Notes for

Algebra I

Summer Semester 2014*
University of Bonn

Jendrik Stelzner

Online available at https://github.com/cionx/algebra-1-notes-ss-14.
Please send comments and corrections at stelzner@uni-bonn.de.

*Last Changes: 2019-02-11 Commit: 0208371

Preface

The following text are my personal notes for the lecture *Algebra I*, which was given by Prof. Dr. Catharina Stroppel at the University of Bonn during the summer semester of 2014. These notes were initially created to provide me with a more readable version of my original handwritten notes, and to help me and some friend prepare for the upcoming exam.

Since then I have reworked these notes by adding things which I found useful for understanding the topics at hand and by adding various remarks. I have done so in the hope of clarifying things and to give me an opportunity for introducing new errors and mistakes. While the overall structure and choice of topics remains unchanged, the choice of exposition does at times not faithfully reflect the original lecture.

Contents

I. Representations of Groups

Linear Representations of Groups

III. Semisimplicity

Part I

Representations of Groups

Linear Representations of Groups

1. Group Actions

Notation 1.1. If G is a group then we denote by $e \in G$ the neutral element, by gh the composition of $g, h \in G$ and by g^{-1} the inverse of $g \in G$.

Definition 1.2. Given a group G and a set X, an *action of* G *on* X is a map

$$\pi \colon G \times X \to X\,, \quad (g,x) \to g.x\,,$$

such that

$$e.x = x \quad \text{and} \quad (gh).x = g.(h.x)$$

for all $x \in X$, $g, h \in G$. A G*-set* is a set X together with an action of G on X.

Example 1.3. Given a set X, the set

$$S(X) \coloneqq \{f \colon X \to X \mid f \text{ is bijective}\}$$

carries a group structure via $fg \coloneqq f \circ g$ (composition of maps) for all $f, g \in S(X)$. The neutral element is given by the identity id_X.

Definition 1.4. This above group is called the *symmetry group of* X.

1.5. Given a group action $\pi \colon G \times X \to X$, any group element $g \in G$ induces a bijection $\pi_g \in S(X)$ which is given by

$$\pi_g(x) \coloneqq g.x$$

for all $x \in X$, $g \in G$. The resulting map $\pi \colon G \to S(X)$, $g \mapsto \pi_g$ is a group homomorphism because

$$\pi_{gh}(x) = (gh).x = g.(h.x) = \pi_g(\pi_h(x)) = (\pi_g \pi_h)(x)$$

for all $g, h \in G$, $x \in X$.

If on the other hand $\varphi \colon G \to S(X)$ is any group homomorphism, then the map

$$\mathring{\varphi} \colon G \times X \to X, \quad (g,x) \mapsto \varphi(g)(x)$$

is an action of G on X because

$$e.x = \varphi(e)(x) = \mathrm{id}_X(x) = x$$

und

$$(gh).x = \varphi(gh)(x) = (\varphi(g)\varphi(h))(x) = \varphi(g)(\varphi(h)(x)) = g.(h.x)$$

for all $g, h \in G$, $x \in X$.

Both of these constructions are inverse to each other. This leads to the following result:

Lemma 1.6. For any group G and set X there is a 1:1-correspondence

$$\begin{aligned} \{G\text{-actions on } X\} &\overset{1:1}{\longleftrightarrow} \{\text{group homomorphisms } G \to S(X)\}\ , \\ \pi &\longmapsto \hat{\pi}\,, \\ \mathring{\varphi} &\longleftarrow\!\shortmid \varphi\,. \end{aligned}$$

From this lemma we get the idea that group actions are "the same" as "representing" groups as permutation groups.

Example 1.7. Let G be a group.

a) The group G acts on itself by left multiplication, i.e.

$$g.x \coloneqq gx$$

for all $g \in G$, $x \in G$. This is called the (*left*) *regular action of* G.

b) The group G acts onto itself by right multiplication with the inverse, i.e

$$g.x \coloneqq xg^{-1}$$

for all $g \in G$, $x \in G$. This is called the *right regular action of* G.

c) The group G acts onto itself by conjugation, i.e.

$$g.x \coloneqq gxg^{-1}$$

for all $g \in G$, $x \in G$.

d) Let X be a set. Then

$$g.x \coloneqq x$$

for all $g \in G$, $x \in X$ defines an action of G on X. This action is called the *trivial action* on X, and X is called a *trivial G-set.* This action corresponds to the trivial group homomorphism $G \to S(X)$.

e) If X, Y are G-sets then G acts on $\mathrm{Maps}(X, Y) = \{f \mid f\colon X \to Y\}$ via

$$(g.f)(x) \coloneqq g.\left(f\left(g^{-1}.x\right)\right)$$

for all $f \in \mathrm{Maps}(X, Y)$, $g \in G$, $x \in X$. In the special case that Y is a trivial G-set we have that

$$(g.f)(x) = f(g^{-1}.x)$$

for all $f \in \mathrm{Maps}(X, Y)$, $g \in G$ and $x \in X$.

f) If X, Y are G-sets then G acts on $X \times Y$ via

$$g.(x,y) \coloneqq (g.x, g.y)$$

for all $g \in G$, $(x,y) \in X \times Y$.

g) If X is a set then the symmetry group $G \coloneqq S(X)$ acts on X via

$$f.x \coloneqq f(x)$$

for all $f \in G$, $x \in X$. Note that the group homomorphism $S(X) \to S(X)$ which corresponds to this action is just the identity $\mathrm{id}_{S(X)} \colon S(X) \to S(X)$.

Definition 1.8. Let G be a group, and let X, Y be G-sets. A map $f \colon X \to Y$ is called *G-equivariant* if

$$f(g.x) = g.f(x)$$

for all $g \in G$ and $x \in X$. Then set of G-equivariant maps $X \to Y$ is denoted by

$$\operatorname{Hom}_G(X,Y) \coloneqq \{f \colon X \to Y \mid f \text{ is } G\text{-equivariant}\}\,.$$

Lemma 1.9. Let G be a group.

a) If X is a G-set, then $\mathrm{id}_X \colon X \to X$ is G-equivariant.

b) If X, Y, Z are G-sets and $f_1 \colon X \to Y$ and $f_2 \colon Y \to Z$ are G-equivariant, then their composition $f_2 \circ f_1 \colon X \to Z$ is also G-equivariant.

Example 1.10. Let G be a group.

a) Consider G as the regular G-set. Then $f \colon G \to G$ is G-equivariant if and only if f is given by right multiplication with some element $a \in G$ (i.e if $f(g) = ga$ for all $g \in G$).

Proof. Assume there exists $a \in G$ such that $f(g) = ga$ for every $g \in G$. Then

$$f(g.x) = f(gx) = gxa = g.f(x)$$

for all $g \in G$, $x \in G$, so that f is G-equivariant. If on the other hand $f \colon G \to G$ is G-equivariant, then it follows for $a \coloneqq f(e)$ that

$$f(g) = f(g.e) = g.f(e) = g.a = ga$$

for every $g \in G$, so that G is given by right multiplication with a. □

b) If X, Y are trivial G-sets then every map $X \to Y$ is G-equivariant, so that $\operatorname{Hom}_G(X,Y) = \operatorname{Maps}(X,Y)$.

c) If X is any G-set and Y is a trivial G-set then $f \colon X \to Y$ is G-equivariant if and only if $f(g.x) = f(x)$ for all $g \in G$, $x \in X$, i.e. if and only if f is constant on the G-orbits of X.

1.11. The previous lemma shows that for every group G, the class of G-sets together with the G-equivariant maps between them form a category, which we will refer to as G-**Sets**. The objects of G-**Sets** are G-sets and the Hom-setits of G-**Sets** are given by

$$\mathrm{Hom}_{G\text{-}\mathbf{Sets}}(X, Y) \coloneqq \mathrm{Hom}_G(X, Y)$$

for all G-sets X and Y.

Definition 1.12. For every G-set X let X/G be the *set of G-orbits* in X.

1.13. Note that the action of G on X induces an action of G on X/G, which is trivial. The canonical map

$$\mathrm{can}\colon X \to X/G\,, \quad x \mapsto G.x = G\text{-orbit of } x$$

is G-equivariant because

$$\mathrm{can}(g.x) = G.g.x = G.x = \mathrm{can}(x) = g.\mathrm{can}(x)$$

for all $g \in G$, $x \in X$.

Definition 1.14. Let X be a G-set. An element $x \in G$ with $g.x = x$ is called *G-invariant* or a G *fixed point*. The set of G-invariants is denoted by

$$X^G \coloneqq \{x \in X \mid g.x = x \text{ for all } g \in G\}\,.$$

Lemma 1.15. Let X, Y be G-sets and let $f\colon X \to Y$ be G-equivariant. Then

$$f\left(X^G\right) \subseteq Y^G\,.$$

Proof. For every $x \in X^G$ we have that

$$g.f(x) = f(g.x) = f(x)$$

for all $g \in G$ and thus $f(x) \in Y^G$. □

1.16. This lemma shows that every G-equivariant map $f\colon X \to Y$ between G-sets X and Y induces a map $f^G\colon X^G \to Y^G$ by restriction. For every G-set X one has

$$\mathrm{id}_X^G = \mathrm{id}_{X^G}\,,$$

and for all G-sets X, Y, Z and G-equivariant maps $f\colon X \to Y$, $g\colon Y \to Z$ one has

$$(g \circ f)^G = g^G \circ f^G\,.$$

This shows that $(-)^G\colon G\text{-}\mathbf{Sets} \to G\text{-}\mathbf{Sets}$ defines a functor. (That f^G is G-equivariant follows from the actions of G on X^G and Y^G being trivial.)

Lemma 1.17. Let X, Y be G-sets. Then $\mathrm{Hom}_G(X, Y) = \mathrm{Maps}(X, Y)^G$.

Proof. For every map $f\colon X \to Y$ one has that

$$\begin{aligned} f \in \operatorname{Hom}_G(X,Y) &\iff f(g.x) = g.f(x) \text{ for all } g \in G,\ x \in X \\ &\iff f\left(g^{-1}.x\right) = g^{-1}.f(x) \text{ for all } g \in G,\ x \in X \\ &\iff g.f\left(g^{-1}.x\right) = f(x) \text{ for all } g \in G,\ x \in X \\ &\iff g.f = f \text{ for all } g \in G \\ &\iff f \in \operatorname{Maps}(X,Y)^G\,. \end{aligned}$$

□

Definition 1.18. Let X be a G-set and let k be field (or a ring). A map $f\colon X \to k$ is called *invariant* or *G-invariant* if

$$f(x) = f\left(g.x\right)$$

for all $g \in G$, $x \in X$.

1.19. If we consider k as a trivial G-set then a map $f\colon X \to k$ is G-invariant if and only if $f \in \operatorname{Hom}_G(X,k) = \operatorname{Hom}(X,k)^G$. So both notions of G-invariance agree.

Lemma 1.20. Let X be a G-set and let k be field (or a ring). Then a map $f\colon X \to k$ is invariant if and only if f factors through the canonical projection $\mathrm{can}\colon X \to X/G$, i.e. if there exists a map $\bar{f}\colon X/G \to k$ which makes the following diagram commute:

$$\begin{tikzcd} X \arrow[rr, "f"] \arrow[dr, "\mathrm{can}"'] & & k \\ & X/G \arrow[ur, dashed, "\bar{f}"'] & \end{tikzcd}$$

Proof. Both conditions are equivalent to f being constant on the G-orbits of X. □

Example 1.21. Let $G = \{e, s\} \cong \mathbb{Z}/2$ where e is the neutral element and $s^2 = e$. Let G act on $X = \mathbb{R}$ by $e.\lambda = \lambda$ and $s.\lambda = -\lambda$ for all $\lambda \in \mathbb{R}$. We want to know for which n the map $p_n\colon \mathbb{R} \to \mathbb{R}$, $x \mapsto x^n$ is G-invariant. For this we need to check for which n we have that

$$p_n(\lambda) = p_n\left(s^{-1}.\lambda\right) = p_n(s.\lambda) = p_n(-\lambda) = (-1)^n p_n(\lambda)$$

for all $\lambda \in \mathbb{R}$. This holds if and only if n is even.

Lemma 1.22. Let X be a finite G-set and let k be a field (or a ring).

a) The set $\operatorname{Maps}(X,k)$ forms a k-vector space (resp. k-module) via pointwise addition and scalar multiplication.

b) A k-basis of $\operatorname{Maps}(X,k)$ is given by the maps χ_x, $x \in X$ with

$$\chi_x(y) = \delta_{xy} = \begin{cases} 1 & \text{if } x = y\,, \\ 0 & \text{otherwise}\,, \end{cases}$$

for all $y \in X$.

c) The set of invariant maps $\mathrm{Maps}(X,k)^G = \mathrm{Hom}_G(X,k)$ is a k-linear subspace (resp. k-submodule) of $\mathrm{Maps}(X,k)$.

d) A k-basis of $\mathrm{Maps}(X,k)^G$ is given by the maps $\chi_{\mathcal{O}}$, $\mathcal{O} \in X/G$ with

$$\chi_{\mathcal{O}}(y) = \begin{cases} 1 & \text{if } y \in \mathcal{O}\,, \\ 0 & \text{otherwise}\,, \end{cases}$$

for all $y \in X$.

Proof.

a) This is clear.

b) For $f \in \mathrm{Maps}(X,k)$ one has that $f = \sum_{x \in X} f(x)\chi_x$. (Note that this sum is finite, hence well defined.) This is true since for every $y \in X$ we have that

$$\left(\sum_{x\in X} f(x)\chi_x\right)(y) = \sum_{x\in X} f(x)\underbrace{\chi_x(y)}_{=\delta_{xy}} = f(y)\,.$$

This shows that the maps χ_x, $x \in X$ generate $\mathrm{Maps}(X,k)$. They are linear independent since for all coefficients $\alpha_x \in k$, $x \in X$ with $\sum_{x\in X} \alpha_x\chi_x = 0$ one has for every $y \in X$ that

$$\alpha_y = \sum_{x\in X} \alpha_x \underbrace{\chi_x(y)}_{=\delta_{xy}} = 0\,.$$

c) We need to check that for all $f, f_1, f_2 \in \mathrm{Maps}(X,k)^G$ and $\lambda \in k$ we have that $f_1 + f_2 \in \mathrm{Maps}(X,k)^G$ and $\lambda f \in \mathrm{Maps}(X,k)^G$. This holds because

$$\begin{aligned}(g.(f_1+f_2))(x) &= (f_1+f_2)\left(g^{-1}.x\right) = f_1\left(g^{-1}.x\right) + f_2\left(g^{-1}.x\right) \\ &= f_1(x) + f_2(x) = (f_1+f_2)(x)\end{aligned}$$

and

$$(g.(\lambda f))(x) = (\lambda f)\left(g^{-1}.x\right) = \lambda f\left(g^{-1}.x\right) = \lambda f(x) = (\lambda f)(x)$$

for all $x \in X$.

d) The maps $\chi_{\mathcal{O}}$, $\mathcal{O} \in X/G$ are contained in $\mathrm{Maps}(X,k)^G$ since they are constant on the G-orbits of X.

To see that they are a basis of $\mathrm{Maps}(X,k)^G$ let $\mathcal{O}_1, \dots, \mathcal{O}_n$ be the G-orbits in X, and for every $i = 1, \dots, n$ let x_i be a representative of $\mathcal{O}_i$, i.e. let $x_i \in \mathcal{O}_i$.

For every $f \in \mathrm{Maps}(X,k)^G$ one then has that $f = \sum_{i=1}^n f(x_i)\chi_{\mathcal{O}_i}$: For every $y \in X$ there exists a unique j with $y \in \mathcal{O}_j$. Since the map f and the maps $\chi_{\mathcal{O}_i}$ are constant on the G-orbits of X it follows that

$$\sum_{i=1}^n f(x_i)\chi_{\mathcal{O}_i}(y) = \sum_{i=1}^n f(x_i)\chi_{\mathcal{O}_i}(x_j) = f(x_j) = f(y)\,.$$

This shows that the maps $\chi_{\mathcal{O}_i}$, $i = 1, \dots, n$ generate $\operatorname{Maps}(X, k)^G$.

The linear independence follows in the same way as above: For all coefficients $\alpha_i \in k$, $i = 1, \dots, n$ with $\sum_{i=1}^n \alpha_i \chi_{\mathcal{O}_i}$ one has that

$$0 = \left(\sum_{i=1}^n \alpha_i \chi_{\mathcal{O}_i} \right) (x_j) = \sum_{i=1}^n \alpha_i \underbrace{\chi_{\mathcal{O}_i}(x_j)}_{=\delta_{ij}} = \alpha_j$$

for every $j = 1, \dots, n$. □

1.23. If X is an infinite G-set then we can replace $\operatorname{Maps}(X, k)$ by

$$kX \coloneqq \{f \in \operatorname{Maps}(X, k) \mid \operatorname{supp}(f) \text{ is finite}\}$$

where

$$\operatorname{supp}(f) = \{x \in X \mid f(x) \neq 0\},$$

is the *support of* f, i.e

$$kX = \{f \colon X \to k \mid f(x) \neq 0 \text{ for only finitely many } x \in X\}.$$

Note that for all $f_1, f_2, f \in \operatorname{Maps}(X, k)$ and $\lambda \in k$ we have that

$$\operatorname{supp}(f_1 + f_2) \subseteq \operatorname{supp}(f_1) \cup \operatorname{supp}(f_2)$$

and

$$\operatorname{supp}(\lambda f) \subseteq \operatorname{supp}(f).$$

Therefore kX is a k-vector space (resp. k-module) via pointwise addition and scalar multiplication.

Note that for every $x \in X$ we have that $\operatorname{supp}(\chi_x) = \{x\}$ and thus $\chi_x \in kX$. By using the same argumentation as above one finds that χ_x, $x \in X$ is a k-basis of kX, i.e. that for every $f \in kX$ we have that $f = \sum_{x \in X} f(x) \chi_x$ (this sum is well-defined since only finitely many coefficients $f(x)$ are nonzero) and the maps χ_x, $x \in X$ are linearly independent.

The calculation from part c) of the above proof shows that $kX^G \coloneqq (kX)^G$ is a k-linear subspace (resp. k-submodule) of kX. We claim that the maps

$$\chi_{\mathcal{O}} \quad \text{where} \quad \mathcal{O} \in X/G \text{ is finite}$$

form a k-basis of kX^G. Let $\{\mathcal{O}_i \mid i \in I\}$ is the set of orbits with finitely many elements and $x_i \in \mathcal{O}_i$ is a representative.

To see that the maps $\chi_{\mathcal{O}_i}$, $i \in I$ generate kX^G, let $f \in kX^G$. The map f is constant on the G-orbits of X because f is G-invariant. Since f has finite support it further follows that f vanishes on all non-finite G-orbits. It therefore follows in the same way as in part d) of the above proof that $f = \sum_{i \in I} f(x_i) \chi_{\mathcal{O}_i}$. (This sum is finite because f has finite support.) It also follows as in part d) of the proof that the maps $\chi_{\mathcal{O}_i}$, $i \in I$ are linearly independent.

Lemma 1.24. Let X be a finite G-set. Suppose that $X = X_1 \mathbin{\dot\cup} X_2$ with $X_1, X_2 \neq \emptyset$ such that $g.x_1 \in X_1$ and $g.x_2 \in X_2$ for all $x_1 \in X_1$, $x_2 \in X_2$, $g \in G$.

a) $\operatorname{Maps}(X, k) \cong \operatorname{Maps}(X_1, k) \oplus \operatorname{Maps}(X_2, k)$ as k-vector spaces (resp. k-modules).

b) $\operatorname{Maps}(X, k)^G \cong \operatorname{Maps}(X_1, k)^G \oplus \operatorname{Maps}(X_2, k)^G$ as k-vector spaces (resp. k-modules) where we have an induced action on both $\operatorname{Maps}(X_1, k)$ and $\operatorname{Maps}(X_2, k)$ from the G-action on $\operatorname{Maps}(X, k)$ via the isomorphism of the first part.

Proof.

a) By Lemma 1.22 the space $\operatorname{Maps}(X, k)$ has the basis $B \coloneqq \{\chi_x \mid x \in X\}$. Similarly $\operatorname{Maps}(X_i, k)$ has the basis $B_i \coloneqq \{\chi_x \mid x \in X_i\}$ for $i = 1, 2$. Since X is the disjoint union of X_1 and X_2, it follows that there exists an isomorphism of k-vector spaces (resp. k-modules) $\operatorname{Maps}(X, k) \xrightarrow{\sim} \operatorname{Maps}(X_1, k) \oplus \operatorname{Maps}(X_2, k)$ given by

$$\chi_x \mapsto \begin{cases} (\chi_x, 0) & \text{if } x \in X_1\,, \\ (0, \chi_x) & \text{if } x \in X_2\,. \end{cases}$$

b) The action of G on X restrict to actions of G on both X_1 and X_2 since these are closed under the action of G. The group G now acts on $\operatorname{Maps}(X, k)$ via $(g.f)(x) = f(g^{-1}.x)$ for all $g \in G$, $x \in X$, and simlilary on both $\operatorname{Maps}(X_1, k)$ and $\operatorname{Maps}(X_2, k)$. The above isomorphism $\operatorname{Maps}(X, k) \xrightarrow{\sim} \operatorname{Maps}(X_1, k) \oplus \operatorname{Maps}(X_2, k)$ is then G-equivariant. The invariants on the left side are $\operatorname{Maps}(X, k)^G$. The invariants on the right side are

$$(\operatorname{Maps}(X_1, k) \oplus \operatorname{Maps}(X_2, k))^G = \operatorname{Maps}(X_1, k)^G \oplus \operatorname{Maps}(X_2, k)^G,$$

because G acts componentwise on $\operatorname{Maps}(X_1, k) \oplus \operatorname{Maps}(X_2, k)$. □

Example 1.25. Let X be a finite trivial G-set. It follows from the decomposition $X = \dot\bigcup_{x \in X} \{x\}$ that

$$\operatorname{Maps}(X, k) = \langle \chi_x \mid x \in X \rangle_k = \bigoplus_{x \in X} k\chi_x \cong \bigoplus_{x \in X} \operatorname{Maps}(\{x\}, k)\,.$$

In this case we have $\operatorname{Maps}(X, k)^G = \operatorname{Maps}(X, k)$ because the G-action on k is trivial.

Warning 1.26. Given a G-set X and a decomposition of k-vector spaces (resp. k-modules) $\operatorname{Maps}(X, k) = V \oplus W$ such that

$$g.v \in V \quad \text{and} \quad g.w \in W$$

for all $v \in V$, $w \in W$, $g \in G$, then this decomposition is not necessarily arising from a decomposition $X = X_1 \mathbin{\dot\cup} X_2$ as above.

Example 1.27. Take for example the group $G = \{e, s\} \cong \mathbb{Z}/2$ with $s^2 = e$ and let G act on $X = G$ itself by left multiplication. Let k be a field with $\operatorname{char}(k) \neq 2$.

Claim. There is no decomposition $X = X_1 \cup X_2$ as above.

