(a)^{d_j}(u_j - v_j)$ equals 0. □

Altogether this gives the rational canonical form.

Theorem 10.4 (Rational Canonical Form)**.** *Let V be a nonzero F-vector space with finite dimension. Let a be an element in $Hom_F(V,V)$. For the minimal polynomial $f = f_1^{e_i}\cdots f_\ell^{e_\ell}$ of a, there exists a direct sum decomposition of V into cyclic, a-stable subspace, each of which is f_i-primary for some monic irreducible factor f_i of f.*

For a cyclic a-stable subspace $F[a]u$ whose minimal polynomial has degree m, say $x^m - (c_{m-1}x^{m-1} + \cdots + c_1x + c_0)$, the ordered basis $\mathcal{B} = (u, au, a^2u, \ldots, a^{m-1}u)$ gives a particularly simple matrix representative of the restriction a_u of a to $F[a]u$, namely $[a_u]^{\mathcal{B}}_{\mathcal{B}}$ is the $m \times m$ matrix,

$$\begin{bmatrix} 0 & 0 & 0 & \ldots & 0 & c_0 \\ 1 & 0 & 0 & \ldots & 0 & c_1 \\ 0 & 1 & 0 & \ldots & 0 & c_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 0 & c_{m-2} \\ 0 & 0 & 0 & \ldots & 1 & c_{m-1} \end{bmatrix}.$$

This the **companion matrix** to the minimal polynomial. Thus, the rational canonical form guarantees that there is an ordered basis for V with respect to which the matrix of a is in block diagonal form, where each block is the companion matrix of f_i^e for some monic irreducible factor of the minimal polynomial f of a, and where e is some positive integer.

For each f_i-primary, cyclic a-stable subspace $F[a]u$, there is another good choice of basis, the **primary basis**. The minimal polynomial of a_u equals f_i^e for some nonnegative integer e. Denote the degree of f_i by m_i. Consider the following ordered basis,

$$\mathcal{C} = (u, au, \ldots, a^{m_i-1}u, f_i(a)u, f_i(a)au, \ldots, f_i(a)a^{m_i-1}u, \ldots, f_i(a)^{e-1}u, f_i(a)^{e-1}au, \ldots, f_i(a)^{e-1}u^{m_i-1}u).$$

With respect to this basis, the matrix of a_u has e diagonal $m_i \times m_i$ blocks equal to the companion matrix of f_i, and the $m_i \times m_i$ block immediately below each of these diagonal $m_i \times m_i$ blocks has a single nonzero entry, namely the entry 1 in the extreme upper right corner. This is the **primary rational canonical form**. In particular, when each m_i equals 1, i.e., when the minimal polynomial of a is a product of linear factors (automatic if the field F is algebraically closed), the matrix representative with respect to $\mathcal{C}$ is precisely Jordan canonical form.

11 Jordan-Chevalley decomposition

This is another name for the "semisimple-nilpotent" decomposition discussed in lecture. In positive characteristic, the decomposition only exists (with its good properties) if every irreducible divisor of the minimal polynomial is *separable*.

Definition 11.1. A homomorphism of rings, $f : A \to B$, is **separable** if the following surjective homomorphism of $B - B$-bimodules has a right inverse homomorphism of $B - B$-bimodules,

$$\beta_{B/A} : B \otimes_A B \to B, \quad b' \otimes b'' \mapsto b' \cdot b''.$$

Right inverse homomorphisms of $B - B$-bimodules are uniquely determined by the images of 1, precisely those idempotent elements ϵ in the fiber of $\beta_{B/A}$ over 1 such that $(b \otimes 1) \cdot \epsilon$ equals $\epsilon \cdot (1 \otimes b)$ for every $b \in B$. Such an element is a **separable idempotent**.

Note that if A and B are commutative, then the kernel of $\beta_{B/A}$ is precisely the ideal generated by all differences $b \otimes 1 - 1 \otimes b$. Thus, an idempotent in the fiber over 1 of $\beta_{B/A}$ is a central idempotent if and only if the idempotent is a (left and right) annihilator of the kernel of $\beta_{B/A}$.

Let F be a field, and let $f \in F[x]$ be a nonconstant, irreducible element. Let E be the corresponding primitive extension field $F[x]/\langle f(x)\rangle$.

Lemma 11.2. *If the formal derivative $f'(x)$ is relatively prime to $f(x)$, then there exists a separable idempotent element for E/F.*

Proof. There exist elements $s(x), t(t) \in F[x]$ such that

$$1 = s(x)f(x) + t(x)f'(x).$$

Inside $F[x,y]$, note that $f(x)-f(y) = (x-y)(f'(x)+(x-y)h(x,y))$ for some unique $h(x,y) \in F[x,y]$. Thus, in the F-algebra $E \otimes_F E = F[x,y]/\langle f(x), f(y)$, the element $e(x,y) = t(x)f'(x)+(x-y)h(x,y)$ is an element that annihilates the kernel $\langle x-y\rangle$ of the multiplication map,

$$\beta_{F,g(x)} : F[x,y]/\langle f(x), f(y)\rangle \mapsto F[z]/\langle f(z)\rangle, \quad x \mapsto z, y \mapsto z,$$

and the ring homomorphism $\beta_{F,f(x)}$ maps $e(x,y)$ to 1. In particular, e^2 and e both map to 1. Thus the difference $e^2 - e$ is of the form $(x-y)k(x,y)$, which is annihilated by e. Therefore, for every integer $r \geq 2$, we have e^{r+1} equals e^r. Setting $\epsilon = e^2$, then ϵ is a separable idempotent in $F[x]/\langle g(x)\rangle$. □

Next assume that $f \in F[x]$ is an irreducible element, so that $E = F[x]/\langle f\rangle$ is a finite field extension of F. There is a unique $g(x) \in F[x]$ such that $g'(x)$ is nonzero and $f(x) = g(x^{p^r})$ for some nonnegative integer r.

Proposition 11.3. *Let F be a field, let $f \in F[x]$ be an irreducible element, and let $E = F[x]/\langle f(x)\rangle$ be the corresponding field extension. Then E is a separable field extension of F if and only if the F-algebra $E \otimes_F E$ has only the zero nilpotent element if and only if the integer r above equals zero if and only if the formal derivative $f_i'(x)$ is nonzero if and only if the formal derivative $f_i'(x)$ is relatively prime to $f_i(x)$.*

Proof. By straightforward computation, $f_i'(x)$ equals zero if and only if I$f_i(x)$ equals $g(x^{p^r})$ for positive r. Since $f_i(x)$ is irreducible, $f_i'(x)$ and $f_i(x)$ have a common factor if and only if $f_i'(x)$ is zero.

If $f_i'(x)$ equals 0, then in the usual Taylor expansion for $f_i(x) - f_i(y)$, which exists as a polynomial identity, we have,

$$f_i(x) - f_i(x) = (x-y)^p h(x,y).$$

It follows that in the ring $E \otimes_F E = F[x,y]/\langle f_i(x), f_i(y)\rangle$, the element $\overline{x} - \overline{y}$ becomes nilpotent after multiplying by a nonzero idempotent. Thus, $E \otimes_F E$ has nonzero nilpotent elements. □