Proof. If such a decomposition would exist then it would either be $X_1 = \{e\}$ and $X_2 = \{s\}$ or $X_1 = \{s\}$ and $X_2 = \{e\}$. But since $s.e = se = s$ and $s.s = ss = e$ we have in both cases that $s(X_1) \subseteq X_2$. □

The vector space $\operatorname{Maps}(X,k)$ has by Lemma 1.22 a basis given by $\{\chi_e, \chi_s\}$ as a basis. Then $\{b_1, b_2\}$ with

$$b_1 \coloneqq \frac{\chi_e + \chi_s}{2} \quad \text{and} \quad b_2 \coloneqq \frac{\chi_e - \chi_s}{2}\,.$$

is also a basis of $\operatorname{Maps}(X,k)$. From $s.\chi_e = \chi_s$ and $s.\chi_s = \chi_e$ it follows that

$$s.b_1 = b_1 \quad \text{and} \quad s.b_2 = -b_2\,.$$

It follows for $V \coloneqq \langle b_1 \rangle_k$ and $W \coloneqq \langle b_2 \rangle_k$ that $\operatorname{Maps}(X,k) = V \oplus W$ with $g.v \in V$ and $g.w \in W$ for all $v \in V$, $w \in W$, $g \in G$.

Lemma 1.28. Suppose the group G acts on a ring R by ring automorphisms (i.e. if $\pi \colon G \times R \to R$ is the action then $\pi_g \colon r \mapsto g.r$ is an ring automorphism of R for every $g \in G$). Then R^G is a subring of R, and therefore in a particular ring itself.

Proof. It holds for every $g \in G$ that $g.1 = \pi_g(1) = 1$, so that $1 \in R^G$. For all $r_1, r_2 \in R^G$, $g \in G$ it holds that

$$g.(r_1 + r_2) = \pi_g(r_1 + r_2) = \pi_g(r_1) + \pi_g(r_2) = g.r_1 + g.r_2 = r_1 + r_2$$

and

$$g.(r_1 r_2) = \pi_g(r_1 r_2) = \pi_g(r_1)\pi_g(r_2) = (g.r_1)(g.r_2) = r_1 r_2\,,$$

so that $r_1 + r_2, r_1 r_2 \in R^G$. □

Example 1.29. Let X be a G-set and k a field (or a ring).

a) The set $\operatorname{Maps}(X,k)$ carries the structure of a ring via pointwise addition and multiplication.

b) The induced G-action on $\operatorname{Maps}(X,k)$ (i.e. $(g.f)(x) = f(g^{-1}.x)$ for all $g \in G$, $x \in X$) is an action by ring automorphisms:

   For all $g \in G$, $x \in X$ it holds that

$$(g.1_{\operatorname{Maps}(X,k)})(x) = 1_{\operatorname{Maps}(X,k)}(g^{-1}.x) = 1 = 1_{\operatorname{Maps}(X,k)}(x)$$

   and therefore $g.1_{\operatorname{Maps}(X,k)} = 1_{\operatorname{Maps}(X,k)}$. For all $f_1, f_2 \in \operatorname{Maps}(X,k)$, $g \in G$, $x \in X$ it holds that

$$\begin{aligned}(g.(f_1 + f_2))(x) &= (f_1 + f_2)\left(g^{-1}.x\right) = f_1\left(g^{-1}.x\right) + f_2\left(g^{-1}.x\right) \\ &= (g.f_1)(x) + (g.f_2)(x) = ((g.f_1) + (g.f_2))(x)\end{aligned}$$

and

$$\begin{aligned}(g.(f_1 f_2))(x) &= (f_1 f_2)\left(g^{-1}.x\right) = f_1\left(g^{-1}.x\right) f_2\left(g^{-1}.x\right) \\ &= (g.f_1)(x)(g.f_2)(x) = ((g.f_1)(g.f_2))(x)\,.\end{aligned}$$

Altogether this shows that G acts by ring homomorphisms. Since π_g has the inverse $\pi_{g^{-1}}$ these homomorphisms are automatically automorphisms.

It follows from Lemma 1.28 that $\mathrm{Maps}(X,k)^G$ is a subring of $\mathrm{Maps}(X,k)$.

c) The symmetric group S_n acts on the polynomial ring $k[X_1,\dots,X_n]$ via

$$\sigma.p(X_1,\dots,X_n) = p(X_{\sigma(1)},\dots,X_{\sigma(n)})$$

for all $\sigma \in S_n$, $p(X_1,\dots,X_n) \in k[X_1,\dots,X_n]$. This is an action by ring automorphisms, so that $k[X_1,\dots,X_n]^{S_n}$ is a subring. This is the ring of *symmetric polynomials*.

Remark 1.30. Similar statements hold for kX and $(kX)^G$ (with the same proofs).

Definition 1.31. Let G, H be groups and let X be both a G-set and H-set. Then the actions of G and H on X *commute* if

$$h.(g.x) = g.(h.x)$$

for all $g \in G$, $h \in H$, $x \in X$.

Remark 1.32. In this case we have that π_g is an H-equivariant map for every $g \in G$ and that π'_h is a G-equivariant map for every $h \in H$, because

$$g.\pi_h(x) = \pi_g(h.x) = g.(h.x) = h.(g.x) = h.\pi_g(x) = \pi_h(g.x)$$

for all $g \in G$, $h \in H$.

Example 1.33. Let G be a group.

a) Then the left regular action and the right regular action of G on G commute.

b) The left regular action and conjugation action on G commute if and only if G is abelian: If . denotes the left regular action and $*$ the conjugation then

$$\begin{aligned} g_1 * (g_2.x) &= g_1(g_2 x)g_1^{-1} = g_1 g_2 x g_1^{-1}\,, && (*) \\ g_2.(g_1 * x) &= g_2\left(g_1 x g_1^{-1}\right) = g_2 g_1 x g_1^{-1}\,, && (**) \end{aligned}$$

for all $g_1, g_2, x \in G$. Therefore

$$\begin{aligned} & (*) = (**) \text{ for all } g_1, g_2, x \in G \\ \iff & g_1 g_2 = g_2 g_1 \text{ for all } g_1, g_2 \in G \\ \iff & G \text{ is abelian}\,. \end{aligned}$$

c) Let $G \coloneqq \mathrm{GL}(2,\mathbb{R})$. Then G acts on $\mathbb{R}^2$ in the natural way. Consider the subgroup

$$H \coloneqq \left\{ \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} \,\middle|\, \lambda \in \mathbb{R}, \lambda \neq 0 \right\} \subseteq \mathrm{GL}(2,\mathbb{R})\,.$$

Then H acts on $\mathbb{R}^2$ by restriction of the G-action. The two actions commute since $gh = hg$ for all $g \in G$, $h \in H$. (Note that H is the center of G.)

Remark 1.34. Let G, H be two groups and let X be a set.

If G and H act on X with commuting actions, then $G \times H$ acts on X via

$$(g,h).x = g.h.x$$

for all $(g,h) \in G \times H$, $x \in X$. This is indeed a group action because

$$1_{(G\times H)}.x = (1_G, 1_H).x = 1_G.1_H.x = x$$

for every $x \in X$, and

$$\begin{aligned}(g',h').((g,h).x) &= (g',h').(g.h.x) = g'.h'.g.h.x \\ &= g'.g.h'.h.x = (g'g).(h'h).x = ((g'g),(h'h)).x = ((g',h')(g,h)).x\end{aligned}$$

for all $(g',h'),(g,h) \in G \times H$, $x \in X$.

If on the other hand $G \times H$ acts on X, then this induces actions of both G and H on X which are given by

$$g.x = (g,1).x \qquad \text{and} \qquad h.x = (1,h).x$$

for all $g \in G$, $h \in H$, $x \in X$. These actions then commute because

$$h.(g.x) = (1,h).(g,1).x = (g,h).x = (g,1).(1,h).x = g.(h.x)$$

for all $g \in G$, $h \in H$, $x \in X$.

The above constructions are inverse to each other. This shows that commuting actions of G and H on X are "the same" as an action of $G \times H$ on X.

2. Representations of Groups

Definition 2.1. Let G be a group, V a k-vector space and $\pi\colon G \times V \to V$ a group action. The action π is *(k-)linear* if for every $g \in G$ the map $\pi_g\colon V \to V$, $v \mapsto g.v$ is (k-)linear. A *G-space*, or *representation of* G is a vector space V together with a linear action of G on V.

Example 2.2. The natural action of $\mathrm{GL}(2,\mathbb{R})$ on $\mathbb{R}^2$ from Example 1.33 is $\mathbb{R}$-linear.

Notation 2.3. For any k-vector space V we set

$$\mathrm{GL}(V) \coloneqq \{f\colon V \to V \mid f \text{ is } k\text{-linear and invertible}\}\,.$$

Lemma 2.4. Let G be a group and V a k-vector space. Then the 1:1-correspondence

$$\{G\text{-actions on } X\} \xleftrightarrow{1:1} \{\text{group homomorphisms } G \to S(V)\} \,.$$

from Lemma 1.6 restrict to a 1:1-correspondence

$$\{\text{linear } G\text{-actions on } X\} \xleftrightarrow{1:1} \{\text{group homomorphisms } G \to \mathrm{GL}(V)\} \,.$$

Remark 2.5. By Lemma 2.4, a representation of G can be equivalently characterized as a group homomorphism $\rho\colon G \to \mathrm{GL}(V)$ for a vector space V.

Example 2.6. Let G be a group and k a field.

a) Let V be a k-vector space. Then $\mathrm{GL}(V)$ acts linearly on V via

$$\varphi.v \coloneqq \varphi(v)$$

for all $\varphi \in \mathrm{GL}(V)$, $v \in V$. Note that this action corresponds to the identity homomorphism $\mathrm{id}_{\mathrm{GL}(V)}\colon \mathrm{GL}(V) \to \mathrm{GL}(V)$.

b) If V is any k-vector space, then the trivial action of G on V is k-linear, and corresponds to the trivial group homomorphism $G \to \mathrm{GL}(V)$. This actions defined the *trivial representation* of G on V. For each fixed dimension there is (up to isomorphism) one trivial representation, which is the referred to as *the* trivial representation (of dimension $\dim V$).

c) The symmetric group S_n acts linearly on k^n such that

$$\sigma.e_i = e_{\sigma(i)}$$

for all $\sigma \in S_n$, $i = 1, \dots, n$, where $e_1, \dots, e_n$ denotes the standard basis of k^n. This action can also be written as

$$\sigma.(a_1, \dots, a_n) = (a_{\sigma^{-1}(1)}, \dots, a_{\sigma^{-1}(n)})$$

for all $\sigma \in S_n$, $(a_1, \dots, a_n) \in k^n$.

d) Suppose that more generally a group G acts on a set X and that V is a vector space. Then G acts linearly on $V^X = \prod_{x \in X} V$ via

$$g.(v_x)_{x \in X} = (v_{g^{-1}.x})_{x \in X}$$

for all $g \in G$, $(v_x)_{x \in X} \in V^X$. For the permutation action of $G = S_n$ on $X = \{1, \dots, n\}$ and $V = k$ we get the above permutation action of S_n on k^n.

This example can not only be understood as a generalization, but also as a special case of the previous example: The symmetry group $S(X)$ acts on V^X by

$$\sigma.(v_x)_{x \in X} = (v_{\sigma^{-1}(x)})_{x \in X}$$

for all $\sigma \in S(X)$, $(v_x)_{x \in X} \in S(X)$, and this linear action corresponds to a group homomorphism $\rho\colon S(X) \to \mathrm{GL}(V^X)$. The action of G on G corresponds to a group homomorphism $\varphi\colon G \to \mathrm{GL}(V^X)$ given by $\varphi(g)(x) = g.x$ for all $g \in G$, $x \in X$. The composition $\rho \circ \varphi\colon S(X) \to \mathrm{GL}(V^X)$ is again a group homomorphism, and the corresponding linear action of G on V^X is the one described above.

e) Let X be a G-set and let V be the free vector space on X, i.e. V has a basis $(e_x)_{x \in X}$. Then the action of G on X extends to a linear action of G on V via

$$g.e_x = e_{g.x}$$

for all $g \in G$, $x \in X$. This representation is the *permutation representation associated to X*.

f) For every k-vector space V the symmetric group S_n also acts linearly on $V^{\otimes n}$ via

$$\sigma.(v_1 \otimes \cdots \otimes v_n) = v_{\sigma^{-1}(1)} \otimes \cdots \otimes v_{\sigma^{-1}(n)}$$

for all $\sigma \in S_n$, $v_1, \dots, v_n \in V$.

g) The group S_n acts linearly on the polynomial ring $k[X_1, \dots, X_n]$ via

$$\sigma.p(X_1, \dots, X_n) = p(X_{\sigma(1)}, \dots, X_{\sigma(n)}) \,.$$

(Note that this is also an action by ring automorphisms, and therefore altogether an action by k-algebra automorphisms.)

h) The symmetric group S_n acts linearly on k such that $\sigma \in S_n$ acts by multiplication with $\operatorname{sgn} \sigma \in \{1, -1\}$. This defines the *sign representation* of S_n.

For $n \geq 2$ this is the only non-trivial one-dimensional representation of S_n: Note that every one-dimensional representation V of S_n corresponds to a group homomorphism $S_n \to \mathrm{GL}(V) \cong \mathrm{GL}_1(k)$, which is abelian. This homomorphism factors through the abelianization $S_n/[S_n, S_n] = S_n/A_n \cong \mathbb{Z}/2$; it is therefore the trivial homomorphism or the sign homomorphism.

i) If X is a G-set then G acts linearly on the vector space kX via

$$g. \left(\sum_{x \in X} a_x \chi_x \right) = \sum_{x \in X} a_x \chi_{g.x}$$

where almost all a_x are zero. This agrees with the previous action $*$ on kX, because

$$(g * \chi_x)(y) = \chi_x(g^{-1}.y) = \delta_{x, g^{-1}.y} = \delta_{g.x, y} = \chi_{g.x}(y) = (g.\chi_x)(y)$$

for all $g \in G$, $x, y \in X$.

j) Let V and W be representations of G over k. Then the induced G-action on $\mathrm{Maps}(V, W)$ induces a linear action of G on $\mathrm{Hom}(V, W)$:

For every $g \in G$ the maps $\pi_g \colon V \to V$, $v \mapsto g.v$ and $\tau_g \colon W \to W$, $w \mapsto g.w$ are linear because G acts linearly on both V and W. It follows for every $g \in G$ and $f \in \mathrm{Hom}(V, W)$ that

$$g.f = \tau_g \circ f \circ \pi_{g^{-1}} \in \mathrm{Hom}(V, W) \,.$$

Hence $\mathrm{Hom}(V, W)$ is closed under the action of G on $\mathrm{Maps}(V, W)$, so that G acts on $\mathrm{Hom}(V, W)$ by restriction. The map $\tau_g \circ (-) \circ \pi_{g^{-1}} \colon \mathrm{Hom}(V, W) \to \mathrm{Hom}(V, W)$ is linear for every $g \in G$, so that this action is linear.

k) The previous example has an important special case: Let V be a representation of G over k. By letting G act trivially on k it follows that G acts linearly on $V^* = \operatorname{Hom}(V, k)$ in such a way that

$$(g.\varphi)(v) = \varphi(g^{-1}.v)$$

for all $\varphi \in V^*$, $v \in V$. Note that this is the unique G-action on V^* such that

$$(g.\varphi)(g.v) = \varphi(v)$$

for all $g \in G$, $v \in V$, i.e. such the actions on V^* and V are compatible with the canonical bilinear form

$$\langle -, - \rangle \colon V^* \times V \to k\,, \quad (\varphi, v) \mapsto \varphi(v)\,.$$

l) If V and W be representations of G over the same field, then G acts linearly on $V \oplus W$ and $V \otimes W$ via

$$g.(v, w) \coloneqq (g.v, g.w)\,, \tag{1}$$
$$g.(v \otimes w) \coloneqq (g.v) \otimes (g.w) \tag{2}$$

for all $v \in V$, $w \in W$, $g \in G$. If the linear actions of G on V, W are denoted by

$$\pi \colon G \times V \to V \quad \text{and} \quad \tau \colon G \times W \to W\,,$$

then the induced actions

$$\pi \oplus \tau \colon G \times (V \oplus W) \to V \oplus W\,,$$
$$\pi \otimes \tau \colon G \times (V \otimes W) \to V \otimes W$$

are given by

$$(\pi \oplus \tau)_g = \pi_g \oplus \tau_g \quad \text{and} \quad (\pi \otimes \tau)_g = \pi_g \otimes \tau_g$$

for every $g \in G$. If $v_1, \dots, v_n$ is a basis of V with respect to which π_g is given by a matrix A, and $w_1, \dots, w_m$ a basis of W with respect to which τ_g is given by a matrix B, then $(\pi \oplus \tau)_g$ and $(\pi \otimes \tau)_g$ are therefore given by the matrices

$$\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1m}B \\ a_{21}B & a_{22}B & \cdots & a_{2m}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}B & a_{n2}B & \cdots & a_{nm}B \end{bmatrix}$$

with respect to the basis $(v_1, 0), \dots, (v_n, 0), (0, w_1), \dots, (0, w_m)$ of $V \oplus W$ and the basis $v_1 \otimes w_1, v_1 \otimes w_2, \dots, v_n \otimes w_m$ of $V \otimes W$.

m) Let V be a representation of G and $\pi\colon G \times V \to V$ the corresponding linear action. Then for every $d \geq 0$ the group G acts linearly on the exterior power $\bigwedge^d V$ and symmetric power $S^d V$ via

$$\begin{aligned} g.(v_1 \wedge \cdots \wedge v_d) &\coloneqq (g.v_1) \wedge \cdots \wedge (g.v_d)\,, \\ g.(v_1 \cdots v_d) &\coloneqq (g.v_m) \cdots (g.v_d)\,. \end{aligned}$$

for all $g \in G$, $v_1, \dots, v_d$. If the corresponding linear actions are denoted by

$$\bigwedge^d \pi\colon G \times \bigwedge^d V \to \bigwedge^d V \quad \text{and} \quad S^d(\pi)\colon G \times S^d(V) \to S^d(V)\,,$$

then

$$\left(\bigwedge^d \pi\right)_g = \bigwedge \pi_g \quad \text{and} \quad S^d(\pi)_g = S^d(\pi_g)$$

for every $g \in G$.

Definition 2.7. Let V be a representation of G.

- A *subrepresentation* of V is a vector subspace $U \subseteq V$ such that $g.u \in U$ for all $g \in G$, $u \in U$. A subrepresentation $U \subseteq V$ is *proper* if $U \neq V$.
- The representation V is *indecomposable* if it it nonzero and can't be written as $V = U_1 \oplus U_2$ where U_1, U_2 are proper subrepresentations of V.
- The representation V is *irreducible* or *simple* if it is nonzero has no nontrivial proper subrepresentation, i.e. no subrepresentation $U \subseteq V$ with $0 \subsetneq U \subsetneq V$.

Example 2.8. Let G be a group and k a field.

a) Let V be a vector space and let G act trivially on V. Then every linear subspace $U \subseteq V$ is a subrepresentation. The representation V is indecomposable if and only if it is one-dimensional. It is also irreducible if and only if it is one-dimensional.

b) Let V be a representation of G. If $(U_i)_{i \in I}$ is any familiy of subrepresentations, then both $\sum_{i \in I} U_i$ and $\bigcap_{i \in I} U_i$ are again subrepresentations of V.

c) Every finite-dimensional representation can be written as a direct sum of indecomposable subrepresentations.

d) Let V be a representation of G over k. For every subset $E \subseteq V$ there exists a smallest subrepresentation of V containing E. This subrepresentation $\langle E \rangle_G \subseteq V$ can be described in the following equivalent ways:

   1) One has that $E \subseteq \langle E \rangle_G$, and for every subrepresentation $U \subseteq V$ with $E \subseteq U$ one has that $\langle E \rangle_G \subseteq U$.

2) The subrepresentation $\langle E \rangle_G$ is given by

$$\langle E \rangle_G = \bigcap_{\substack{\text{subrep. } U \subseteq V \\ E \subseteq U}} U \,.$$

3) The subrepresentation $\langle E \rangle_G$ is given by

$$\langle E \rangle_G = \left\{ \sum_{i=1}^{n} \lambda_i g_i.e_i \,\middle|\, n \geq 0, \lambda_i \in k, g_i \in G, e_i \in E \right\} = \langle g.e \,|\, g \in G, e \in E \rangle_k \,.$$

e) A non-zero representation V of G is irreducible if and only if every non-zero $v \in V$ generates the representation V:

Suppose that V is irreducible and let $v \in V$ be non-zero. Then $\langle v \rangle_G$ is a non-zero subrepresentation of V, so that $\langle v \rangle_G = V$ by irreducibility.

Suppose that V is reducible. Then there exists an non-zero, proper subrepresentation $0 \subsetneq U \subsetneq V$. Then there exists some non-zero $v \in U$, for which it follows that $\langle v \rangle \subseteq U \subsetneq V$, so that v does not generate V.

f) The group $G \coloneqq \mathbb{Z}/n$, $n \geq 1$ acts on the plane $V \coloneqq \mathbb{R}^2$ by rotation, i.e.

$$\overline{n}.\begin{bmatrix} x \\ y \end{bmatrix} \coloneqq \begin{bmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} .$$

Then V is irreducible if and only if $n \geq 3$:

For $n = 1$ the action is trivial, but V is two-dimensional, and therefore reducible. For $n = 2$ every element $g \in G$ acts by multiplication with a scalar, so that every one-dimensional subspace is a non-zero proper subrepresentation.

If $n \geq 3$ then for every non-zero vector $v \in V$ the two vectors $v, \overline{1}.v$ are linearly independent. Thus V is spanned by $\{v, \overline{1}.v\}$ as a $\mathbb{R}$-vector space and therefore also as a representation. This shows that every non-zero $v \in V$ generates the representation V, so that V is irreducible.

g) Let the symmetric group S_n act linearly on the polynomial ring $k[X_1, \dots, X_n]$ via

$$\sigma.p(X_1, \dots, X_n) = p(X_{\sigma(1)}, \dots, X_{\sigma(n)})$$

for all $\sigma \in S_n$, $p(X_1, \dots, X_n) \in k[X_1, \dots, X_n]$. For every degree $d \geq 0$ let

$$k[X_1, \dots, X_n]_d \coloneqq \left\langle X_1^{d_1} \cdots X_n^{d_n} \,\middle|\, d_1 + \cdots + d_n = d \right\rangle_k \,.$$

Then $k[X_1, \dots, X_n]_d$ is a subrepresentation of $k[X_1, \dots, X_n]$ because the action of S_n on the monomials preserves the degree. Hence

$$k[X_1, \dots, X_n] = \bigoplus_{d \geq 0} k[X_1, \dots, X_n]_d$$

is a decomposition into finite-dimensional subrepresentations.

h) If V is a representation of G and $U \subseteq V$ is a subrepresentation, then the quotient V/U is again a representation of G via

$$g.\overline{v} = \overline{g.v}$$

for all $g \in G$, $v \in V$. To see that this action is well-defined note for the given linear action $\pi\colon G \times V \to V$ we have for every $g \in G$ that $\pi_g\colon V \to V$ with $\pi_g(U) \subseteq U$. It thus follows from linear algebra that π_g descends to a well-defined linear map

$$\overline{\pi_g}\colon V/U \to V/U\,, \quad \overline{v} \mapsto \overline{\pi_g(v)} = \overline{g.v}$$

2.9. Every irreducible representation is also indecomposable, but as the following example shows, the converse is not true:

Example 2.10. Let

$$G := \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \,\middle|\, a, b, c \in \mathbb{C} \text{ and } a, c \neq 0 \right\}.$$

be the group of upper, triangular, complex (2×2)-matrices. The group G acts on the vector space $V := \mathbb{C}^2$ in the natural way, i.e. via left multiplication.

The representation V is not irreducible because $U := \operatorname{span}(e_1)$ is a subrepresentation.

Claim. The subrepresentation $U \subseteq V$ is the unique 1-dimensional subrepresentation.

From this claim it follows that there exists no proper subrepresentations U_1, U_2 of V with $V = U_1 \oplus U_2$, so that V is indecomposable.

Proof of the claim. Let W be any one-dimensional subrepresentation of V. Then

$$W = \operatorname{span}\left\{ \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \right\} \quad \text{for some } 0 \neq \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \in \mathbb{C}^2 .$$

Because W is a subrepresentation of V it follows that

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha + \beta \\ \beta \end{bmatrix} \in W .$$

and therefore that

$$\begin{bmatrix} \beta \\ 0 \end{bmatrix} \in W .$$

If $\beta \neq 0$ then it follows that

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \in W ,$$

and if $\beta = 0$ then the same follows from $\alpha \neq 0$. Because W is one-dimensional it follows that

$$W = \operatorname{span}\left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right\} = U .$$

This proves the claim. □

Warning 2.11. Example 2.10 also show that subrepresentations do not necessarily have direct complements which are again subrepresentations.

Lemma 2.12. If G is a finite groups then every irreducible representation of G is finite-dimensional.

Proof. If V is an irreducible representation then V is nonzero so there exists some nonzero $v \in V$. Then $\langle g.v \mid g \in G \rangle_k$ is a nonzero subrepresentation of V and it follows that $V = \langle g.v \mid g \in G \rangle_k$ from the irreducibility of V. □

Lemma 2.13. Let G be a group.

a) Given a representation V of G, the subset $V^G \subseteq V$ is a subrepresentation of V.

b) For every collection V_i, $i \in I$ of representations of G one has that

$$\left(\bigoplus_{i \in I} V_i \right)^G = \bigoplus_{i \in I} V_i^G \,.$$

Proof.

a) Since G acts trivially on V^G it sufficies to check that V^G is a vector subspace of V. This holds because $\pi_g \colon V \to V$, $v \mapsto g.v$ is linear for every $g \in G$ and

$$V^G = \bigcap_{g \in G} \ker(\pi_g - \mathrm{id}_V) \,.$$

b) Let $v \in \bigoplus_{i \in I} V_i$. Then $v = (v_i)_{i \in I}$ with $v_i = 0$ for all but finitely many $i \in I$. For every $g \in G$ one has that

$$g.v = g.(v_i)_{i \in I} = (g.v_i)_{i \in I}$$

and therefore

$$\begin{aligned} v \in \left(\bigoplus_{i \in I} V_i \right)^G &\iff g.v = v \text{ for every } g \in G \\ &\iff (g.v_i)_{i \in I} = (v_i)_{i \in I} \text{ for every } g \in G \\ &\iff g.v_i = v_i \text{ for all } g \in G,\ i \in I \\ &\iff v_i \in V_i^G \text{ for every } i \in I \iff v \in \bigoplus_{i \in I} V_i^G \,. \end{aligned}$$

This shows the claimed equality. □

Remark 2.14. Given representations V, W of a group G we have that

$$V^G \otimes W^G \subseteq (V \otimes W)^G$$

because for all simple tensors $v \otimes w \in V^G \otimes W^G$ with $v \in V^G$, $w \in W^G$ we have that

$$g.(v \otimes w) = (g.v) \otimes (g.w) = v \otimes w$$

and thus $v \otimes w \in (V \otimes W)^G$.

But the other inclusion does not necessarily hold: Consider for example the action of $G = S_2 = \{1, s\}$ on $V = W = k^2$ given by swapping the coordinates, i.e.

$$s.(x_1, x_2) = (x_2, x_1)$$

for every $(x_1, x_2) \in k^2$. Then $V^G = W^G = \langle e_1 + e_2 \rangle_k$ and thus

$$\begin{aligned} V^G \otimes W^G &= \langle e_1 + e_2 \rangle_k \otimes \langle e_1 + e_2 \rangle_k \\ &= \langle (e_1 + e_2) \otimes (e_1 + e_2) \rangle_k \\ &= \langle e_1 \otimes e_1 + e_1 \otimes e_2 + e_2 \otimes e_1 + e_2 \otimes e_2 \rangle_k \,. \end{aligned}$$

Then $e_1 \otimes e_2 + e_2 \otimes e_1 \in (V \otimes W)^G$ is not contained in $V^G \otimes W^G$.

We can look at the case $G = S_2 = \{1, s\}$ with $\operatorname{char}(k) \neq 2$ in a bit more detail: Then the linear map

$$f \colon V \to V, \quad v \mapsto s.v$$

satisfies $f^2 = \mathrm{id}_V$ and thus satisfies the polynomial $X^2 - 1 = (X-1)(X+1) \in k[X]$. It follows from $\operatorname{char}(k) \neq 2$ that this polynomial decomposes into pairwise different linear factors, and therefore that f is diagonalizable with possible eigenvalues $1, -1$. We therefore have that

$$V = V_+ \oplus V_-$$

where s acts on V_+, V_- by their respective sign changes. This is in particular a decomposition into subrepresentations with

$$V^G = (V_+ \oplus V_-)^G = V_+^G \oplus V_-^G = V_+ \,.$$

We similary have that $W = W_+ \oplus W_-$ with $W^G = W_+$.

We then have that

$$\begin{aligned} V \otimes W &= (V_+ \oplus V_-) \otimes (W_+ \oplus W_-) \\ &= (V_+ \otimes W_+) \oplus (V_- \otimes W_-) \oplus (V_+ \otimes W_-) \oplus (V_- \otimes W_+) \end{aligned}$$

where s acts trivially on the summands $V_+ \otimes W_+$ and $V_- \otimes W_-$ and by a sign change on the summands $V_+ \otimes W_-$ and $V_- \otimes W_+$. It thus follows that

$$\begin{aligned} (V \otimes W)^G &= ((V_+ \otimes W_+) \oplus (V_- \otimes W_-) \oplus (V_+ \otimes W_-) \oplus (V_- \otimes W_+))^G \\ &= (V_+ \otimes W_+)^G \oplus (V_- \otimes W_-)^G \oplus (V_+ \otimes W_-)^G \oplus (V_- \otimes W_+)^G \\ &= (V_+ \otimes W_+) \oplus (V_- \otimes W_-) \,. \end{aligned}$$

We that that compared to $V^G \otimes W^G = V_+ \otimes W_+$ we gain the additional summand $V_- \otimes W_-$, which is invariant because the actions of s on the factors cancels out.

In the previous example we have for $\operatorname{char}(k) \neq 2$ that

$$V_+ = W_+ = \langle e_1 + e_2 \rangle_k \,, \qquad V_- = W_- = \langle e_1 - e_2 \rangle_k \,.$$

By the above discussion we find that

$$\begin{aligned}
&(V \otimes W)^G = (V_+ \otimes W_+) \oplus (V_- \otimes W_-) \\
&= (\langle e_1 + e_2 \rangle_k \otimes \langle e_1 + e_2 \rangle_k) \oplus (\langle e_1 - e_2 \rangle_k \otimes \langle e_1 - e_2 \rangle_k) \\
&= \langle e_1 \otimes e_1 + e_1 \otimes e_2 + e_2 \otimes e_1 + e_2 \otimes e_2 \rangle_k \oplus \langle e_1 \otimes e_1 - e_1 \otimes e_2 - e_2 \otimes e_1 + e_2 \otimes e_2 \rangle_k \\
&= \langle e_1 \otimes e_1 + e_1 \otimes e_2 + e_2 \otimes e_1 + e_2 \otimes e_2, e_1 \otimes e_1 - e_1 \otimes e_2 - e_2 \otimes e_1 + e_2 \otimes e_2 \rangle \\
&= \langle e_1 \otimes e_1 + e_2 \otimes e_2, e_1 \otimes e_2 + e_2 \otimes e_1 \rangle \,.
\end{aligned}$$

3. Group Algebras

Definition 3.1. Let k be a field (or a ring) and G a group. Then the *group algebra of G over k* is the k-algebra given by the k-vector space

$$k[G] \coloneqq \{ f \colon G \to k \mid f(g) \neq 0 \text{ for only finitely many } g \in G \}$$

with pointwise addition and scalar multiplication, and multiplication given by convolution, i.e.

$$(f_1 \cdot f_2)(x) = \sum_{y \in G} f_1(y) f_2 \left(y^{-1} x \right) \tag{3.1}$$

for all $f_1, f_2 \in k[G]$, $x \in G$. The unit of the group algebra is given by the function χ_e.

3.2. To make it easier to work with the group algebra $k[G]$ we provide another way to think about it:

Every function $f \in k[G]$ can be written as a linear combination $f = \sum_{g \in G} a_g \chi_g$ with $a_g \in k$ for every $g \in G$ (namely $a_g = f(g)$), where almost all of the coefficients a_g are zero. Because the functions χ_g, $g \in G$ form a basis of $k[G]$, the linear combination $\sum_{g \in G} a_g \chi_g$ can be identified with the formular linear combination $\sum_{g \in G} a_g g$. Note that $g \in G$ is then identified with $\chi_g \in k[G]$, so that G becomes a k-basis of $k[G]$.

The addition and scalar multiplication of $k[G]$ are then given by

$$\left(\sum_{g \in G} a_g g \right) + \left(\sum_{g \in G} b_g g \right) = \sum_{g \in G} (a_g + b_g) g \,, \qquad \lambda \left(\sum_{g \in G} a_g g \right) = \sum_{g \in G} (\lambda a_g) g$$

for every $\lambda \in k$, and the multiplication of $k[G]$ is then given by

$$\left(\sum_{g \in G} a_g g \right) \cdot \left(\sum_{g \in G} b_g g \right) = \sum_{g, g' \in G} a_g b_{g'} (g g') \,. \tag{3.2}$$

To see that (3.2) defines the same multiplication as (3.1) note that

$$(\chi_{g_1} \cdot \chi_{g_2})(h) = \sum_{g \in G} \chi_{g_1}(g)\chi_{g_2}\left(g^{-1}h\right) = \chi_{g_2}\left(g_1^{-1}h\right) = \delta_{g_2, g_1^{-1}h} = \delta_{g_1 g_2, h} = \chi_{g_1 g_2}(h)\,,$$

for every $h \in G$, so that

$$\chi_{g_1} \cdot \chi_{g_2} = \chi_{g_1 g_2}$$

for all $g_1, g_2 \in G$. This shows that the multiplications (3.1) and (3.2) agree on the k-basis $(\chi_g)_{g \in G}$, resp. $(g)_{g \in G}$ of $k[G]$, and thus on the whole of $k[G]$ by the k-bilinearity of both (3.1) and (3.2).

Altogether this shows that we can think of the group algebra $k[G]$ as a linearization of the group G: The group G is a k-basis of $k[G]$, the multiplication of $k[G]$ is the (unique) k-bilinear extension of the multiplication of G, and $e = 1_{k[G]}$ for the neutral element $e \in G$. Note also that $k[G]$ is commutative if and only if G is abelian.

3.3. If V is a representation of a group G over a field k, then the corresponding group homomorphismus $\rho\colon G \to \mathrm{GL}(V)$ can be regarded as a map $G \to \mathrm{End}(V)$, which then extends (uniquely) to a k-linear map

$$R\colon k[G] \to \mathrm{End}(V)\,, \quad \sum_{g \in G} a_g g \mapsto \sum_{g \in G} a_g \rho(g)\,.$$

The k-linear map R is multiplicative on the basis $G \subseteq k[G]$ because $R|_G = \rho$, and is therefore a homomorphisms of k-algebras. This homomorphisms corresponds to a $k[G]$-module structure on V given by

$$x \cdot v \coloneqq R(x)(v) = R\left(\sum_{g \in G} a_g g\right)(v) = \sum_{g \in G} a_g \rho(g)(v) = \sum_{g \in G} a_g (g.v)$$

for all $x = \sum_{g \in G} a_g g \in k[G]$, $v \in V$.

If on the other hand V is a $k[G]$-module, then the corresponding homomorphism of k-algebras

$$T\colon k[G] \to \mathrm{End}(V), \quad a \mapsto (v \mapsto a \cdot v)$$

maps every group element $g \in G$ to linear map $T(g)\colon V \to V$ in a multiplicative way. Note that the linear map $T(g)$ is necessarily bijective because

$$T(g)T(g^{-1}) = T(gg^{-1}) = T(e) = T(1_{K[G]}) = \mathrm{id}_V\ .$$

Hence T restrict to a group homomorphism $\tau \coloneqq T|_G\colon G \to \mathrm{GL}(V)$, which makes V into a representation of G given via

$$g.v \coloneqq \tau(g)(v) = T(g)(v) = g \cdot v$$

for all $g \in G$, $v \in V$.

The above constructions are inverse to each other, and thus lead to the following result:

Corollary 3.4. Let G be a group and V a k-vector space. Then there exists a 1:1-correspondence

$$\begin{array}{ccc} \{k\text{-linear } G\text{-actions on } V\} & \overset{1:1}{\longleftrightarrow} & \{k[G]\text{-module structures on } V\}\,, \\ \pi & \longmapsto & P \end{array}$$

where for every linear action $\pi\colon G\times V \to V$, $(g,v)\mapsto g.v$ the corresponding $k[G]$-module structure is given by

$$P\colon k[G]\times V \to V\,, \quad \left(\sum_{g\in G} a_g g, v\right) \mapsto \sum_{g\in G} a_g (g.v)\,.$$

Definition 3.5. The group algebra $k[G]$ is a module over itself via left multiplication. This $k[G]$-module structure corresponds to the linear action of G on $k[G]$ via left multiplication on the basis vectors $h\in G$, i.e.

$$g.\left(\sum_{h\in G} a_h h\right) = \sum_{h\in G} a_h (gh)$$

for all $g\in G$, $\sum_{h\in G} a_h h \in k[G]$. This is the (*left*) *regular representation* of G.

Remark 3.6. Let V and W be representations of G over a field k. Then a map $f\colon V\to W$ is a homomorphism of $k[G]$-modules with respect to the corresponding $k[G]$-module structures on V and W if and only if f is a morphism of representations:

If f is a homomorphism of $k[G]$-modules, then it is in particular k-linear map. For every $g\in G$ we have that

$$f(g.v) = f(g\cdot v) = g\cdot f(v) = g.f(v)$$

for every $v\in V$, so that f is G-equivariant.

If f is a morphism of representations then it is also k-linear. For every algebra element $x=\sum_{g\in G} a_g g \in k[G]$ it then follows that

$$\begin{aligned} f(x\cdot v) &= f\left(\sum_{g\in G} a_g g\cdot v\right) = \sum_{g\in G} a_g f(g\cdot v) \\ &= \sum_{g\in G} a_g f(g.v) = \sum_{g\in G} a_g g.f(v) = \sum_{g\in G} a_g g\cdot f(v) = x\cdot f(v) \end{aligned}$$

for every $v\in V$, so that f is a homomorphism of $k[G]$-modules.

Altogether we have now constructed an isomorphism of category k-G-**Rep** of representations of G over k and the category $k[G]$-**Mod** of left $k[G]$-modules.

Remark 3.7. Given any ring R and monoid M the *monoid algebra* $R[M]$ is given by the set of all formal linear combination $\sum_{x \in M} r_x x$ (where $r_x = 0$ for all but finitely many $x \in M$) together with the addition

$$\left(\sum_{x \in M} r_x x \right) + \left(\sum_{x \in M} s_x x \right) = \sum_{x \in M} (r_x + s_x) x \,,$$

the scalar multiplication

$$r \cdot \left(\sum_{x \in M} r_x x \right) = \sum_{x \in M} (r r_x) x \,,$$

and the multiplication

$$\left(\sum_{x \in M} r_x x \right) \cdot \left(\sum_{x \in M} s_x x \right) = \sum_{x,y \in M} (r_x s_y)(xy) \,.$$

Then R can be regarded as a subring of $R[M]$ via the inclusion

$$R \hookrightarrow R[M], \quad r \mapsto r1_{R[M]} \,,$$

and M can be regarded as an R-basis of $R[M]$. The monoid algebra $R[M]$ has the following universal property:

Let S be any ring. Then every ring homomorphism $\Phi\colon R[M] \to S$ restrict to a ring homomorphism $\varphi\colon R \to S$ and to a monoid homomorphism $\psi\colon M \to (S, \cdot)$, while every pair (φ', ψ') consisting of a ring homomorphism $\varphi'\colon R \to S$ and monoid homomorphism $\psi'\colon M \to (S, \cdot)$ extend to a ring homomorphism $\Phi'\colon R[M] \to S$. These constructions are inverse to each other and thus lead to a 1:1-correspondence

$$\begin{aligned} &\{\text{ring homomorphism } \Phi\colon R[M] \to S\} \\ \overset{1:1}{\longleftrightarrow} &\left\{ (\varphi, \psi) \,\middle|\, \begin{array}{c} \text{ring homomorphisms } \varphi\colon R \to S, \\ \text{monoid homomorphisms } \psi\colon M \to (S, \cdot) \end{array} \right\} , \end{aligned}$$

given by the restriction(s) $\Phi \mapsto (\Phi|_R, \Phi|_M)$. (The necessary calculations are the same as in 3.3.)

If $M = G$ is a group then we retrieve the previous definition of the group algebra $R[G]$. Then the image of every monoid homomorphism $G \to (S, \cdot)$ is already contained in the unit group $S^\times$, and the universal property above becomes a 1:1-correspondence

$$\begin{aligned} &\{\text{ring homomorphism } \Phi\colon R[G] \to S\} \\ \overset{1:1}{\longleftrightarrow} &\left\{ (\varphi, \psi) \,\middle|\, \begin{array}{c} \text{ring homomorphisms } \varphi\colon R \to S, \\ \text{group homomorphisms } \psi\colon M \to S^\times \end{array} \right\} . \end{aligned}$$

One can then retrieve Corollary 3.4 from the universal property of the group algebra: Suppose that $R = k$ is a field, $M = G$ is a group, V is a k-vector space and $S = \operatorname{End}(V)$.

Then by letting $\varphi\colon k \to \mathrm{End}(V)$ be the canonical inclusion $\lambda \mapsto \lambda \cdot 1_V$, we get a 1:1-correspondence

$$\begin{aligned}&\{k\text{-algebra homomorphims } R\colon k[G] \to \mathrm{End}(V)\}\\ \overset{1:1}{\longleftrightarrow}\, &\{\text{group homomorphisms } \rho\colon G \to \mathrm{End}(V)^\times = \mathrm{GL}(V)\}\,,\end{aligned}$$

which is given by restriction $R \mapsto R|_G$.

Remark 3.8. Let k be a commutative ring and let k-**Alg** be the category of k-algebras. Let **Mon** be the category of monoids.

There exists a forgetful functor $U\colon k\text{-}\mathbf{Alg} \to \mathbf{Mon}$ which assigns to each k-algebra S its underlying multiplicative monoid $U(S) = (S, \cdot)$, and which regards every k-algebra homomorphism $f\colon S \to T$ as a monoid homomorphism (i.e. multipicative map) $f\colon (S,\cdot) \to (T,\cdot)$.

Note that every homomorphism of monoids $f\colon M \to N$ induces a homomorphism of k-algebras

$$f_*\colon k[M] \to k[N]\,, \quad \sum_{x\in M} a_x x \mapsto \sum_{x \in M} a_x f(x)\,,$$

in such a way that $(\mathrm{id}_M)_* = \mathrm{id}_{k[M]}$ and $(g \circ f)_* = g_* \circ f_*$. The monoid algebra over k can therefore be regarded as a functor $k[-]\colon \mathbf{Mon} \to k\text{-}\mathbf{Alg}$.

The universal property of the monoid algebra then states that the functor $k[-]$ is left-adjoint to the forgetful functor U. This also holds true if k is replaced by an arbitrary (not necessarily commutative) ring R, if one does not require R-algebras to be central.

4. Morphism of Representations & Schur's Lemma

Definition 4.1. Let G be a group, k a field and let V, W be representations of G.

- A map $f\colon V \to W$ is called a *morphism of representations of* G or *morphism of* G*-spaces* if it is both k-linear and G-equivariant. The space of morphisms of representations $V \to W$ is denoted by

$$\mathrm{Hom}_G(V, W) \coloneqq \{f\colon V \to W \mid f \text{ is a morphism of representations}\}\,.$$

- An *isomorphism of representations* is an morphism of representations which is also invertible, i.e. bijective.
- Two representations V and W are *isomorphic*, denoted by $V \cong W$, if there exists an isomorphism of representations between V and W.

Remark 4.2. If $f\colon V \to W$ is an isomorphism of representations, then its inverse f^{-1} is again a morphism of representations: It is know from linear algebra that f^{-1} is again linear. It is G-equivariant, because

$$f^{-1}(g.v) = f^{-1}\left(g.f\left(f^{-1}(v)\right)\right) = f^{-1}\left(f\left(g.f^{-1}(v)\right)\right) = g.f^{-1}(v)$$

for all $g \in G$, $v \in V$.

Example 4.3. Let G be a group and k a field.

a) If V_1, V_2, W are representations of G, then the linear isomorphism

$$\alpha\colon (V_1 \oplus V_2) \otimes W \to V_1 \times W \oplus V_2 \otimes W\,, \quad (v_1, v_2) \otimes w \mapsto (v_1 \otimes w, v_2 \otimes w)$$

is an isomorphism of representations because

$$\begin{aligned}\alpha(g.((v_1, v_2) \otimes w)) &= \alpha((g.(v_1, v_2)) \otimes (g.w)) = \alpha((g.v_1, g.v_2) \otimes (g.w)) \\ &= ((g.v_1) \otimes (g.w), (g.v_2) \otimes (g.w)) = (g.(v_1 \otimes w), g.(v_2 \otimes w)) \\ &= g.(v_1 \otimes w, v_2 \otimes w) = g.\alpha((v_1, v_2) \otimes w)\,.\end{aligned}$$

b) If V, W are finite-dimensional representations of G, then the linear isomorphism

$$\beta\colon V^* \otimes W \to \mathrm{Hom}(V, W)\,, \quad \varphi \otimes w \mapsto (v \mapsto \varphi(v)w)$$

is an isomorphism of representations because

$$\begin{aligned}\beta(g.(\varphi \otimes w))(v) &= \beta((g.\varphi) \otimes (g.w))(v) = (g.\varphi)(v)(g.w) = \varphi(g^{-1}.v) \cdot (g.w) \\ &= g.\bigl(\varphi(g^{-1}.v)w\bigr) = g.\bigl(\beta(\varphi \otimes w)(g^{-1}.v)\bigr) = (g.\beta(\varphi \otimes w))(v)\,,\end{aligned}$$

where we used for the fourth equality that $g \in G$ acts linearly on W.

c) If V is a representation of G over k, then the evaluation homomorphism

$$\alpha\colon V^* \otimes V \to k\,, \quad \varphi \times v \mapsto \varphi(v)$$

is a morphism of representations when we regard k as the trivial representation. This holds because

$$\begin{aligned}\alpha(g.(\varphi \otimes v)) &= \alpha((g.\varphi) \otimes (g.v)) = (g.\varphi)(g.v) \\ &= \varphi(g^{-1}.g.v) = \varphi(v) = g.\varphi(v) = g.\alpha(\varphi \otimes v)\,.\end{aligned}$$

Note that the linear action of G on V is defined precisely so that α is a morphism of representations.

d) Let V be a representation of G over k and regard k as the trivial representation. Then for every $v \in V$ the homomorphism

$$k \to V\,, \quad \lambda \mapsto \lambda v$$

is a morphism of representations if and only if $g.(\lambda v) = \lambda v$ for every $\lambda \in K$, i.e. if and only if v is G-invariant (as can be seen by considering $\lambda = 1$). Thus we have an isomorphism of vector spaces (which is also an isomorphism of trivial representations)

$$\mathrm{Hom}_G(k, V) \to V^G\,, \quad e \mapsto e(1)\,.$$

Remark 4.4. If V, W are two representations of G over the same field, then by the restricting the equality from Lemma 1.17 to the subset of k-linear maps on both sides, it follows that

$$\mathrm{Hom}_G(V,W) = \mathrm{Hom}(V,W)^G\,.$$

It follows in particular that $\mathrm{Hom}_G(V,W)$ is a k-vector space via pointwise addition und scalar multiplication.

Lemma 4.5. Let G be a group and let U, V, W, be representations of G.

a) The identity $\mathrm{id}_V\colon V \to V$ is a morphism of representations.

b) If $f\colon U \to V$, $g\colon V \to W$ are morphism of representations, then $g \circ f\colon U \to W$ is also a morphism of representations.

4.6. Lemma 4.5 shows that for any group G and field k the class of representations of G over k together with the morphisms of representations between them form a category, which we will denote by k-G-**Rep**. As before there exists a functor from k-G-**Rep** to k-G-**Rep** which maps every representations V to its invariants V^G and every morphism of representations $f\colon V \to W$ to the restriction $f^G\colon V^G \to W^G$.

Lemma 4.7. Let V, W be representations of a group G, and let $f\colon V \to W$ be a morphism of representations. Then $\ker f$ is a subrepresentation of V and $\operatorname{im} f$ is a subrepresentation of W.

Proof. It is known from linear algebra that $\ker f$ is a vector subspace of V, and that $\operatorname{im} f$ is a vector subspace of W.

Let $x \in \ker f$. Then $f(g.x) = g.f(x) = g.0 = 0$ for every $g \in G$, because G acts linearly on V. This shows that $g.x \in \ker f$ for all $g \in G$, $x \in \ker f$, so that $\ker f$ is a subrepresentation.

Let $y \in \operatorname{im} f$ with $y = f(x)$ for some $x \in V$. Then $g.y = g.f(x) = f(g.x) \in \operatorname{im} f$ for every $g \in G$. This shows that $\operatorname{im} f$ is a subrepresentation. □

Proposition 4.8 (Schur's lemma)**.** Let V, W be representations of a group G over the same field k.

a) If V is irreducible then every nonzero morphism $V \to W$ is injective.

b) If W is irreducible then every nonzero morphism $V \to W$ is surjective.

Let V, W both be irreducible.

c) Every nonzero morphism $f\colon V \to W$ is an isomorphism.

d) If $V \ncong W$ then $\mathrm{Hom}_G(V,W) = 0$, and if $V \cong W$ then $\mathrm{Hom}_G(V,W) \neq 0$.

e) The endomorphism ring $\mathrm{End}_G(V) = \mathrm{Hom}_G(V,V)$ is a divison algebra over k.

f) If k is algebraically closed (e.g. $k = \mathbb{C}$) and both V and W are finite-dimensional then

$$\mathrm{Hom}_G(V,W) \cong \begin{cases} k & \text{if } V \cong W\,, \\ 0 & \text{if } V \ncong W\,. \end{cases}$$

Proof.

a) The kernel $\ker f$ is a proper subrepresentation of V, so that $\ker f = 0$.

b) The image $\operatorname{im} f$ is a non-zero subreprentation of W, so that $\operatorname{im} f = W$.

c) This follows from parts a), b)

d) By c) there exists a non-zero isomorphism $V \to W$ if and only if $V \cong W$.

e) This follows from c); that $0 \neq \mathrm{id}_V$ follows from $V \neq 0$.

f) For $V \ncong W$ this follows from c), so it sufficies to consider the case $V \cong W$. Every isomorphism $\alpha\colon W \to V$ induces an isomorphism of vector spaces

$$\alpha_*\colon \operatorname{Hom}_G(V, W) \to \operatorname{Hom}_G(V, V)\,, \quad f \mapsto \alpha \circ f\,.$$

We may therefore assume w.l.o.g. that $W = V$.

Then every morphism of representations $f\colon V \to V$ has an eigenvalues $\lambda \in k$, for which $f - \lambda\,\mathrm{id}_V\colon V \to V$ is a morphism of representations with $\ker(f - \lambda\,\mathrm{id}_V) \neq 0$. Because V is irreducible it follows that $f - \lambda\,\mathrm{id}_V = 0$, so that $f = \lambda\,\mathrm{id}_V$. □

Corollary 4.9. Let k be an algebraically closed field and let G be an abelian group. Then every irreducible finite-dimensional representation of G over k is one-dimensional.

Proof. Let V be such a representation. Because every two group elements $g, h \in G$ commute, it follows that the actions of g and h on V commute, so that the map $\pi_g\colon V \to V$, $v \mapsto g.v$ is G-equivariant for every group element $g \in G$. Hence $\pi_g \in \operatorname{End}_G(V)$ for every $g \in G$.

By Schur's Lemma we find that $\operatorname{End}_G(V) \cong k$, and so every group element $g \in G$ acts by multiplication with some scalar $\lambda \in k$. It follows that every k-linear subspace of V is a subrepresentation of V. Since V is irreducible we find that V is one-dimensional. □

Corollary 4.10. Let k be an algebraically closed field and let G be a finite abelian group. Then every irreducible representation of G over k is one-dimensional.

Proof. Every irreducible representation of G is one-dimensional by Lemma 2.12 so the claim follows from Corollary 4.9. □

Example 4.11. Let k be algebraically closed and consider the finite abelian group $\mathbb{Z}/n$. Then every irreducible representation of $\mathbb{Z}/n$ over k is one-dimensional. To classify these representations we therefore need to understand the group homomorphisms $\rho\colon \mathbb{Z}/n \to \mathrm{GL}_1(k) = k^\times$.

For the n-th roots of unity $\omega_1, \dots, \omega_n \in k^\times$ the map

$$\rho_i\colon \mathbb{Z}/n \to k^\times \quad \overline{m} \mapsto \omega_i^m\,.$$

is a group homomorphism. Every group homomorphisms $\rho\colon \mathbb{Z}/n \to k^\times$ is determined by the image $\rho(\overline{1})$, which needs to satisfy $\rho(\overline{1})^n = 1$, so it follows that ρ must be of the form $\rho = \rho_i$ for some i. It follows that the irreducible representations of $\mathbb{Z}/n$ are given by $V_1, \dots, V_n$, where V_i is one-dimensional and $\overline{m} \in \mathbb{Z}/n$ acts by multiplication with ω_i^m.

For $\omega_i \neq \omega_j$ the representations V_i and V_j are isomorphic if and only if $\omega_i = \omega_j$. The roots of unity $\omega_1, \dots, \omega_n$ are pairwise different if and only if the polynomial $X^n - 1 \in k[X]$ is separable, which holds if and only if $\operatorname{char}(k) \nmid n$.

a) It follows for $\operatorname{char}(k) = 0$ that $\mathbb{Z}/n$ has up to isomorphism precisely n pairwise different irreducible representations over k.

b) If $\operatorname{char}(k) = p$ and $n = p^r m$ with $p \nmid m$ then

$$X^n - 1 = X^{p^r m} - 1^{p^r} = (X^m - 1)^{p^r}$$

with the map $k \to k$, $x \mapsto x^{p^r}$ being bijective (because k is perfect as it is algebraically closed). It then follows that the n-th roots of unity are precisely the m-th roots of unity, so $\mathbb{Z}/n$ has precisely m pairwise non-isomorphic irreducible representations over k.

Remark 4.12. Let G be a group, k an algebraically closed field and $V_1, \dots, V_n$ pairwise non-isomorphic irreducible representations of G over k. Then

$$\dim \operatorname{Hom}_G(V_i, V_j) = \delta_{ij}$$

for all $i, j = 1, \dots, n$ by Schur's lemma. Hence the representations $V_1, \dots, V_n$ can be thought of as "orthonormal" with respect to $\dim \operatorname{Hom}_G(-,-)$. We will come back to this idea in Remark 30.17 when we encounter characters of representations.

Remark 4.13. Part f) of Schur's lemma holds true as long as the cardinality of the algebraically closed field k is strictly larger than the k-dimension of V, i.e. as long as $\operatorname{card} k > \dim_k V$. We will prove this in Remark 22.26 (but the interested reader can check this out right away).

Remark 4.14. We can regard a group G as a category $\mathcal{G}$ in the usual way, i.e. $\mathcal{G}$ consists of only a sinlge object $*$ with $\operatorname{Hom}_{\mathcal{G}}(*,*) = G$, and the composition of morphisms is just the multiplication of G. Then a representation V of G over a field k with corresponding group homomorphism $\rho\colon G \to \operatorname{GL}(V)$ is "the same" as a functor $R\colon \mathcal{G} \to k\text{-}\mathbf{Vect}$ with $R(*) = V$ and $R(g) = \rho(g)$ for every $g \in G = \operatorname{Hom}_{\mathcal{G}}(*,*)$. The category k-G-**Rep** is then isomorphic (!) to the functor category $[\mathcal{G}, k\text{-}\mathbf{Vect}]$.

It follows from this abstract point of view how morphism in k-G-**Rep** should be defined and that k-G-**Rep** inherts a lot of structure from k-**Vect** which can be computed pointswise: Thus k-G-**Rep** is again a k-linear abelian category, it is complete and cocomplete, it has a closed monoidal structure, we have the usual isomorphims known from vector spaces, etc.

5. Maschke's Theorem

Definition 5.1. Let G be a group. A representation V of G (over a field k) is *completely reducible* if

$$V = V_1 \oplus \cdots \oplus V_r$$

for some irreducible subrepresentations $V_1, \dots, V_r \subseteq V$.

Remark 5.2. Not every representation is completely reducible, even if k is algebraically closed. Consider for example the group

$$G \coloneqq \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \,\middle|\, a, b, c \in \mathbb{C} \text{ and } a, c \neq 0 \right\} \subseteq \mathrm{GL}_2(\mathbb{C})$$

and the natural linear action of G on $\mathbb{C}^2$. We have seen in example 2.10 that the corresponding representation is not irreducible, but still indecomposable. It can therefore not be decomposed into a direct sum of irreducible subrepresentations.

Example 5.3. Let $n \geq 2$ and let the symmetric group S_n acts on k^n via

$$\sigma.e_i = e_{\sigma(i)}$$

for all $\sigma \in S_n$, $i = 1, \dots, n$, where $e_1, \dots, e_n$ denotes the standard basis of k^n. We denote this representation by V. We will show that V is reducible, but completely reducible if and only if $\mathrm{char}(k) \nmid n$. We do so by determining all subrepresentations of V.

We consider the linear subspaces $U_1, U_2 \subseteq k^n$ given by

$$U_1 \coloneqq \{(x_1, \dots, x_n) \in V \mid x_1 = \cdots = x_n\},$$
$$U_2 \coloneqq \left\{ (x_1, \dots, x_n) \in V \,\middle|\, \sum_{i=1}^n x_i = 0 \right\}.$$

These are proper non-zero subrepresentations of V of complementary dimensions $\dim U_1 = 1$ and $\dim U_2 = n - 1$: Both subspaces are invariant under the action of S_n because the conditions $x_1 = \cdots = x_n$ and $\sum_{i=1}^n x_i = 0$ do not depend on the order of the x_i. A basis of U_1 is given by the single vector $(1, \dots, 1)$, while a basis of U_2 is given by the vectors of the form $(0, \dots, 0, 1, -1, 0, \dots, 0)$, of which there are $n - 1$ many. Note that the existence of U_1 and U_2 already shows that V itself is reducible.

To determine when V is completely reducible we note that the subrepresentations U_1, U_2 are the only non-zero proper subrepresentations of V. To see this, we consider an arbitrary non-zero proper subrepresentation $U \subseteq V$ and distinguish between two cases:

- If for every $(x_1, \dots, x_n) \in U$ we have that $x_1 = \cdots = x_n$ then U is contained in U_1. Because U is non-zero it follows from $\dim U_1 = 1$ that $U = U_1$.

- Otherwise there exists some $v = (x_1, \dots, x_n) \in U$ with $x_i \neq x_j$ for some i, j. By using the action of S_n on U we may assume w.l.o.g. that $x_1 \neq x_2$. Then $v = (x_1, x_2, x_3, \dots, x_n)$ and $(1\,2).v = (x_2, x_1, x_3, \dots, x_n)$, hence

  $$v - (1\,2).v = (x_1 - x_2, x_2 - x_1, 0, \dots, 0) \in U\,.$$

  After dividing by $x_1 - x_2 \neq 0$ we arrive at

  $$(1, -1, 0, \dots, 0) \in U\,.$$

  By using the action of S_n on U it further follows that all vectors of the form

  $$(0, \dots, 0, 1, -1, 0, \dots, 0)$$

  are contained in U. It follows that $U_2 \subseteq U$ because these vectors form a k-basis of the subrepresentation U_2. Because U is a proper subrepresentation it further follows from $\dim U_2 = n - 1$ that $U = U_2$.

Because V itself is not irreducible, it follows that V is completely reducible if and only both U_1 and U_2 are irreducible and $V = U_1 \oplus U_2$, as no other decomposition into subrepresentations is possible.

- The condition $V = U_1 \oplus U_2$ is equivalent to $U_1 \cap U_2$ because U_1 and U_2 have complementary dimensions. Because U_1 is one-dimensional this holds if and only if $U_1 \nsubseteq U_2$.

- The representation U_1 is one-dimensional, and therefore irreducible. As every subrepresentation of U_2 is also a subrepresentation of V it follows that U_2 is irreducible if and only if U_1 is not a proper subrepresentation of U_2.

Hence V is completely reducible if and only if $U_1 \nsubseteq U_2$, which is equivalent to $\operatorname{char}(k) \nmid n$.

Example 5.4.

a) Let $k = \mathbb{C}$ and let the cyclic group $G = \mathbb{Z}/n$ act linearly on the vector space $V := \mathbb{C}^n$ by rotating the coordinates to the left, i.e.

   $$\overline{k}.(x_1, x_2, \dots, x_n) = (x_2, \dots, x_n, x_1)\,.$$

   The representation V is completely reducible, with the irreducible subrepresentations being one-dimensional by Corollary 4.9.

   Let $\omega_0, \dots, \omega_{n-1} \in \mathbb{C}$ denotes the n-th roots of unity, i.e. $\omega_j = e^{2\pi i j/n}$. Then the group G acts on the vectors $v_0, \dots, v_{n-1} \in V$ with

   $$v_j = (1, \omega_j, \omega_j^2, \dots, \omega_j^{n-1})$$

   by mutliplication with scalars, namely

   $$\overline{1}.v_j = \omega_j v_j$$

for every $j = 0, \dots, n-1$. The one-dimensional subspaces $U_j := \langle v_j \rangle_{\mathbb{C}}$ are therefore subrepresentations of V. The vectors $v_0, \dots, v_{n-1}$ are linearly independent because the Vandermonte determinant

$$\det \begin{bmatrix} 1 & \omega_0 & \omega_0^2 & \cdots & \omega_0^{n-1} \\ 1 & \omega_1 & \omega_1^2 & \cdots & \omega_1^{n-1} \\ 1 & \omega_2 & \omega_2^2 & \cdots & \omega_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_{n-1} & \omega_{n-1}^2 & \cdots & \omega_{n-1}^{n-1} \end{bmatrix} = \prod_{i>j} (\omega_i - \omega_j)$$

is non-zero. The resulting decomposition $V = U_0 \oplus \cdots \oplus U_{n-1}$ is a decomposition into one-dimensional subrepresentations.

b) More generally, let G be a finite abelian groups and k an algebraically closed field with $\operatorname{char}(k) = 0$. Then every representation V of G over k is completely reducible, with the irreducible subrepresentations being one-dimensional by Corollary 4.9:

Let $|G| = n$ and let $\rho\colon G \to \mathrm{GL}(V)$ be the group homomorphism which corresponds to the linear action of G on V. Then $\rho(g)^n = \rho(g^n) = \rho(1) = \mathrm{id}_V$ for every $g \in G$, so that every endomorphism $\rho(g)\colon V \to V$ satisfies the polynomial identity $\rho(g)^n - \mathrm{id}_V = 0$, i.e. satisfies the polynomial $p(t) := t^n - 1 \in k[t]$. The polynomials $p(t)$ decomposes into linear factors because k is algebraically closed. The roots of $p(t)$ are the n-th roots of unity $w_1, \dots, w_n$, which are pairwise different because $\operatorname{char}(k) = 0$. Hence $\rho(g)$ satisfies the polynomial $p(t)$ which decomposes into pairwise different linear factors $p(t) = (t - w_1) \cdots (t - w_n)$. It follows from linear algebra that every $\rho(g)$ is diagonalizable with possible eigenvalues $w_1, \dots, w_n$.

Because G is abelian it further follows that the endomorphisms $\rho(g)$ are simultaneously diagonalizable, i.e. there exists a decomposition

$$V = U_1 \oplus \cdots \oplus U_r$$

such that every $\rho(g)$ acts on each U_i by multiplication with some scalar $\lambda_i(g) \in k$, namely some of the roots of unity $w_1, \dots, w_n$. It then follows that every linear subspace of every U_i is a subrepresentation. By decomposing every U_i into a direct sum of one-dimensional linear subspaces we arrive at a decomposition of V into one-dimensional subrepresentations.

Theorem 5.5 (Maschke's theorem)**.** Let G be a finite group and let k be a field such that $\operatorname{char}(k) \nmid |G|$. Then any finite-dimensional representation of G over k is completely reducible.

Proof. It is enough to show that every subrepresentation $U \subseteq V$ has a direct complement $W \subseteq V$ which is again a subrepresentation, i.e. such that $V = U \oplus W$ as (sub)representations.

Given a subrepresentation $U \subseteq V$ let $W \subseteq V$ be a direct complement as vector spaces. Then $V = U \oplus W$ as vector spaces. Let $p\colon V \to V$ be the projection onto U along W, i.e. the unique k-linear map $V \to V$ with

$$p(u + w) = u$$

for all $u \in U$, $w \in W$. Note that $\operatorname{im} p = U$. The map p is not necessarily G-equivariant, which is why we want to replace p with a G-equivariant projection $\hat{p} \colon V \to V$ onto U. We define $\hat{p}$ as

$$\hat{p}(v) \coloneqq \frac{1}{|G|} \sum_{g \in G} g^{-1}.p(g.v)\,.$$

The factor $1/|G|$ is well-defined because $|G|$ is finite and $|G|$ is nonzero as an element of k because $\operatorname{char}(k) \nmid |G|$.

For all $g \in G$, $v \in V$ we have that $p(g.v) \in \operatorname{im} p = U$, and because U is a subrepresentation therefore also $g^{-1}.p(g.v) \in U$. It follows that $\operatorname{im} \hat{p} \subseteq U$. From p being a projection onto U it follows that

$$\hat{p}(u) = \frac{1}{|G|} \sum_{g \in G} g^{-1}.p(g.u) = \frac{1}{|G|} \sum_{g \in G} g^{-1}.g.u = \frac{1}{|G|} \sum_{g \in G} u = \frac{1}{|G|} |G| \cdot u = u$$

for every $u \in U$. Together with $\operatorname{im} \hat{p} \subseteq U$ this shows that $\hat{p}$ is again a projection onto U (but not along necessarily W). The projection $\hat{p}$ is G-equivariant because

$$\begin{aligned} \hat{p}(h.v) &= \frac{1}{|G|} \sum_{g \in G} g^{-1}.p(gh.v) = \frac{1}{|G|} \sum_{g \in G} h.h^{-1}.g^{-1}.p(g.h.v) \\ &= \frac{1}{|G|} \sum_{\bar{g} \in G} h.\bar{g}^{-1}.p(\bar{g}.v) = h.\hat{p}(v) \end{aligned}$$

for all $h \in G$, $v \in V$.

Because $\hat{p}$ is a projection onto U it follows that $V = \operatorname{im} \hat{p} \oplus \ker \hat{p} = U \oplus \ker \hat{p}$. The direct complement $\ker \hat{p}$ is a subrepresentation because $\hat{p}$ is G-equivariant. □

Remark 5.6. We will later (subsection 22.3) see that the decomposition of a representation into irreducible subrepresentations is unique up to permutation and isomorphism of the summands: If V is a representation of a group G and

$$V = \bigoplus_{i \in I} V_i = \bigoplus_{j \in J} V'_j$$

are two decomposition into irreducible subrepresentations V_i, V'_j, then $\operatorname{card} I = \operatorname{card} J$ and there exists a bijection $\pi \colon I \to J$ with $V'_{\pi(i)} \cong V_i$ for every $i \in I$.

Example 5.7.

a) Consider the linear action of the symmetric group S_n on the polynomial ring $k[X_1, \dots, X_n]$ given by

$$\sigma.p(X_1, \dots, X_n) = p(X_{\sigma(1)}, \dots, X_{\sigma(n)})$$

for all $\sigma \in S_n$, $p(X_1, \dots, X_n) \in k[X_1, \dots, X_n]$. For every $d \geq 0$ let

$$k[X_1, \dots, X_n]_d \coloneqq \left\langle X_1^{d_1} \cdots X_n^{d_n} \,\middle|\, d_1 + \dots + d_n = d \right\rangle_k$$

and consider the resulting decomposition $k[X_1, \dots, X_n] = \bigoplus_{d \geq 0} k[X_1, \dots, X_n]_d$ into finite-dimensional subrepresenations. If $\operatorname{char}(k) = 0$ then it follows from Maschke's theorem that every $k[X_1, \dots, X_n]_d$ is completely reducible. Hence $k[X_1, \dots, X_n]$ is completely reducible.

b) By combining Maschke's theorem with Corollary 4.9 we can reconstruct the result from Example 5.4: Under the given conditions the representation V decomposes into a direct sum of irreducible subrepresentations, each of which is one-dimensional. The actions on these one-dimensional subrepresentations must be given by multiplication with scalars from $k^\times$. Because G is finite, so that every element $g \in G$ has finite order, it then follows that these scalars must have finite order in $k^\times$, i.e. must be roots of unity.

Warning 5.8. If $\operatorname{char}(k)$ divides $|G|$ then Maschke's theorem does not hold: The left regular representation $k[G]$ is then not completely reducible. We will later give a proof of this, when we have another characterization of complete reducibility available.

5.9. It is worthwhile to mention another proof of Maschke's theorem for the case that $k \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$:

Suppose first that V is endowed with an inner product $\langle -, - \rangle$ which is G-invariant in the sense that

$$\langle g.v_1, g.v_2 \rangle = \langle v_1, v_2 \rangle$$

for all $g \in G$, $v_1, v_2 \in V$. Then for every subrepresentation $U \subseteq V$ the orthogonal complement $U^\perp \subseteq V$ is again a subrepresentation: It is a linear subspace, and for all $g \in G$, $v \in U^\perp$ one has that

$$\langle g.v, u \rangle = \langle g.v, g.g^{-1}.u \rangle = \langle v, g^{-1}.u \rangle = 0$$

for every $u \in U$ because $g^{-1}.u \in U$. It follows that for every subrepresentation $U \subseteq V$ there exists a subrepresentation $W \subseteq V$ with $V = U \oplus W$, namely $W = U^\perp$.

It remains to show that there exists a G-invariant inner product on V. For this we start off with an arbitrary inner product $\langle -, - \rangle$ on V and then define $\langle -, - \rangle'$ by

$$\langle v_1, v_2 \rangle' := \frac{1}{|G|} \sum_{g \in G} \langle g.v_1, g.v_2 \rangle$$

for all $v_1, v_2 \in V$. Then $\langle -, - \rangle'$ is also an inner product on V: The bilinearity (resp. sesquilinearity) of $\langle -, - \rangle'$ follows from the one of $\langle -, - \rangle$ and the linearity of the G-action. For every $v \in V$ with $v \neq 0$ we have that

$$\langle v, v \rangle' := \frac{1}{|G|} \langle g.v, g.v \rangle \geq \frac{\langle v, v \rangle}{|G|} > 0 \,,$$

so that $\langle -, - \rangle'$ is positive definite. This new inner product $\langle -, - \rangle'$ is G-invariant because

$$\langle g.v_1, g.v_2 \rangle' = \frac{1}{|G|} \sum_{h \in G} \langle h.g.v_1, h.g.v_2 \rangle = \frac{1}{|G|} \sum_{h' \in G} \langle h'.v_1, h'.v_2 \rangle = \langle v_1, v_2 \rangle$$

for all $v_1, v_2 \in V$.

Remark 5.10. Both proofs of Maschke's theorem show the seemingly stronger statement that every subrepresentation $U \subseteq V$ has a direct complement which is again a subrepresenation. We will see in Proposition 22.13 that both of these conditions are actually equivalent, i.e. that a representation V is completely reducible if and only if every subrepresentation $U \subseteq V$ has a direct complement which is again a subrepresentation.

Remark 5.11. Both proofs of Maschke's theorem make use of a powerful technique, the so called *projection onto the invariants*: If V is a representation of a finite group G over a field k with $\operatorname{char}(k) \nmid |G|$, then consider the map

$$\widehat{(-)} : V \to V^G \,, \quad v \mapsto \hat{v} := \frac{1}{|G|} \sum_{g \in G} g.v \,.$$

This map "averages" a vector $v \in V$ over the linear group action. The map $\widehat{(-)}$ is linear because G acts linearly on V. For every $v \in V$ the element $\hat{v}$ is G-invariant because

$$g.\hat{v} = g. \left(\frac{1}{|G|} \sum_{h \in G} h.v \right) = \frac{1}{|G|} \sum_{h \in G} (gh).v = \frac{1}{|G|} \sum_{g' \in G} g'.v = \hat{v} \,.$$

If v is already invariant itself then $g.v = v$ for every $g \in G$, so that

$$\hat{v} = \frac{1}{|G|} \sum_{g \in G} g.v = \frac{1}{|G|} \sum_{g \in G} v = \frac{|G|}{|G|} v = v \,.$$

Together this shows that $\widehat{(-)}$ is a projection onto the subspace of invariants $V^G \subseteq V$.

In the first proof of Maschke's theorem it follows for the linear map $p \in \operatorname{Hom}(V, V)$ that $\hat{p} \in \operatorname{Hom}(V, V)^G = \operatorname{Hom}_G(V, V)$, so that $\hat{p}$ is a morphism of representations. Note however, that from this argumentations is it not yet clear, that $\hat{p}$ is again a projection onto the subrepresentation U. A possible explanation of this can be found at [MS18a].

In the second proof we let G act linearly on the space $\operatorname{BF}(V)$ (resp. $\operatorname{SF}(V)$) of bilinear (resp. sesquilinear) forms $\beta \colon V \times V \to k$ via

$$(g.\beta)(v_1, v_2) = \beta\left(g^{-1}.v_1, g^{-1}.v_2\right)$$

for all $g \in G$, $v_1, v_2 \in V$. Then the bilinear (resp. sesquilinear) form β is invariant in the sense of 5.9 if and only if it is invariant in the sense of groups actions. It is then only natural to construct the required invariant inner product $\langle -, - \rangle'$ by projection the given inner product $\langle -, - \rangle$ onto the invariants $\operatorname{BF}(V)^G$ (resp. $\operatorname{SF}(V)^G$).

Part II

Invariant Theory and Zariski Density

Polynomial Functions

6. Graded and Filtered Algebras

6.1. Graded Algebras

Definition 6.1. A *grading* of a k-algebra A is a decomposition $A = \bigoplus_{d \in \mathbb{N}} A_d$ into k-linear subspaces $A_d \subseteq A$ such that $A_i A_j \subseteq A_{i+j}$ for all $i, j \in \mathbb{N}$. A *graded k-algebra* is a k-algebra A together with a grading $A = \bigoplus_{d \in \mathbb{N}} A_d$. The direct summand A_d is then the *homogeneous part of degree d of A* and the elements $x \in A_d$ are *homogeneous of degree d.*

A *grading* of a ring R is a decomposition $R = \bigoplus_{d \in \mathbb{N}} R_d$ into additive subgroups $R_d \subseteq R$ such that $R_i R_j \subseteq R_{i+j}$ for all $i, j \in \mathbb{N}$. A *graded ring* is a ring R together with a grading of R. The *homogeneous parts* and *homogeneous elements* of R are defined as above.

Remark 6.2.

a) Every graded k-algebra is also a graded ring, as every k-linear subspace $A_d \subseteq A$ is in particular an additive subgroup.

b) If R is graded ring then $1 \in R_0$:

   There exists a decomposition $1 = \sum_{d \in \mathbb{N}} e_d$ with $e_d \in R_d$ for every $d \in \mathbb{N}$. For every homogeneous Element $x \in R_{d'}$ we then have that

$$R_{d'} \ni x = 1 \cdot x = \sum_{d \in \mathbb{N}} \underbrace{e_d x}_{\in R_{d+d'}} ,$$

   from which it follows that $e_d x = 0$ for every $d \neq 0$ and that $e_0 x = x$. It follows that $e_0 x = x$ for every $x \in R$, as every such x is a sum of homogeneous elements. Hence e_0 is the multiplicative neutral element of R, so that $1 = e_0 \in R_0$.

c) It follows that if R is a graded ring then R_0 is a subring of R. Every homogeneous part R_d then inherits the structure of an R_0-R_0-bimodule from the multiplication of R.

d) If A is a graded ring which is also a k-algebra, then A is a graded algebra with respect to the given grading if and only if A_0 contains the linear space $\langle 1 \rangle_k$: If A is a graded k-algebra then it follows from $1 \in A_0$ that $\langle 1 \rangle_k \subseteq A_0$. If on the other hand $\langle 1 \rangle_k \subseteq A_0$ then

$$kA_d = k1A_d = \langle 1 \rangle_k A_d \subseteq A_0 A_d \subseteq A_d$$

for every $d \in \mathbb{N}$, which shows that the additive subgroup A_d is already a k-linear subspace.

Remark 6.3. If A is a graded algebra with grading $A = \bigoplus_{d \in \mathbb{N}} A_d$ then can more generally define for every non-zero $x \in A$ with homogeneous decomposition $x = \sum_{d \in \mathbb{N}} x_d$ the *degree of* x as the maximal $d \in \mathbb{N}$ with $x_d \neq 0$. If x is homogeneous, then the degree of x coincides with its homogeneous degree.

Remark 6.4. Let $(M, \cdot)$ be a monoid.

a) Instead of using the natural numbers $\mathbb{N}$ one can also define gradings over M:

For a monoid $M = (M, \cdot)$ an *M-grading* of a k-algebra A is a decomposition $A = \bigoplus_{m \in M} A_m$ into k-linear subspaces $A_m \subseteq A$ such that $A_m A_{m'} \subseteq A_{mm'}$ for all $m, m' \in M$. An *M-graded k-algebra* is a k-algebra A together with an M-grading $A = \bigoplus_{m \in M} A_m$. The notion of an M-graded ring can be defined in the same way.

A grading as defined in Definition 6.1 is precisely an $\mathbb{N}$-grading.

b) Let $R = \bigoplus_{m \in M} R_m$ be an M-graded ring. If the monoid M is right cancellative (i.e. it follows for all $m_1, m_2, m \in M$ from $m_1 m = m_2 m$ that $m_1 = m_2$) then it still follows from the calculations of part b) of Remark 6.2 that $1 \in R_e$, where e denotes the neutral element of M. By using the identity $x = x \cdot 1$ instead of $x = 1 \cdot x$ in this calculation it follows that this also holds if M is left cancellative.

This holds in particular if M is a group or a submonoid of a group.

In then follows that R_e is a subring of R and that for every $m \in M$ the homogeneous part R_m inherits the structure of an R_e-R_e-bimodule from the multiplication of R.

c) Suppose that $N \subseteq M$ is a submonoid, i.e. we have that $e_M \in N$ and $n_1 n_2 \in N$ for all $n_1, n_2 \in N$. Then every N-graded k-algebra $A = \bigoplus_{n \in N} A_n$ can be regarded as an M-graded k-algebra $A = \bigoplus_{m \in M} A_m$ by setting $A_m = 0$ for every $m \in M$ with $m \notin N$. The same holds for graded rings.

As a special case of this construction every $\mathbb{N}$-grading of a k-algebra A (resp. ring R) can be regarded as a $\mathbb{Z}$-grading with $A_d = 0$ (resp. $R_d = 0$) for all $d < 0$.

Indeed, the definition of a grading given in the lecture did not use an $\mathbb{N}$-grading as we have in done in Definition 6.1 but a $\mathbb{Z}$-grading. But all the examples and applications of graded k-algebras presented in this lecture were actually only using an $\mathbb{N}$-gradings, so we adjusted the definition accordingly.

Example 6.5.

a) Every k-algebra A can be given a grading $(A_d)_{d \in \mathbb{N}}$ with $A_0 = A$ and $A_d = 0$ otherwise. We then say that A is *concentrated in degree* 0.

b) Let k be a field (resp. ring) and let $A \coloneqq k[X_1, \dots, X_n]$. For every $d \in \mathbb{N}$ let $A_d \subseteq A$ be given by

$$A_d \coloneqq \left\langle X_1^{\alpha_1} \cdots X_n^{\alpha_n} \,\middle|\, \sum_{i=1}^n a_i = d \right\rangle_k .$$

This defined a grading for A:

Note that A_d is a k-linear subspace, resp. additive subgroup of A by definition. Because the monomials $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ with $\alpha_1, \dots, \alpha_n \geq 0$ form a k-basis of A we find that $A = \bigoplus_{d \in \mathbb{N}} A_d = \bigoplus_{d \in \mathbb{N}} A_d$. For all monomials $X^{\alpha_1} \cdots X^{\alpha_n} \in A_i$, $X^{\beta_1} \cdots X^{\beta_n} \in A_j$ we have that

$$(X_1^{\alpha_1} \cdots X_n^{\alpha_n})(X_1^{\beta_1} \cdots X_n^{\beta_n}) = X_1^{\alpha_1+\beta_1} \cdots X_n^{\alpha_n+\beta_n} \in A_{i+j}$$

because $\sum_{l=1}^{n} (\alpha_l + \beta_l) = (\sum_{l=1}^{n} \alpha_l) + (\sum_{l=1}^{n} \beta_l) = i + j$. By the k-bilinearity of the multiplication of A it follows that $A_i A_j \subseteq A_{i+j}$ for all $i, j \in \mathbb{N}$.

Note that the degree of any non-zero polynomial $f \in k[X_1, \dots, X_n]$ with respect to this grading (as defined in Remark 6.3) coincides with its total degree.

c) In a similar matter the k-algebra of Laurant polynomials

$$A \coloneqq k[X_1, X_1^{-1}, \dots, X_n X_n^{-1}]$$

has a $\mathbb{Z}$-grading given by

$$A_d \coloneqq \left\langle X_1^{\alpha_1} \cdots X_n^{\alpha_n} \,\middle|\, \sum_{i=1}^{n} a_i = d \right\rangle_k .$$

for all $d \in \mathbb{Z}$.

d) Let V be a k-vector space. For every $d \geq 0$ we denote by $V^{\otimes d}$ the d-th tensor power of V. Recall that $V^{\otimes 0} = k$.

For all $p, q \in \mathbb{N}$ there exists a unique k-bilinear map $V^{\otimes p} \times V^{\otimes q} \to V^{\otimes (p+q)}$, $(x, y) \mapsto x \cdot y$ which is given on simple tensors by

$$(v_{i_1} \otimes \cdots \otimes v_{i_p}) \cdot (v_{j_1} \otimes \cdots \otimes v_{j_q}) = v_{i_1} \otimes \cdots \otimes v_{i_p} \otimes v_{j_1} \otimes \cdots \otimes v_{j_q}$$

for all $v_{i_1}, \dots, v_{i_p}, v_{j_1}, \dots, v_{j_q} \in V$. The *tensor algebra* (*over* V) is given by the k-vector space $T(V) \coloneqq \bigoplus_{d \in \mathbb{N}} V^{\otimes d}$ together with the unique k-bilinear extension $T(V) \times T(V) \to V$ of the above multiplications. The decomposition $T(V) = \bigoplus_{d \in \mathbb{N}} V^{\otimes d}$ is then a grading of $T(V)$.

e) Let $n \geq 1$ and let E_{ij} with $i, j = 1, \dots, n$ be the standard basis of $\mathrm{M}_n(k)$. We set $E_{ij} \coloneqq 0$ for all $i, j \in \mathbb{Z}$ with $i \notin \{1, \dots, m\}$ or $j \notin \{1, \dots, n\}$. Then the k-algebra $\mathrm{M}_n(k)$ has a $\mathbb{Z}$-grading given by

$$\mathrm{M}_n(k)_d = \langle E_{i,i+d} \,|\, i \in \mathbb{Z} \rangle_k$$

for all $d \in \mathbb{Z}$. That $\mathrm{M}_n(k) = \bigoplus_{d \in \mathbb{Z}} \mathrm{M}_n(k)_d$ follows from the choice of the E_{ij}. To see that $\mathrm{M}_n(k)_d \, \mathrm{M}_n(k)_{d'} \subseteq \mathrm{M}_n(k)_{d+d'}$ note that $\mathrm{M}_n(k)_d$ consists of precisely those matrices who have non-zero entries only on the d-th diagonal. The k-algebra $\mathrm{M}_n(k)_0$ is precisely the k-subalgebra of diagonal matrices.

Remark 6.6. Given two graded k-algebras A and B with gradings $A = \bigoplus_{d \in \mathbb{N}} A_d$ and $B = \bigoplus_{d \in \mathbb{N}} B_d$ a *morphism of graded k-algebras* $A \to B$ is a homomorphism of k-algebras $f \colon A \to B$ with $f(A_d) \subseteq B_d$ for every $d \in \mathbb{N}$.

For every graded k-algebra A the identity $\mathrm{id}_A \colon A \to A$ is a morphism of graded k-algebras, and for any two composable morphisms of graded k-algebras $f \colon A \to B$ and $g \colon B \to C$ their composition $g \circ f \colon A \to C$ is again a morphism of graded k-algebras.

It follows that the class of graded k-algebras together with the morphisms of graded k-algebras forms a category k-**grAlg**.

6.2. Filtered Algebras

Definition 6.7. Let A be a k-algebra. A *filtration of A* is a (possibly infinite) sequence F of k-linear subspaces

$$0 = F_{-1}(A) \subseteq F_0(A) \subseteq F_1(A) \subseteq F_2(A) \subseteq \cdots \subseteq A$$

such that $A = \bigcup_{d \geq -1} F_d(A)$, $1 \in F_0(A)$ and

$$F_i(A)F_j(A) \subseteq F_{i+j}(A)$$

for all i, j. A *filtered k-algebra* is a k-algebra A together with a filtration of A.

Remark 6.8. The condition $F_{-1}(A) = 0$ is not terribly interesting. We only use this convention to later form the quotients $F_d(A)/F_{d-1}(A)$ for all $d \in \mathbb{N}$ without having to worry about the case $d = 0$.

Example 6.9. Let A be a k-algebra.

a) Every grading $A = \bigoplus_{d \in \mathbb{N}} A_d$ of A leads to a filtration F of A which is given by $F_d(A) \coloneqq \bigoplus_{i=0}^{d} A_i$ for every d.

b) By considering the grading $A_0 = A$ and $A_d = 0$ for $d \geq 1$ it follows that A carries a filtration F given by $F_d(A) = A$ for every $d \geq 0$.

c) Let A be a filtered k-algebra with filtration F, and let $I \subseteq A$ be an ideal. Then the quotient algebra A/I inherits a filtration F' given by $F'_d \coloneqq \pi(F_d)$ for every d, where $\pi \colon A \to A/I$ denotes the canonical projection.

Remark 6.10. Given two filtered k-algebras A and B with filtrations F and G a *morphism of filtered k-algebras* $A \to B$ is a homomorphism of k-algebras $f \colon A \to B$ with $f(F_d(A)) \subseteq G_d(B)$ for every d.

For every filtered k-algebra A the identity $\mathrm{id}_A \colon A \to A$ is a morphism of filtered k-algebras, and for any two composable morphisms of filtered k-algebras $f \colon A \to B$ and $g \colon B \to C$ their composition $g \circ f \colon A \to C$ is again a morphism of filtered k-algebras.

It follows that the class of filtered k-algebras together with the morphisms of filtered k-algebras forms a category k-**filtAlg**.

Example 6.11. Let A, B be graded k-algebras with gradings $A = \bigoplus_{d\in\mathbb{N}} A_d$ and $B = \bigoplus_{d\in\mathbb{N}} B_d$, and let F and G be the associated filtrations given by $F_d(A) = \bigoplus_{i=0}^{d} A_i$ and $G_d(B) = \bigoplus_{i=0}^{d} B_i$ for every $d \in \mathbb{N}$. Then every morphism $f\colon A \to B$ of graded k-algebras is also a morphism of filtered k-algebras.

We therefore get a (faithful) functor k-**grAlg** $\to$ k-**filtAlg**.

Definition 6.12. Let A be a filtered k-algebra with filtration F. The *degree* of a nonzero element $x \in A$ is the minimal $d \geq 0$ with $x \in F_d$. The degree of $0 \in A$ is $-\infty$.

Example 6.13. Let $A = \bigoplus_{d\geq 0} A_d$ be a graded k-algebra and let F be the associated filtration of A given by $F_d(A) = \bigoplus_{d'=0}^{d} A_d$ for every $d \geq -1$. Then the degeree of $x \in A$ with respect to the filtration F coincides with the degree of x with respect to the grading as defined in Remark 6.3.

Lemma 6.14. Let F be a filtration of a k-algebra A and let $f\colon A \to B$ be a homomorphism of a k-algebras. For every $d \geq -1$ let $G_d(B) \coloneqq f(A_d)$. Then

$$0 = G_{-1}(B) \subseteq G_0(B) \subseteq G_1(B) \subseteq \cdots$$

is a filtration of B.

Proof. Every G_i is a k-linear subspace of B and $G_{-1}(B) = f(F_{-1}(A)) = f(0) = 0$. For all $i, j \geq -1$ we have that

$$G_i(B)G_j(B) = f(F_i(A))f(F_j(A)) = f(F_i(A)F_j(A)) \subseteq f(F_{i+j}(A)) = G_{i+j}(B)\,.$$

This proves the claim. □

6.15. Let A be a k-algebra. Then the previous example a) shows that every grading of A leads to a filtration of A. But not all filtration of A need to arise in this way, as we will see in 6.28.

If A is a filtered algebra with filtration F, then there in general no good way to assign a “corresponding” grading of A. It is, however, possible to construct a graded algebra $\mathrm{gr}_F(A)$ as follows:

For every $d \geq 0$ let

$$\mathrm{gr}_F(A)_d \coloneqq F_d(A)/F_{d-1}(A)\,,$$

and let $\mathrm{gr}_F(A) \coloneqq \bigoplus_{d\geq 0} \mathrm{gr}_F(A)_d$. For every $d \in \mathbb{N}$, $x \in F_d(A)$ we denote the residue class of x in $\mathrm{gr}_F(A)_d$ by $[x]_d$. Note that for every $x \in A$, $x \neq 0$ there exists some minimal $d \in \mathbb{N}$ with $x \in F_d(A)$. Then $[x]_{d'}$ is not defined for $d' < d$, $[x]_d \neq 0$ and $[x]_{d'} = 0$ for every $d' > d$.

For $[x]_i \in \mathrm{gr}_F(A)_i$ and $[y]_j \in \mathrm{gr}_F(A)_j$ we define their product as

$$[x]_i \cdot [y]_j \coloneqq [xy]_{i+j} \in \mathrm{gr}_F(A)_{i+j}\,.$$

This product is well-defined: If $[x]_i = [x']_i$ and $[y]_j = [y']_j$ for some $x, x' \in F_i(A)$ and $y, y' \in F_j(A)$, then $x - x' \in F_{i-1}(A)$ and $y - y' \in F_{j-1}(A)$, so that

$$\begin{aligned} xy - x'y' &= xy - xy' + xy' - x'y' \\ &= x(y - y') + (x - x')y \in F_{i+j-1}(A) + F_{i-1+j}(A) = F_{i+j-1}(A) \end{aligned}$$

and therefore $[xy]_{i+j} = [x'y']_{i+j}$. By putting all these multiplications together we arrive at a multiplication $\mathrm{gr}_F(A) \times \mathrm{gr}_F(A) \to \mathrm{gr}_F(A)$. This multiplication is k-bilinear, associative and distributive, as can be checked on (homogeneous) representatives. For $[1]_0 \in \mathrm{gr}_F(A)_0$ we have for every $[x]_i \in \mathrm{gr}_F(A)_i$ that

$$[1]_0 \cdot [x]_i = [1 \cdot x]_{0+i} = [x]_i \,.$$

As every element of $\mathrm{gr}_F(A)$ is the sum of such homogeneous elements it follows that $[1]_0$ is a multiplicative identity for $\mathrm{gr}_F(A)$. Altogether this shows that $\mathrm{gr}_F(A)$ is a k-algebra. The decomposition $\mathrm{gr}_F(A) = \bigoplus_{d\geq 0} \mathrm{gr}_F(A)_d$ is a grading of $\mathrm{gr}_F(A)$ by construction of the multiplication of $\mathrm{gr}_F(A)$.

The algebra $\mathrm{gr}_F(A)$ is the *associated graded algebra* of the filtered algebra A. The filtration F may be surpressed from the notation, writting $\mathrm{gr}(A)$ instead of $\mathrm{gr}_F(A)$.

Example 6.16. Let A be a graded k-algebra and let $F_d(A) = \bigoplus_{i=0}^{d} A_i$ be the induced filtration. Then

$$\mathrm{gr}_F(A)_d = \left(\bigoplus_{i=0}^{d} A_i \right) \Bigg/ \left(\bigoplus_{i=0}^{d-1} A_i \right) \cong A_d$$

for all $d \in \mathbb{N}$, and the induced multiplication $\mathrm{gr}_F(A)_i \times \mathrm{gr}_F(A)_j \to \mathrm{gr}_F(A)_{i+1}$ corresponds to the original multiplication $A_i \times A_j \to A_{i+j}$ for all $i, j \in \mathbb{N}$. Hence $\mathrm{gr}_F(A)$ is nothing but the orginal graded algebra A.

Remark 6.17. Let A and B be filtered k-algebras with filtrations F and G. Let $f\colon A \to B$ be a morphism of filtered k-algebras. Then $f(F_d(A)) \subseteq G_d(B)$ for every d, so that f induces for every $d \geq 0$ an k-linear map

$$f_d\colon\ \mathrm{gr}_F(A)_d = \mathrm{gr}_G(B)_d \,, \quad [x]_d \mapsto [f(x)]_d \,.$$

By putting all of these maps together, we arriven at a linear map

$$\mathrm{gr}(f)\colon\ \mathrm{gr}(A) \to \mathrm{gr}(B) \,.$$

For $[x]_i \in \mathrm{gr}(A)_i$ and $[y]_j \in \mathrm{gr}(B)_j$ we have that

$$\begin{aligned} f_i([x]_i) f_j([y_j]) &= [f(x)]_i [f(y)]_j = [f(x)f(y)]_{i+j} \\ &= [f(xy)]_{i+j} = f_{i+j}([xy]_{i+j}) = f_{i+j}([x]_i [y]_j) \,. \end{aligned}$$

Hence $\mathrm{gr}(f)$ is multipliative on homogeneous elements, and thus multiplicative as a whole. We also have that

$$f_0([1_A]_0) = [f(1_A)]_0 = [1_B]_0 \,,$$

so that $\mathrm{gr}(f)(1_{\mathrm{gr}(A)}) = 1_{\mathrm{gr}(B)}$. Altogether this shows that $\mathrm{gr}(f)$ is a k-algebra homomorphism. It respects the gradings of $\mathrm{gr}(A)$ and $\mathrm{gr}(B)$ by construction, and thus is a morphism of graded k-algebras.

For every filtered k-algebra A we have that $\mathrm{gr}(\mathrm{id}_A) = \mathrm{id}_{\mathrm{gr}(A)}$, and for any two composable morphisms of filtered k-algebras $f\colon A \to B$ and $g\colon B \to C$ we have that $\mathrm{gr}(g \circ f) = \mathrm{gr}(g) \circ \mathrm{gr}(f)$.

Altogether this shows that gr defined a functor k-**filtAlg** → k-**grAlg**.

Lemma 6.18. Let A be a k-algebra with filtration F. If $\mathrm{gr}_F(A)$ has no zero-divisors then A has no zero divisors.

Proof. Suppose that there exist nonzero elements $x, y \in A$ with $xy = 0$. Then x is of degree $d \geq 0$ and y is of degree $d' \geq 0$. It follows that $[x]_d, [y]_{d'} \in \mathrm{gr}_F(A)$ are nonzero with

$$[x]_d [y]_{d'} = [xy]_{dd'} = [0]_{dd'} = 0\,.$$

This shows that $\mathrm{gr}_F(A)$ has zero divisors. □

6.3. Example: The First Weyl Algebra

6.19. Let k be a field with $\mathrm{char}(k) = 0$. For the polynomial ring $k[x]$ the multiplication with x defines an element of $\xi \in \mathrm{End}_k(k[x])$. Let $\partial \coloneqq \partial/\partial x \in \mathrm{End}_k(k[x])$ be the (formal) derivative with respect to x. The *first Weyl algebra* is the subalgebra $\mathcal{A}$ of $\mathrm{End}_k(k[X])$ which is generated by ξ and ∂. In this section we will examine some of the properties of $\mathcal{A}$.

6.20. It follows from the product rule that

$$\partial\xi = \xi\partial + \mathrm{id}\,. \tag{6.1}$$

We denote by $k\langle X, D\rangle$ the free k-algebra in two generators X, D and by

$$(DX - XD - 1) \trianglelefteq k\langle X, D\rangle$$

the two-sided ideal generated by $DX - XD - 1$. By abuse of notation we denote the images of X, D in $k\langle X, D\rangle/(DX - XD - 1)$ also by X, D. It follows from (6.1) that the unique k-algebra homomorphisms $\Phi\colon k\langle X, D\rangle \to \mathcal{A}$ with $\Phi(X) = \xi$ and $\Phi(D) = \partial$ induces a homomorphism of k-algebras

$$\Psi\colon k\langle X, D\rangle/(DX - XD - 1) \to \mathcal{A}$$

which is given by $\Psi(X) = \xi$ and $\Psi(D) = \partial$. We abbreviate

$$\mathcal{A}' \coloneqq k\langle X, D\rangle/(DX - XD - 1)\,.$$

Lemma 6.21.

a) The monomials $\xi^n \partial^m$ with $n, m \geq 0$ are linearly independent.

b) We have for all $n, m \geq 0$ that $D \cdot X^n D^m = X^n D^{m+1} + nX^{n-1} D^m$.

c) The monomials $X^n D^m$ span $\mathcal{A}'$ as a k-vector space.

Proof.

a) Let $0 = \sum_{n,m \geq 0} c_{n,m} \xi^n \partial^m$ be linear combination. We show that $c_{n,m} = 0$ for all $n, m \geq 0$ by induction over $m \geq 0$: We start for $m = 0$ by observing that

$$0 = \left(\sum_{n,m \geq 0} c_{n,m} \xi^n \partial^m \right) (X^0) = \sum_{n,m \geq 0} c_{n,m} x^n \partial^m (X^0) = \sum_{n \geq 0} c_{n,0} x^n \,,$$

which shows that $c_{n,0} = 0$ for all $n \geq 0$. If $m \geq 1$ and $c_{n,m'} = 0$ for all $m' < m$, $n \geq 0$ then it follows that

$$\begin{aligned} 0 &= \left(\sum_{n,m' \geq 0} c_{n,m'} \xi^n \partial^{m'} \right) (x^m) = \sum_{n,m' \geq 0} c_{n,m'} x^n \partial^{m'} (x^m) \\ &= \sum_{m'=0}^{m} \sum_{n \geq 0} c_{n,m'} m \cdots (m - m' + 1) x^{n+m-m'} = \sum_{n \geq 0} c_{n,m} \, m! \, x^n \,. \end{aligned}$$

It then follows that $c_{n,m} = 0$ for all $n \geq 0$ because $\operatorname{char}(k) = 0$.

b) It suffices to consider the case $m = 0$, which follows from $DX = XD + 1$ by induction over n.

c) Let $I \trianglelefteq \mathcal{A}'$ be the k-linear subspace spanned by all monomials $X^n D^m$, i.e. let

$$I := \langle X^n D^m \,|\, n, m \geq 0 \rangle_k \,.$$

We have that $1 \in I$ so it sufficies to show that I is a left-sided ideal in $\mathcal{A}'$. For this it sufficies to show that I is closed under left multiplication by X and D because $\mathcal{A}'$ is generated by these two elements as a k-algebra. It is enough to show that $X \cdot X^n D^m \in I$ and $D \cdot X^n D^m \in I$ for all $n, m \geq 0$, and we have that $X \cdot X^n D^m = X^{n+1} D^m \in I$ and

$$D \cdot X^n D^m = X^n D^{m+1} + n X^{n-1} D^m \in I$$

by part b). □

Corollary 6.22.

a) The monomials $\xi^n \partial^m$ with $n, m \geq 0$ form a k-basis of $\mathcal{A}$.

b) The monomials $X^n D^m$ with $n, m \geq 0$ form a k-basis of $\mathcal{A}'$.

c) The k-algebra homomorphism $\Psi \colon \mathcal{A}' \to \mathcal{A}$ is an isomorphism.

Proof. We have for all $n, m \geq 0$ that $\Psi(X^n D^m) = \xi^n \partial^m$. It therefore follows from the linear independence of the monomials $\xi^n \partial^m$ that the monomials $X^n D^m$ are also linear independent. It follows from the surjecivity of Ψ that the monomials $\xi^n \partial^m$ form a k-generating set of $\mathcal{A}$ because the monomials $X^n D^m$ generate $\mathcal{A}'$.

This shows that the monomials $X^n D^m$ form a k-basis of $\mathcal{A}'$ and that the monomials $\xi^n \partial^m$ form a k-basis of $\mathcal{A}$. The k-linear map Ψ is an isomorphism because it restricts to a bijection between these bases. □

6.23. The k-algebra $\mathcal{A}'$ inherits a filtration F' from $k\langle X, D\rangle$ given by

$$F'_i(\mathcal{A}') = \langle X^{n_1} D^{n_2} \cdots X^{n_{\ell-1}} D^{n_\ell} \mid \ell \geq 0,\, n_1, \dots, n_\ell \geq 0,\, n_1 + \cdots + n_\ell = i \rangle_k \tag{6.2}$$

for every $i \geq 0$. By the *degree* of a nonzero element $x \in \mathcal{A}'$ we mean its degree with respect to F'. The relation $DX = XD + 1$ gives us the following slogan:

The elements D, X commute up to smaller degree.

This idea leads to the following results:

Lemma 6.24.

a) We have that $XF'_i(\mathcal{A}') \subseteq F'_{i+1}(\mathcal{A}')$ and $DF'_i(\mathcal{A}') \subseteq F'_{i+1}(\mathcal{A}')$ for all $i \geq -1$.

b) For all $n, m, n', m' \geq 0$ we have that

$$X^n D^m X^{n'} D^{m'} = X^{n+n'} D^{m+m'} + \text{terms of lower degree}$$

i.e. that

$$X^n D^m X^{n'} D^{m'} \in X^{n+n'} D^{m+m'} + F'_{n+n'+m+m'-1}(\mathcal{A}') \,.$$

Proof.

a) This follows from $X, D \in F'_1(\mathcal{A}')$.

b) We first consider the case $n = 0$:

The claim holds for $n = 0$, $m = 0$ and it holds for $n = 0, m = 1$ by part b) of Lemma 6.21. It follows that

$$\begin{aligned} D^{m+1} X^{n'} D^{m'} &= D D^m X^{n'} D^{m'} \\ &\in D\left(X^{n'} D^{m+m'} + F'_{n'+m+m'-1}(\mathcal{A}')\right) \\ &= D X^{n'} D^{m+m'} + D F'_{n'+m+m'-1}(\mathcal{A}') \\ &\subseteq X^{n'} D^{m+m'+1} + F'_{n'+m+m'}(\mathcal{A}') + F'_{n'+m+m'}(\mathcal{A}') \\ &= X^{n'} D^{m+m'+1} + F'_{n'+m+m'}(\mathcal{A}') \,, \end{aligned}$$

which shows the claim for $n = 0$ and $m + 1$

We now have for all $n, m \geq 0$ that

$$\begin{aligned} X^n D^m X^{n'} D^{m'} &\in X^n (X^{n'} D^{m+m'} + F'_{n'+m+m'-1}(\mathcal{A}')) \\ &= X^n X^{n'} D^{m+m'} + X^n F'_{n'+m+m'-1}(\mathcal{A}') \\ &= X^{n+n'} D^{m+m'} + F'_{n+n'+m+m'-1}(\mathcal{A}') \,. \end{aligned}$$

This proves the claim. □

Corollary 6.25. For all $\ell \geq 0$, $n_1, m_1, \dots, m_\ell, n_\ell \geq 0$ we have that

$$X^{n_1} D^{m_1} \cdots X^{n_\ell} D^{m_\ell} = X^{n_1 + \dots + n_\ell} D^{m_1 + \dots + m_\ell} + \text{terms of smaller degree}\,.$$

Proof. This follows from Lemma 6.24 by induction on ℓ. □

Corollary 6.26. For every $d \geq 0$ the monomials $X^n D^m$ of degree $n + m \leq d$ form a k-basis of $F'_d(\mathcal{A}')$.

Proof. It suffices to show that $F'_d(\mathcal{A}')$ is k-spanned by the monomials $X^n D^m$ with $n + m \leq d$ because we know from Corollary 6.22 that these monomials are linearly independent. We show this by induction over d.

We have that $F'_0(\mathcal{A}') = \langle 1 \rangle_k = \left\langle X^0 D^0 \right\rangle_k$, which shows the claim for $d = 0$. Let $d \geq 0$ and suppose that for every $d' \leq d$ the k-linear space $F'_{d'}(\mathcal{A}')$ is spanned by the monomials $X^n D^m$ of degree $n + m \leq d'$. To show the claim for $d + 1$ it sufficies to show that the monomials

$$X^{n_1} D^{n_2} \cdots X^{n_{\ell-1}} D^{n_\ell} \quad \text{with} \quad \begin{gathered} \ell \geq 0, \\ n_1, \dots, n_\ell, m_1, \dots, m_\ell \geq 0, \\ n_1 + \dots + n_\ell = d + 1 \end{gathered}$$

can be expressed as suitable linear combinations. We know from Corollary 6.25 that

$$X^{n_1} D^{n_2} \cdots X^{n_{\ell-1}} D^{n_\ell} = X^{n_1 + \dots + n_{\ell-1}} D^{n_2 + \dots + n_\ell} + (\text{terms of degree} \leq d)\,,$$

and it follows from the induction hypothesis that the additional terms of degree $\leq d$ can be expressed as suitable linear combinations. □

6.27. We have now found that

$$F'_d(\mathcal{A}') = \langle X^n D^m \mid n + m \leq d \rangle_k$$

for all $d \geq 0$. It follows that for a nonzero element $f \in \mathcal{A}'$ with linear combination $f = \sum_{n,m \geq 0} c_{n,m} X^n D^m$ the degree of f coincides with the maximal degree d for which $c_{n+m} \neq 0$ for some $n, m \geq 0$ with $n + m = d$.

We can use the above observations to determine the associated graded algebra $\operatorname{gr}_{F'}(\mathcal{A}')$: It follows from Corollary 6.26 for every $d \geq$ that the quotient

$$\operatorname{gr}_{F'}(\mathcal{A}')_d = F'_d(\mathcal{A}') / F'_{d-1}(\mathcal{A}')$$

has a basis given by all residue classes $[X^n D^m]_d$ with $n + m = d$. Note that for $d, d' \geq 0$ and $n, m, n', m' \geq 0$ with $n + m = d$, $n' + m' = d'$ the muliplication of two such basis elements $[X^n D^m]_d$ and $[X^{n'} D^{m'}]_{d'}$ is given by

$$[X^n D^m]_d \cdot [X^{n'} D^{m'}]_{d'} = [X^n D^m X^{n'} D^{m'}]_{d+d'} = [X^{n+n'} D^{m+m'}]_{d+d'}\,.$$

because of Lemma 6.24. Altogether this shows that $\operatorname{gr}_{F'}(\mathcal{A}')$ is just the commutative polynomial ring in the two-variables $[X]_1$ and $[D]_1$, i.e. there exists a (unique) k-algebra homomorphism

$$k[t, u] \longrightarrow \operatorname{gr}_{F'}(\mathcal{A}')$$

which maps t to $[X]_1$ and u to $[D]_1$ and this is an isomorphism.

Note that it follows that the filtration F' of $\mathcal{A}'$ does not come from a grading of $\mathcal{A}'$: Otherwise the associated graded algebra $\operatorname{gr}_{F'}(\mathcal{A}')$ would be isomorphic to $\mathcal{A}'$ by Example 6.16, which would contradict $DX = XD + 1$.

It also follows from Lemma 6.18 that $\mathcal{A}'$ has no zero divisors because $\operatorname{gr}_{F'}(\mathcal{A}')$ has no zero divisors.

6.28. We have choosen to work with $\mathcal{A}' = k\langle X, D\rangle/(DX - XD - 1)$ for the above calculations but via the isomorphism $\Psi\colon \mathcal{A}' \to \mathcal{A}$ all of our results also hold for the Weyl algebra $\mathcal{A}$: We have a filtration F on $\mathcal{A}$ given by

$$F_d(\mathcal{A}) = \langle \xi^n \partial^m \mid n + m \leq d\rangle$$

and the monomials $\xi^n\partial^m$ with $n, m \geq 0$ are a basis of $\mathcal{A}$. We also have that

$$\xi^n \partial^m \xi^{n'} \partial^{m'} = \xi^{n+n'} \partial^{m+m'} + \text{terms of lower degree}$$

for all $n, n', m, m' \geq 0$. The associated graded algebra $\operatorname{gr}_F(\mathcal{A})$ is the commutative polynomial ring in the two free variables ξ and ∂. This shows that the filtration F of $\mathcal{A}$ does not come from a grading of $\mathcal{A}$, and it follows from Lemma 6.18 that $\mathcal{A}$ has no zero divisors.

Remark 6.29. We have seen that for the two generators X, D of $\mathcal{A}'$ the corresponding elements $[X]_1, [D]_1$ are again generators of $\operatorname{gr}_{F'}(\mathcal{A}')$. We may ask ourselves if more generally for every algebra A, filtration F of A and k-algebra generators x_i, $i \in I$ of degree $d_i := \deg_F(x_i)$ the elements $[x_i]_{d_i}$, $i \in I$ are again k-algebra generators for $\operatorname{gr}_F(A)$.

This is not always the case. It is shown in [MO15] that for $I = \{1, \dots, n\}$ finite this is the case if and only if the filtration F is the one induced from $k\langle X_1, \dots, X_n\rangle$ via the surjective k-algebra homomorphism $\phi\colon k\langle X_1, \dots, X_n\rangle \to A$ given by $\phi(X_i) = x_i$ for all $i = 1, \dots, n$.

Note that this is the case for the filtration F' of $\mathcal{A}'$ by definition of F'.

Remark 6.30. (Skew polynomial rings) We have seen above that we can think about the first Weyl algebra $\mathcal{A}$ in two ways:

- The k-algebra of linear differential operators $\sum_{n,m\geq 0} c_{n,m}\xi^n\partial^m$ on $k[x]$.
- The k-algebra with generators X, D subject to the relation $DX = XD + 1$.

Yet another way to think about $\mathcal{A}$ is provided by the theory of skew polynomial rings:

We may replace the polynomial ring $k[\xi] \subseteq \mathcal{A}$ by the polynomial ring $k[x]$ and rename the generator ∂ of $\mathcal{A}$ to y. We then have that

$$yx = xy + 1\,,$$

and the more general formula from part b) of Lemma 6.21 becomes

$$yx^n = x^n y + nx^{n-1} = x^n y + \partial(x^n)\,. \tag{6.3}$$

It follows that

$$yp = py + \partial(p)$$

for every polynomial $p \in k[x]$. Note also that the monomials $1, y, y^2, \dots$ form a $k[x]$-basis. We can therefore think about the Weyl algebra $\mathcal{A}$ as resulting from $k[x]$ by adjoining a new variable y for which the multiplication with the original elements of $k[x]$ is given by $yp = \partial(p)$ for all $p \in k[x]$. This idea leads to the notion of skew polynomial rings:

Let R be a k-algebr ($R = k[x]$ in the above case) and let $\delta \colon R \to R$ be a map. We want to give the k-vector space $R[y]$ the structure of a k-algebra (different from the usual structure of a polynomial ring) such that $R \subseteq R[y]$ is a subring and

$$yr = ry + \delta(r) \tag{6.4}$$

for all $r \in R$. For the multiplications $R[y] \to R[y]$, $f \mapsto yf$ and $y \mapsto fy$ to be k-linear we then need the map δ to be k-linear, and for the above multiplication to be associative we need that $\delta(rs) = r\delta(s) + \delta(r)s$ because

$$y \cdot rs = rs \cdot y + \delta(rs)$$

and

$$\begin{aligned} y \cdot rs &= (y \cdot r) \cdot s = (r \cdot y + \delta(r)) \cdot s = r \cdot y \cdot s + \delta(r)s \\ &= r(s \cdot y + \delta(s)) + \delta(r)s = rs \cdot y + r\delta(s) + \delta(r)s \end{aligned}$$

for all $r, s \in R$. Such a k-linear map $\delta \colon R \to R$, i.e. a k-linear map $\delta \colon R \to R$ satisfying the *Leibniz rule*

$$\delta(rs) = r\delta(s) + \delta(r)s\,,$$

is a *k-derivation* of R. If $\delta \colon R \to R$ is a k-derivation then it can be shown that there exists a unique k-algebra structure on $R[y]$ such that $R \subseteq R[y]$ is a subring and Equation 6.4 holds. This k-algebra is then denoted by $R[y; \delta]$ and is a *skew polynomial ring* or *differential polynomial ring* of R. We already know two examples of skew polynomial rings:

- For $R = k[x]$ and $\delta = 0$ the skew polynomial ring $k[x][y; 0] = k[x, y]$ is just the usual commutative polynomial ring in two variables x, y.
- For $R = k[x]$ and $\delta = \partial$ we have seen above that $k[x][y; \partial]$ is the Weyl algebra $\mathcal{A}$.

In addition to the k-derivation one can also consider a k-algebra homomorphism $\alpha \colon R \to R$: Then a map $\delta \colon R \to R$ is an *α-derivation* if

$$\delta(rs) = \alpha(r)\delta(s) + \delta(r)s$$

for all $r, s \in R$. There then exists a unique k-algebra structure on $R[y]$ such that $R \subseteq R[y]$ is a subring and

$$yr = \alpha(r)y + \delta(r)$$

for every $r \in R$. This k-algebra, which is denoted by $R[y; \alpha, \delta]$, is an *Ore extension* of R. For $\alpha = \mathrm{id}_R$ we retrieve the notion of a skew polynomial ring. Ore extensions, and therefore also skew polynomial rings, inhert properties from the original ring R:

- If R has no zero divisors then $R[y; \alpha, \delta]$ has no zero divisors.
- If R is noetherian and α is an automorphism then $R[y; \alpha, \delta]$ is noetherian. This holds in particular for skew polynomial rings, for which $\alpha = \mathrm{id}$.

An more thorough introduction to skew polynomial rings and Ore extensions can be found in [GW04, § 3]. We can also recommend [Lam91, §1] for a short introduction.

Remark 6.31. Let $\mathrm{char}(k) = 0$. One can more generally consider for every $n \geq 0$ the n-th Weyl algebra $\mathcal{A}_n$, which can be defined in multiple ways:

- The k-algebra $\mathcal{A}_n$ can be defined as the k-algebra of linear differential operators of $k[x_1, \dots x_n]$, i.e. the k-subalgebra of $\mathrm{End}_k(k[x_1, \dots, x_n])$ generated by $\xi_1, \dots, \xi_n$, where ξ_i is the multiplication with x_i, and the partial derivatives $\partial_1, \dots, \partial_n$.
- The k-algebra $\mathcal{A}_n$ can be described by the generators $X_1, \dots, X_n, D_1, \dots, D_n$ and relations

$$\begin{aligned} X_i X_j &= X_j X_i \text{ for all } i, j, & D_i D_j &= D_j D_i \text{ for all } i, j, \\ D_i X_j &= X_j D_i \text{ for all } i \neq j, & D_i X_i &= X_i D_i + 1 \text{ for all } i\,. \end{aligned}$$

- The n-th Weyl algebra $\mathcal{A}_n$ can be constructed from the first Weyl algebra $\mathcal{A}_1$ as the n-fold tensor product $\mathcal{A}_1 \otimes \cdots \otimes \mathcal{A}_1$.
- By defining more generaly the first Weyl algebra $\mathcal{A}_1(R)$ of any k-algebra R, the n-th Weyl algebra $\mathcal{A}_n(R)$ can then inductively be constructed as $\mathcal{A}_n(R) = \mathcal{A}_1(\mathcal{A}_{n-1}(R))$.

7. Polynomial Maps

7.1. In this section we introduce the notion of polynomial maps between (finite-dimensional) vector spaces and show some of their basic properties.

Conventions 7.2. For the rest of this section let k be an infinite field. We denote by V a finite-dimensional k-vector space and by $v_1, \dots, v_n$ a basis of V.

7.1. Polynomial Functions

Definition 7.3. A function $f\colon V \to k$ is *polynomial* if there exists a polynomial $p \in k[X_1, \dots, X_n]$ with

$$f(\lambda_1 v_1 + \cdots + \lambda_n v_n) = p(\lambda_1, \dots, \lambda_n)$$

for all $\lambda_1, \dots, \lambda_n \in k$. The space of polynomial functions $V \to k$ is denoted $\mathcal{P}_k(V)$, or by $\mathcal{P}(V)$ if the field is clear.

Remark 7.4. Other popular notations for $\mathcal{P}(V)$ are $k[V]$, $A(V)$ and $\mathcal{O}(V)$. The k-algebra $\mathcal{P}(V)$ is also known as the *coordinate ring* of V.

7.5. This definition does not depend on the chosen basis. If $(w_1, \dots, w_n)$ is another basis of V with $w_i = \sum_{j=1}^n a_{ij} v_j$ for all $i = 1, \dots, n$ then

$$f\left(\sum_{i=1}^n \lambda_i w_i\right) = f\left(\sum_{i,j=1}^n \lambda_i a_{ij} v_j\right) = p\left(\sum_{i=1}^n \lambda_i a_{i1}, \dots, \sum_{i=1}^n a_{in} \lambda_i\right) = p'(\lambda_1, \dots, \lambda_n)$$

for $p' \in k[X_1, \dots, X_n]$ given by

$$p'(X_1, \dots, X_n) = p\left(\sum_{i=1}^n a_{i1} X_i, \dots, \sum_{i=1}^n a_{in} X_i\right).$$

So if $f\colon V \to k$ is polynomial with respect to the basis $(v_1, \dots, v_n)$, then it is also polynomial with respect to the basis $(w_1, \dots, w_n)$.

This basis independence allows us to simplify problems by choosing the right kind of basis for V. The following result can be seen as consequence of this:

Corollary 7.6. Let $U \subseteq V$ be k-linear subspace. Then for every polynomial function $f\colon V \to k$ the restriction $f|_U\colon U \to k$ is also polynomial.

Proof. Let $v_1, \dots, v_m, v_{n+1}, \dots, v_n$ be a basis of V such that $v_1, \dots, v_m$ is a basis of U. There exist some polynomial $p \in k[X_1, \dots, X_n]$ with

$$f(\lambda_1 v_1 + \cdots + \lambda_n v_n) = p(\lambda_1, \dots, \lambda_n)$$

for all $\lambda_1, \dots, \lambda_n \in k$ because f is polynomial. It follows for the polynomial

$$\bar{p} := p(X_1, \dots, X_m, 0, \dots, 0) \in k[X_1, \dots, X_m]$$

that

$$\begin{aligned} f|_U(\lambda_1 v_1 + \cdots + \lambda_m v_m) &= f(\lambda_1 v_1 + \cdots + \lambda_m v_m) \\ &= p(\lambda_1, \dots, \lambda_m, 0, \dots, 0) = \bar{p}(\lambda_1, \dots, \lambda_m) \end{aligned}$$

for all $\lambda_1, \dots, \lambda_m \in k$. This shows that $f|_U$ is polynomial. □

Example 7.7.

a) Every linear map $f\colon V \to k$ is polynomial: There exists $a_1, \dots, a_n$ with

$$f(\lambda_1 v_1 + \cdots + \lambda_n v_n) = a_1 v_1 + \cdots + a_n v_n$$

for all $\lambda_1, \dots, \lambda_n \in k$, so that for the polynomial

$$p := a_1 X_1 + \cdots + a_n X_n \in k[X_1, \dots, X_n]$$

we have that

$$f(\lambda_1 v_1 + \cdots + \lambda_n v_n) = p(\lambda_1, \dots, \lambda_n)$$

for all $\lambda_1, \dots, \lambda_n \in k$.

b) The determinant function $\det\colon \mathrm{M}_n(k) \to k$ is polynomial:

Let E_{ij}, $i, j = 1, \dots, n$ be the standard basis of $\mathrm{M}_n(k)$. Then for every matrix $A \in \mathrm{M}_n(k)$ with $A = (A_{ij})_{i,j=1,\dots,n}$ we have that $A = \sum_{i,j} a_{ij} E_{ij}$ and

$$\det A = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) A_{1\sigma(1)} \cdots A_{n\sigma(n)} \,.$$

It follows for the polynomial

$$\begin{aligned} p &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) X_{1\sigma(1)} \cdots X_{n\sigma(n)} \\ &\in k[X_{11}, \dots, X_{1n}, X_{21}, \dots, X_{2n}, \dots, X_{n1}, \dots, X_{nn}] \end{aligned}$$

that

$$\det(A_{11}E_{11} + \cdots + A_{nn}E_{nn}) = p(A_{11}, \dots, A_{nn})$$

for all $A_{11}, \dots, A_{nn} \in k$.

7.8. The space $\mathcal{P}(V)$ of polynomial functions $V \to k$ carries the structure of a k-algebra via pointwise addition, scalar multiplication and multiplication. Every polynomial $p \in k[X_1, \dots, X_n]$ leads to a polynomial function $f\colon V \to k$ given by

$$f(\lambda_1 v_1 + \cdots + \lambda_n v_n) \coloneqq p(\lambda_1, \dots, \lambda_n) \,,$$

and resulting map $k[X_1, \dots, X_n] \to \mathcal{P}(V)$ is a homomorphism of k-algebras. It is surjective by the definition of a polynomial function, and injective by the following lemma:

Lemma 7.9. Let $p \in k[X_1, \dots, X_n]$ with $p(\lambda_1, \dots, \lambda_n) = 0$ for all $\lambda_1, \dots, \lambda_n \in k$. Then $p = 0$.

Proof. We show the claim by induction over n. For $n = 0$ there is nothing to do, and for $n = 1$ the claim is known from elementary algebra (note that the field k is infinite).

Let $n \geq 2$. Thanks to the the usual isomorphism

$$k[X_1, \dots, X_n] = k[X_1, \dots, X_{n-1}, X_n] \cong k[X_1, \dots, X_{n-1}][X_n]$$

we may decompose the polynomial p as

$$p(X_1, \dots, X_n) = \sum_{i=0}^{\infty} p_i(X_1, \dots, X_{n-1}) X_n^i$$

with $p_i \in k[X_1, \dots, X_{n-1}]$ for every i and $p_i = 0$ for all but finitely many i. For fixed $\lambda_1, \dots, \lambda_{n-1}$ it follows for the polynomial

$$q(X) \coloneqq p(\lambda_1, \dots, \lambda_{n-1}, X) = \sum_{i=0}^{\infty} p_i(\lambda_1, \dots, \lambda_{n-1}) X^i \in k[X]$$

that $q(\lambda) = 0$ for every $\lambda \in k$. By induction hypothesis it follows that $q = 0$, so that

$$p_i(\lambda_1, \dots, \lambda_{n-1}) = 0$$

for all i. As this holds for all $\lambda_1, \dots, \lambda_{n-1}$ it further follows by induction hypothesis that $p_i = 0$ for every i. This shows that $p = 0$. □

Corollary 7.10. The homomorphism of k-algebras $\Phi\colon k[X_1, \dots, X_n] \to \mathcal{P}(V)$ given by

$$\Phi(p)(\lambda_1 v_1 + \dots + \lambda_n v_n) = p(\lambda_1, \dots, \lambda_n)$$

is an isomorphism of k-algebras.

7.11. In the case of $V = k^n$ one can therefore identify $\mathcal{P}(k^n)$ with $k[X_1, \dots, X_n]$ by using the standard basis $e_1, \dots, e_n$ of k^n. For every polynomial $p \in k[X_1, \dots, X_n]$ the corresponding polynomial function $f\colon k^n \to k$ is then given

$$f(x_1, \dots, x_n) = p(x_1, \dots, x_n)$$

for every $(x_1, \dots, x_n) \in k^n$.

Remark 7.12. Suppose that k is a finite field.

a) Every map $f\colon V \to k$ is polynomial: For every $x = \lambda_1 v_1 + \dots + \lambda_n v_n \in V$ there exists a polynomial function $h_x\colon V \to k$ which vanishes everywhere except at x, namely

$$h_x(\mu_1 v_1 + \dots + \mu_n v_n) = \prod_{\substack{\nu_1 \in K \\ \nu_1 \neq \lambda_1}} (\mu_1 - \nu_1) \cdots \prod_{\substack{\nu_n \in K \\ \nu_n \neq \lambda_n}} (\mu_n - \nu_n)\,.$$

Then the function $\delta_x = h_x / h_x(x)$ satisfies

$$\delta_x(y) = \delta_{x,y}$$

for every $y \in V$, so that f can be expressed as $f = \sum_{x \in X} f(x)\delta_x$.

b) Lemma 7.9 does not hold for finite fields: Suppose that $K = \mathbb{F}_q$ is the field with q elements. Then the nonzero polynomial $f(X) = X^q - X \in K[X]$ vanished everywhere. (To see this note that the group $K^\times$ has order $q - 1$, so that $x^{q-1} = 1$ for every $x \in K$ with $x \neq 0$, and thus $x^q = x$ for every $x \in K$.) Also note that therefore $f(X) = \prod_{\lambda \in K}(X - \lambda)$ by consideration of degrees.

c) We still have the surjective k-algebra homomorphism

$$\Phi\colon k[X_1, \dots, X_n] \to \mathcal{P}(V) = \operatorname{Maps}(V, k)$$

from 7.8 (where the k-algebra structure of $\operatorname{Maps}(V, k)$ is defined pointwise). The kernel of Φ is given by the ideal

$$I := (f(X_1), \dots, f(X_n))\,.$$

By the above discussion we have that $I \subseteq \ker \Phi$. For the other inclusion note that in the case $n = 1$ we have that

$$\dim_k k[X]/f(X) = \deg f(X) = q = |V| = \dim \operatorname{Maps}(V, k)\,,$$

and more generally we have that

$$\begin{aligned} k[X_1, \dots, X_n]/I &= k[X_1, \dots, X_n]/(f(X_1), \dots, f(X_n)) \\ &\cong \biggl(\Bigl(\bigl(k[X_1]/f(X_1) \bigr) [X_2]/f(X_2) \Bigr) \cdots \biggr) [X_n]/f(X_n) \end{aligned}$$

and therefore that

$$\dim_k k[X_1, \dots, X_n]/I = q^n = |V| = \dim_k \operatorname{Maps}(V, k)\,.$$

Remark 7.13. Note that the constructed isomorphism $\Phi\colon k[X_1, \dots, X_n] \to \mathcal{P}(V)$ from Corollary 7.10 depends on the choice of the basis $v_1, \dots, v_n$.

More specifillay, the basis $v_1, \dots, v_n$ is uniquely determined by the isomorphism Φ. To see this note that

$$\Phi(X_i)(\lambda_1 v_1 + \dots + \lambda_n v_n) = \lambda_i$$

for all $i = 1, \dots, n$, $\lambda_1, \dots, \lambda \in K$. Hence the basis vector v_j is the uniquely determined vector $v \in V$ with

$$\Phi(X_i)(v) = \delta_{ij}$$

for all $i = 1, \dots, n$. The basis $v_1, \dots, v_n$ is therefore uniquely determined by the images $\Phi(X_1), \dots, \Phi(X_n)$, which in turn are uniquely determined by Φ.

7.2. Decomposition into Homogeneous Components

7.14. Through the isomorphism $\Phi\colon k[X_1, \dots, X_n] \to \mathcal{P}(V)$ the k-algebra $\mathcal{P}(V)$ inherits the grading of $k[X_1, \dots, X_n]$, making Φ into an isomorphism of graded k-algebras. In the following we will give an alternative construction of the resulting grading of $\mathcal{P}(V)$. This will in particular show that this grading does not depend on the choice of the basis $v_1, \dots, v_n$.

Definition 7.15. Let $d \in \mathbb{N}$. A function $f\colon V \to k$ is *homogeneous of degree d* if $f(\lambda x) = \lambda^d f(x)$ for all $\lambda \in k$, $x \in V$. Let

$$\mathcal{P}(V)_d := \{ f \in \mathcal{P}(V) \mid f \text{ is homogeneous of degree } d \}\,.$$

7.16. For every homogeneous polynomial $p \in k[X_1, \dots, X_n]$ of degree d the corresponding polynomial function $\Phi(p)\colon V \to k$ is homogeneous of degree d, as can be checked on monomials. This connection between homogeneous polynomials and homogeneous polynomial functions leads to the following result:

Lemma 7.17.

a) For every $d \in \mathbb{N}$ the set of homogeneous polynomials maps $\mathcal{P}(V)_d \subseteq \mathcal{P}(V)$ is a k-linear subspace.

b) Every polynomial function $f \colon V \to k$ can be written as a sum of homogeneous polynomial functions $f_d \in \mathcal{P}_d(V)$.

c) The k-linear subspaces $\mathcal{P}(V)_d$ with $d \in \mathbb{N}$ of $\mathcal{P}(V)$ are linearly independent (i.e. the sum $\sum_{d \in \mathbb{N}} \mathcal{P}_d(V)$ is direct).

d) For all $i, j \in \mathbb{N}$ one has for all $f \in \mathcal{P}(V)_i$ and $g \in \mathcal{P}(V)_j$ that $fg \in \mathcal{P}(V)_{i+j}$.

Proof.

a) For all $f_1, f_2 \in \mathcal{P}(V)_d$ we have that

$$\begin{aligned}(f_1 + f_2)(\lambda v) &= f_1(\lambda v) + f_2(\lambda v) = \lambda^d f_1(v) + \lambda^d f_2(v) \\ &= \lambda^d (f_1(v) + f_2(v)) = \lambda^d (f_1 + f_2)(v)\end{aligned}$$

for all $\lambda \in k$, $v \in V$, so that $f_1 + f_2 \in \mathcal{P}(V)_d$. For all $f \in \mathcal{P}(V)$, $\mu \in k$ we have that

$$(\mu f)(\lambda v) = \mu f(\lambda v) = \lambda^d \mu f(v) = \lambda^d (\mu f)(v)$$

for all $\lambda \in k$, $v \in V$, so that $\mu f \in \mathcal{P}(V)_d$.

b) There exists a polynomial $p \in k[X_1, \dots, X_n]$ with $f = \Phi(p)$. Then p can be written as a sum $p = \sum_{d \in \mathbb{N}} p_d$ where p_d is homogeneous of degree d, with $p_d = 0$ for all but finitely many $d \in \mathbb{N}$. It follows for $f_d \coloneqq \Phi(p_d)$ from 7.16 that f_d is homogeneous of degree d. The claim follows because

$$\Phi(p) = \Phi\left(\sum_{d \in \mathbb{N}} p_d\right) = \sum_{d \in \mathbb{N}} \Phi(p_d) = \sum_{d \in \mathbb{N}} f_d \,.$$

c) Let $m \geq 0$ and $f_0 \in \mathcal{P}(V)_0, \dots, f_m \in \mathcal{P}(V)_m$ with $\sum_{d=0}^m f_d = 0$. We fix some $x \in V$ and show that $f_d(x) = 0$ for every $d = 0, \dots, m$.

For every $\lambda \in k$ we have that

$$0 = \sum_{d=0}^{m} f_d(\lambda x) = \sum_{d=0}^{m} \lambda^d f_d(x) \,.$$

It follows for pairwise different $\lambda_0, \dots, \lambda_m \in k$ that

$$\begin{bmatrix} 1 & \lambda_0 & \lambda_0^2 & \cdots & \lambda_0^m \\ 1 & \lambda_1 & \lambda_1^2 & \cdots & \lambda_1^m \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \lambda_m & \lambda_m^1 & \cdots & \lambda_m^m \end{bmatrix} \begin{bmatrix} f_0(x) \\ f_1(x) \\ \vdots \\ f_m(x) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

The matrix on the left is invertible as it is the Vandermonde matrix of the values $\lambda_1, \dots, \lambda_n$, and has therefore determinant $\prod_{i>j} (\lambda_i - \lambda_j)$. It follows that $f_0(x) = \cdots = f_m(x) = 0$, as desired.

d) For all $\lambda \in k$, $v \in V$ we have that

$$(fg)(\lambda v) = f(\lambda v)g(\lambda v) = \left(\lambda^i f(v)\right)\left(\lambda^j g(v)\right) = \lambda^{i+j} f(v)g(v) = \lambda^{i+j}(fg)(v)\,,$$

and therefore $fg \in \mathcal{P}(V)_{i+j}$. □

Corollary 7.18. The k-algebra $\mathcal{P}(V)$ has a grading given by $\mathcal{P}(V) = \bigoplus_{d\in\mathbb{N}} \mathcal{P}(V)_d$.

7.19. Note that for the isomorphism Φ we have that $\Phi(k[X_1,\dots,X_n]_d) \subseteq \mathcal{P}(V)_d$ for every $d \in \mathbb{N}$ by 7.16. Thus Φ is an isomorphism of graded k-algebras. It follows that the constructed grading of $\mathcal{P}(V)$ coincides with the one inherited under Φ. This shows, as claimed in 7.14, that this grading does not depend on the choice of the basis $v_1,\dots,v_n$.

7.3. Polynomial Maps between Vector Spaces

7.20. So far we have only considered polynomial functions $V \to k$. In the following we will generalize this to the notion of *polynomial maps* $V \to W$ between finite-dimensional k-vector spaces V and W.

Conventions 7.21. In the following U, V, W will denote finite-dimensional k-vector spaces.

Definition 7.22. A map

$$f\colon V \to W$$

is *polynomial* if the coordinate functions of f with respect to a basis $w_1,\dots,w_m$ of W are polynomial, i.e. if the functions $f_1,\dots,f_m\colon V \to k$ with

$$f(v) = \sum_{i=1}^{m} f_i(v) w_i$$

for every $v \in V$ are polynomial. The space of polynomial maps $V \to W$ is denoted by

$$\operatorname{Pol}_k(V,W) \coloneqq \{f\colon V \to W \mid f \text{ is a polynomial}\}\,,$$

or just by $\operatorname{Pol}(V,W)$.

Remark 7.23. One can show as for $\mathcal{P}(W)$ that this definition does not depend on the choice of the basis of W. From Corollary 7.6 it follows for every polynomial map $f\colon V \to W$ that the restriction $f|_U$ to any k-linear subspace $U \subseteq V$ is again polynomial.

Example 7.24. Let $v_1,\dots,v_n$ be a basis of V, and let $w_1,\dots,w_m$ be a basis of W.

a) We have that $\operatorname{Pol}(V,k) = \mathcal{P}(V)$.

b) Every linear map $f\colon V \to W$ is polynomial: There exist k-valued functions $f_1,\dots,f_m\colon V \to k$ with

$$f(v) = f_1(v)w_1 + \dots + f_m(v)w_m$$

for every $v \in V$, and all of the f_i are linear by the linearity of f. It follows that the f_i are polynomial, as seen in Example 7.7.

c) For every $r \geq 0$ the map

$$f\colon V \to V^{\otimes r}, \quad v \mapsto v \otimes \cdots \otimes v$$

is polynomial. To see this we choose a basis $v_1, \dots, v_n$ of V. Then the elements

$$v_{\boldsymbol{i}} = v_{i_1} \otimes \cdots \otimes v_{i_r} \quad \text{with} \quad \boldsymbol{i} = (i_1, \dots, i_r) \in \{1, \dots, n\}^r$$

form a basis of $V^{\otimes r}$. For $v \in V$ with $v = \sum_{i=1}^r \lambda_i v_i$ we have that

$$f(v) = v \otimes \cdots \otimes v = \left(\sum_{i=1}^r \lambda_i v_i \right) \otimes \cdots \otimes \left(\sum_{i=1}^r \lambda_i v_i \right) = \sum_{\boldsymbol{i}} \lambda_{i_1} \cdots \lambda_{i_r} v_{\boldsymbol{i}} \,.$$

For the polynomials $p_{\boldsymbol{i}} \coloneqq X_{i_1} \cdots X_{i_r}$ and their corresponding polynomial maps $f_{\boldsymbol{i}}\colon V \to k$ given by

$$f_{\boldsymbol{i}}\left(\lambda_1 v_1 + \cdots + \lambda_n v_n\right) = p_{\boldsymbol{i}}(\lambda_1, \dots, \lambda_r)$$

we thus have that $f(v) = \sum_{\boldsymbol{i}} f_{\boldsymbol{i}}(v) v_{\boldsymbol{i}}$ for every $v \in V$.

Lemma 7.25.

a) The identity map $\mathrm{id}_V\colon V \to V$ is polynomial.

b) For any two composable polynomial maps $f\colon U \to V$ and $g\colon V \to W$ their composition $g \circ f$ is also composable.

Proof.

a) The identity id_V is linear, and therefore polynomial.

b) Let $u_1, \dots, u_r$ be a basis of U, let $v_1, \dots, v_s$ be a basis of V, and let $w_1, \dots, w_t$ be a basis of W. Because the map $f\colon U \to V$ is polynomial there exist polynomials $p_1, \dots, p_s \in k[X_1, \dots, X_r]$ such that

$$f(\lambda_1 u_1 + \cdots + \lambda_r u_r) = \sum_{i=1}^s p_i(\lambda_1, \dots, \lambda_r) v_i \,,$$

and because the g polynomial we can find polynomials $q_1, \dots, q_t \in k[X_1, \dots, X_s]$ such that

$$g(\mu_1 w_1 + \cdots + \mu_s w_s) = \sum_{j=1}^t q_j(\mu_1, \dots, \mu_s) w_j \,.$$

By combining these two formulas we find that

$$(g \circ f)(\lambda_1 u_1 + \cdots + \lambda_r u_r) = g\left(\sum_{i=1}^s p_i(\lambda_1, \dots, \lambda_r) v_i \right)$$

$$= \sum_{j=1}^t q_j(p_1(\lambda_1, \dots, \lambda_r), \dots, p_s(\lambda_1, \dots, \lambda_r)) w_j = \sum_{j=1}^t r_j(\lambda_1, \dots, \lambda_r) w_j$$

for the polynomials

$$r_j \coloneqq q_j(p_1(X_1, \dots, X_r), \dots, p_s(X_1, \dots, X_r)) \in k[X_1, \dots, X_r]\,.$$

This shows that $g \circ f$ is again polynomial. □

Remark 7.26. It follows that the class of finite-dimensional k-vector spaces together with the polynomial maps between them form a category. We will denote this category by k-**pol**. Note that $\mathrm{Hom}_{k\text{-}\mathbf{pol}}(W, V) = \mathrm{Pol}_k(W, V)$ for all finite-dimensional k-vector spaces V and W. Note also that k-**vect** is a subcategory of k-**pol** since every linear map between finite-dimensional vector spaces is polynomial.

Proposition 7.27.

a) The space $\mathrm{Pol}_k(V, W)$ of polynomial maps $V \to W$ carries the structure of a k-vector space via pointwise addition and scalar multiplication.

b) The k-vector space $\mathrm{Pol}_k(V, W)$ carries the structur of a $\mathcal{P}_k(V)$-module via

$$(g \cdot f)(v) = g(v) f(v) \tag{7.1}$$

for all $g \in \mathcal{P}_k(V)$, $f \in \mathrm{Pol}_k(V, W)$, $v \in V$.

Proof.

a) The space $\mathrm{Maps}(V, W)$ carries the structure of a k-vector space via pointwise addition und scalar multiplication. Then $\mathrm{Pol}_k(V, W)$ is a k-linear subspace of $\mathrm{Maps}(V, W)$ as sums and scalar multiplices of polynomial maps are again polynomial.

b) The k-vector space $\mathrm{Maps}(V, W)$ becomes a $\mathrm{Maps}(V, k)$-module by defining the multiplication via (7.1). Then $\mathcal{P}(V)$ is a k-subalgebra of $\mathrm{Maps}(V, k)$, so that $\mathrm{Maps}(V, W)$ becomes a $\mathcal{P}(V)$-module by restriction. The proposition claims that $\mathrm{Pol}_k(V, W)$ is a $\mathcal{P}(V)$-submodule of $\mathrm{Maps}(V, W)$. It now sufficies to show that $\mathrm{Pol}_k(V, W)$ is preserved under the action of $\mathcal{P}_k(V)$ on $\mathrm{Maps}(V, W)$.

   Let $w_1, \dots, w_m$ be a basis of W. For every $f \in \mathrm{Pol}_k(V, W)$ there then exist $f_1, \dots, f_m \in \mathcal{P}_k(V)$ with

$$f(v) = f_1(v) w_1 + \cdots + f_m(v) w_m$$

   for all $v \in V$. Then

$$\begin{aligned} (g \cdot f)(v) &= g(v) \cdot f(v) \\ &= g(v) \cdot (f_1(v) w_1 + \cdots + f_m(v) w_m) \\ &= g(v) f_1(v) w_1 + \cdots + g(v) f_m(v) w_m \\ &= (g f_1)(v) w_1 + \cdots + (g f_m)(v) w_m \end{aligned}$$

   for all $v \in V$, with $g f_1, \dots, g f_m \in \mathcal{P}(V)$. So $g \cdot f$ is again polynomial. □

Lemma 7.28. Let $f\colon V \to W$ be a polynomial map. Then

$$f^*\colon \mathcal{P}(W) \to \mathcal{P}(V), \quad h \mapsto h \circ f$$

is a homomorphism of k-algebras.

Proof. The map f^* is well-defined as the composition of polynomial maps is again polynomial. To show that f is a homomorphism of k-algebras let $h, h_1, h_2 \in \mathcal{P}(W)$. For every $v \in V$ we have that

$$\begin{aligned} f^*(h_1 + h_2)(v) &= (h_1 + h_2)(f(v)) = h_1(f(v)) + h_2(f(v)) \\ &= f^*(h_1)(v) + f^*(h_2)(v) = (f^*(h_1) + f^*(h_2))(v) \end{aligned}$$

and therefore

$$f^*(h_1 + h_2) = f^*(h_1) + f^*(h_2)\,.$$

For all $\lambda \in k$, $v \in V$ we have that

$$f^*(\lambda h)(v) = (\lambda h)(f(v)) = \lambda h(f(v)) = \lambda f^*(h)(v) = (\lambda f^*(h))(v)$$

and therefore

$$f^*(\lambda h) = \lambda f^*(h)\,.$$

Together this shows that f^* is k-linear. For every $v \in V$ we have that

$$\begin{aligned} f^*(h_1 h_2)(v) &= (h_1 h_2)(f(v)) = h_1(f(v)) h_2(f(v)) \\ &= f^*(h_1)(v)\, f^*(h_2)(v) = (f^*(h_1) f^*(h_2))(v) \end{aligned}$$

and therefore

$$f^*(h_1 h_2) = f^*(h_1) f^*(h_2)\,.$$

This shows that f^* is multiplicative. We also have that

$$f^*\left(1_{\mathcal{P}(W)}\right) = 1_{\mathcal{P}(W)} \circ f = 1_{\mathcal{P}(V)}\,.$$

Altogether this shows that f^* is a homomorphism of k-algebras. □

Definition 7.29. For every polynomial map $f\colon V \to W$ the homomorphism of k-algebras $f^*\colon \mathcal{P}(W) \to \mathcal{P}(V)$ is the *comorphism associated with* f.

Lemma 7.30.

a) For the identity id_V we have that $\mathrm{id}_V^* = \mathrm{id}_{\mathcal{P}(V)}$.

b) For every two composable polynomial maps $f\colon U \to V$ and $g\colon V \to W$ we have that $(g \circ f)^* = f^* \circ g^*$.

7.31. We have associated to every finite-dimensional k-vector space V a k-algebra $\mathcal{P}(V)$, and to any polynomial map $f\colon V \to W$ an associated homomorphism of k-algebras $f^*\colon \mathcal{P}(W) \to \mathcal{P}(V)$. This association is functorial by Lemma 7.30. We have therefore constructed a contravariant functor $\mathcal{P}\colon k\text{-}\mathbf{pol} \to k\text{-}\mathbf{Alg}$ which is given on objects by $V \mapsto \mathcal{P}(V)$ and on morphisms by $f \mapsto f^*$.

This functor turns out to be fully faithful:

Proposition 7.32. The map

$$\operatorname{Pol}_k(V, W) \to \operatorname{Hom}_{k\text{-}\mathbf{Alg}}(\mathcal{P}(W), \mathcal{P}(V)), \quad f \mapsto f^*$$

is bijective.

Proof. Let $w_1, \dots, w_m$ be a k-basis of W and let $\psi_1, \dots, \psi_m \in \mathcal{P}(W)$ be the corresponding coordinate functions.

For every k-algebra homomorphism $F \colon \mathcal{P}(W) \to \mathcal{P}(V)$ we set $F_j^\circ := F(\psi_j) \in \mathcal{P}(V)$ for every $j = 1, \dots, m$. Then

$$F^\circ \colon V \to W, \quad v \mapsto F_1^\circ(v) w_1 + \dots + F_m^\circ(v) w_m$$

is a polynomial map $F^\circ \colon V \to W$.

Let $f \colon V \to W$ be a polynomial map and let $f_1, \dots, f_m \in \mathcal{P}(V)$ be the coordinates of f with respect to the basis $w_1, \dots, w_n$ of W, i.e. let $f_1, \dots, f_m \colon V \to k$ such that

$$f(v) = f_1(v) w_1 + \dots + f_m(v) w_m$$

for every $v \in V$. For $F := f^*$ we then have that

$$F_j^\circ = F(\psi_j) = f^*(\psi_j) = \psi_j \circ f = f_j$$

for every $j = 1, \dots, m$ and therefore $(f^*)^\circ = F^\circ = f$.

Let $F \colon \mathcal{P}(W) \to \mathcal{P}(V)$ be a homomorphism of k-algebras, and set $f := F^\circ$. Then

$$f^*(\psi_j) = \psi_j \circ f = \psi_j \circ F^\circ = F_j^\circ = F(\psi_j)$$

for every $j = 1, \dots, m$. The k-algebra $\mathcal{P}(V)$ is generated by the coordinate functions $\psi_1, \dots, \psi_m$ as a k-algebra, so it follows that $(F^\circ)^* = f^* = F$.

This shows that $(-)^*$ and $(-)^\circ$ are mutually inverse bijections. □

Remark 7.33. Proposition 7.32 shows that the functor $\mathcal{P} \colon k\text{-}\mathbf{pol} \to k\text{-}\mathbf{Alg}$ is a contravariant embedding. It follows that the category k-**pol** is dual to a full category of k-**Alg**. By Corollary 7.10 the corresponding strictly full subcategory of k-**Alg** consists precisely of those k-algebras which are isomorphic a polynomial ring over k in finitely many variables.

8. Covariants

8.1. Let G be a group acting on a set X Then G acts on linearly on $\operatorname{Maps}(X, k)$ via

$$(g.f)(x) := f(g^{-1}.x)$$

for all $g \in G$, $f \in \operatorname{Maps}(X, k)$, $x \in X$.

If G acts linearly on a finite-dimensional k-vector space V then it follows that G acts linearly on $\operatorname{Maps}(V, k)$ in the above way. The k-linear subspace $\mathcal{P}(V) \subseteq \operatorname{Maps}(V, k)$ is then a subrepresentation (because the precomposition of a polynomial function by a linear function is again polynomial).

This shows that the linear action of G on V induces a linear action of G on $\mathcal{P}(V)$ given by $(g.f)(v) = f(g^{-1}.v)$. Note that this is already an action by k-algebra automorphisms because additionaly

$$\begin{aligned}(g.(f_1 f_2))(v) &= (f_1 f_2)(g^{-1}.v) = f_1(g^{-1}.v) f_2(g^{-1}.v) \\ &= (g.f_1)(v)\,(g.f_2)(v) = ((g.f_1)(g.f_2))(v)\end{aligned}$$

for every $v \in V$, and thus $g.(f_1 f_2) = (g.f_1)(g.f_2)$, as well as

$$\left(g.1_{\mathcal{P}(V)}\right)(v) = 1_{\mathcal{P}(V)}(g^{-1}.v) = 1$$

for every $v \in V$, and thus $g.1_{\mathcal{P}(V)} = 1_{\mathcal{P}(V)}$. It follows in particular that $\mathcal{P}(V)^G$ is a k-subalgebra of $\mathcal{P}(V)$.

Conventions 8.2. In the following, U, V, W will denote finite-dimensional representations of a group G over an infinite field k.

Definition 8.3. A map $f\colon V \to W$ is *covariant* if it is both polynomial and G-equivariant. The space of covariant functions $V \to W$ is denoted by $\operatorname{Cov}_k(V, W)$, or just by $\operatorname{Cov}(V, W)$.

Example 8.4.

a) For every $r \geq 0$ the map

$$\beta\colon V \to V^{\otimes r}, \quad v \mapsto v \otimes \cdots \otimes v$$

is polynomial, as seen in Example 7.24. It is also G-equivariant since

$$\beta(g.v) = (g.v) \otimes \cdots \otimes (g.v) = g.(v \otimes \cdots \otimes v) = g.\beta(v)$$

for all $g \in G$, $v \in W$.

b) The group $\mathrm{GL}_n(k)$ on $\mathrm{M}_n(k)$ via conjugation, i.e. via

$$g.A := gAg^{-1}$$

for all $g \in \mathrm{GL}_n(k)$, $A \in \mathrm{M}_n(k)$. Then the map

$$\beta_i\colon \mathrm{M}_n(k) \to \mathrm{M}_n(k), \quad A \mapsto A^i$$

is covariant for every $i \geq 1$.

8.5. We know that $\operatorname{Maps}(V, W)$ is a G-set via

$$(g.f)(v) = g.f\left(g^{-1}.v\right) \tag{8.1}$$

for all $g \in G$, $v \in V$. As in 8.1 we find that $\operatorname{Pol}(V,W) \subseteq \operatorname{Maps}(V,W)$ is a subrepresentation. Thus G acts linearly on $\operatorname{Pol}(V,W)$ via (8.1).

Note that it follows in particular that $\operatorname{Cov}(V,W) = \operatorname{Pol}_k(V,W)^G$ is a k-linear subspace of $\operatorname{Pol}_k(V,W)$.

Let $\beta\colon V \to W$ be a covariant map. Then the induced k-algebra homomorphism $\beta^*\colon \mathcal{P}(W) \to \mathcal{P}(V)$ is also G-equivariant because

$$\begin{aligned}(g.\beta^*(f))(v) &= \beta^*(f)(g^{-1}.v) = f(\beta(g^{-1}.v)) \\ &= f(g^{-1}.\beta(v)) = (g.f)(\beta(v)) = \beta^*(g.f)(v)\end{aligned}$$

for all $g \in G$, $f \in \mathcal{P}(W)$, $v \in V$, and therefore $g.\beta^*(f) = \beta^*(g.f)$ for all $g \in G$, $f \in \mathcal{P}(W)$. It follows that $\beta^*(\mathcal{P}(W)^G) \subseteq \mathcal{P}(V)^G$, so that β^* restricts to a k-algebra homomorphism $\mathcal{P}(W)^G \to \mathcal{P}(V)^G$.

Proposition 8.6. The $\mathcal{P}(V)$-module structure of $\operatorname{Pol}(V,W)$ restrict to a $\mathcal{P}(V)^G$-module structure on $\operatorname{Cov}(V,W)$ by restriction.

Proof. The $\mathcal{P}(V)$-module structure of $\operatorname{Pol}(V,W)$ restricts to a $\mathcal{P}(V)^G$-module structure. We thus need to show that $\operatorname{Cov}(V,W)$ is preserved under the action of $\mathcal{P}(V)^G$.

We already know that $\operatorname{Cov}(W,V)$ is a k-linear subspace of $\operatorname{Pol}_k(W,V)$. For all $f \in \mathcal{P}(W)^G$, $\beta \in \operatorname{Cov}(W,V)$ we have for all $g \in G$, $v \in V$ that

$$\begin{aligned}(g.(f \cdot \beta))(v) &= g.\left((f \cdot \beta)\left(g^{-1}.v\right)\right) = g.\left(f\left(g^{-1}.v\right) \cdot \beta\left(g^{-1}.v\right)\right) \\ &= f\left(g^{-1}.v\right) \cdot \left(g.\beta\left(g^{-1}.v\right)\right) = (g.f)(v) \cdot (g.\beta)(v) \\ &= f(v) \cdot \beta(v) = (f \cdot \beta)(v)\,,\end{aligned}$$

where we used in the second to last equality that $g.f = f$ and $g.\beta = \beta$ (note that $\beta \in \operatorname{Cov}(V,W)$ is G-equivariant, und thus G-invariant). This shows the claim. □

Symmetric Polynomials

9. The Fundamental Theorem of Symmetric Functions

Conventions 9.1. We fix a number of variables $n \in \mathbb{N}$.

9.2. The symmetric group S_n acts by k-algebra automorphisms on the polynomial ring $k[X_1, \dots, X_n]$ by

$$\sigma.f(X_1, \dots, X_n) = f(X_{\sigma(1)}, \dots, X_{\sigma(n)}) .$$

In this section we will be concerned by the k-algebra of invariants $k[X_1, \dots, X_n]^{S_n}$.

Definition 9.3. Let k be a field. The polynomial $f \in k[X_1, \dots, X_n]^{S_n}$ are *symmetric*, and $k[X_1, \dots, X_n]^{S_n}$ is the *ring of symmetric polynomials* (*in n variables*) (*over k*).

Example 9.4. In $k[X_1, X_2, X_3]$ we have the symmetric polynomials

$$\begin{aligned} p_2 &\coloneqq X_1^2 + X_2^2 + X_3^2 , \\ h_2 &\coloneqq X_1^2 + X_1X_2 + X_1X_3 + X_2^2 + X_2X_3 + X_3^2 , \\ e_2 &\coloneqq X_1X_2 + X_1X_3 + X_2X_3 , \\ m_{(4,4,2)} &\coloneqq X_1^4X_2^2X_3^2 + X_1^2X_2^4X_3^2 + X_1^2X_2^2X_3^4 . \end{aligned}$$

In the next subsections we will generalize these examples.

Lemma 9.5. With respect to the usual grading $k[X_1, \dots, X_n] = \bigoplus_{d \in \mathbb{N}} k[X_1, \dots, X_n]_d$ a polynomial $f \in k[X_1, \dots, X_n]$ is symmetric if and only if all of its homogeneous parts are symmetric.

Proof. The decomposition $k[X_1, \dots, X_n] = \bigoplus_{d \geq 0} k[X_1, \dots, X_n]_d$ is a decomposition into subrepresentations of S_n, thus the claim follows from Lemma 2.13. □

9.6. In the following subsections we will consider families of symmetric polynomials which generalize the polynomials given in Example 9.4.

We will start off with the so called *elemantary symmetric polynomials*. We prove the famous *fundamental theorem of symmetric functions*, which roughly states that every every symmetric polynomial can be uniquely expressed in terms of the elementary symmetric polynomials.

We will then use the elementary symmetric polynomials to study other kinds of symmetric polynomials: Namely the *complete homogeneous symmetric polynomials*, *power sums monomial symmetric polynomials*. Along the way we will also introduce *partitions* as a natural way for labeling these different kinds of symmetric polynomials.

Definition 9.7. For all $r \in \mathbb{N}$ the *r-th elementary symmetric polynomial* (in n variables) is

$$e_r \coloneqq \sum_{1 \leq i_1 \leq \cdots \leq i_r \leq n} X_{i_1} \cdots X_{i_r} = \sum_{\substack{I \subseteq \{1,\dots,n\} \\ |I|=r}} \prod_{i \in I} X_i \,.$$

In particular $e_0 = 1$ and $e_r = 0$ for every $r > n$.

9.8. For all $a_1, \dots, a_n \in k$ we have that

$$\begin{aligned} &(t-a_1)\cdots(t-a_n) \\ &= t^n - (a_1 + \cdots + a_n)t^{n-1} + \left(\sum_{1 \leq i_1 < i_2 \leq n} a_{i_1} a_{i_2} \right) t^{n-2} + \cdots + (-1)^n a_1 \cdots a_n \\ &= t^n - e_1(a_1, \dots, a_n)t^{n-1} + e_2(a_1, \dots, a_n)t^{n-2} - \cdots + (-1)^n e_n(a_1, \dots, a_n) \end{aligned}$$

in $k[t]$. We will formalize this observation in the following lemma:

Lemma 9.9. For all $n \in \mathbb{N}$ we have in $k[X_1, \dots, X_n][t]$ the equality

$$\begin{aligned} \prod_{i=1}^n (t - X_i) &= e_0 t^n - e_1 t^{n-1} + e_2 t^{n-2} - \cdots + (-1)^n e_n \\ &= t^n - e_1 t^{n-1} + e_2 t^{n-2} - \cdots + (-1)^n e_n \end{aligned}$$

Proof. On both sides the r-th coefficient is given by $\prod_{I \subseteq \{1,\dots,n\}, |I|=r} \prod_{i \in I} X_i$. □

Theorem 9.10 (Fundamental theorem of symmetric functions)**.** The symmetric polynomials $e_1, \dots, e_n$ generate the k-algebra of symmetric functions $k[X_1, \dots, X_n]^{S_n}$ and are algebraically independent, i.e. the unique k-algebra homomorphism

$$k[Y_1, \dots, Y_n] \to k[X_1, \dots, X_n]^{S_n} \,, \quad Y_r \mapsto e_r$$

is an isomorphism of k-algebras.

9.11. We will give two proofs of the fundamental theorem. The one given in the lecture is the second one.

First proof of the fundamental theorem. We introduce an ordering on the set monomials in $k[X_1, \dots, X_n]$. For this we first order the monomials by their power of X_1 in decreasing order. The monomials with the same power of X_1 are then ordered in decreasing order by their power of X_2. We then continue this process trough the variables $X_3, \dots, X_n$.

For any two monomials $X^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ and $X^\beta = X_1^{\beta_1} \cdots X_n^{\beta_n}$ we thus have $X^\alpha > X^\beta$ if and only if there exists some $1 \leq i \leq n$ such that $\alpha_j = \beta_j$ for all $j < i$ and $\alpha_i > \beta_i$. This gives a well-ordering on the set of monomials in $k[X_1, \dots, X_n]$.

For any polynomial $p \in k[X_1, \dots X_n]$ with $p \neq 0$ we define the initial term $\operatorname{init} p$ to be the highest monomial occuring in p, including its coefficient. Then the following properties hold:

- If $p \neq 0$ is symmetric then for $\operatorname{init} p = cX_1^{\alpha_1} \cdots X_n^{\alpha_n}$ one has $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n$.
- For $p, q \in k[X_1, \dots, X_n]$ with $p, q \neq 0$ one has $\operatorname{init}(p \cdot q) = \operatorname{init} p \cdot \operatorname{init} q$.
- For all $1 \leq k \leq n$ one has $\operatorname{init} e_k = X_1 \cdots X_k$.

With this we are now well-equipped to prove the theorem:

We first show that $e_1, \dots, e_n$ generate $k[X_1, \dots, X_n]^{S_n}$ as a k-algebra. For this let $f \in k[X_1, \dots, X_n]^{S_n}$ with $f \neq 0$. By Lemma 9.5 we may assume that f is homogeneous of degree $d \geq 0$. For

$$\operatorname{init} f = cX_1^{\alpha_1} \cdots X_n^{\alpha_n}$$

we then have $d = \alpha_1 + \cdots + \alpha_n$.

We consider the polynomial

$$p = ce_1^{\alpha_1 - \alpha_2} \cdots e_{n-1}^{\alpha_{n-1} - \alpha_n} e_n^{\alpha_n} .$$

Then $\operatorname{init} p = \operatorname{init} f$ by the above properties of init. Because e_k is homogenous of degree k it follows that p is homogeneous of degree

$$\begin{aligned} &(\alpha_1 - \alpha_2) + 2(\alpha_2 - \alpha_3) + \cdots + (n-1)(\alpha_{n-1} - \alpha_n) + n\alpha_n \\ =&\alpha_1 + \cdots + \alpha_n = d\,. \end{aligned}$$

Combining these observations we find that $f - p$ is a homogeneous symmetric polynomial of degree d with either $f - p = 0$ or at least $\operatorname{init}(f - p) < \operatorname{init} f$.

Because there are only finitely many monomials of homogeneous degree d we can repeat the above process to arrive at the zero polynomial in finitely many steps. Hence f can be expressed as a poylynomial in $e_1, \dots, e_n$.

To show that $e_1, \dots, e_n$ are algebraically independent we need to show that the monomials in $e_1, \dots, e_n$, i.e. the polynomials

$$e^{\boldsymbol{\alpha}} = e_1^{\alpha_1} \cdots e_n^{\alpha_n} \quad \text{for} \quad \boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$$

are linearly independent. For this we notice that for all $\boldsymbol{\alpha} \neq \boldsymbol{\beta}$ we have that

$$\begin{aligned} \operatorname{init} e^{\boldsymbol{\alpha}} &= \operatorname{init} e_1^{\alpha_1} \cdots e_n^{\alpha_n} \\ &= X_1^{\alpha_1 + \cdots + \alpha_n} X_2^{\alpha_2 + \cdots + \alpha_n} \cdots X_n^{\alpha_n} \\ &\neq X_1^{\beta_1 + \cdots + \beta_n} X_2^{\beta_2 + \cdots + \beta_n} \cdots X_n^{\beta_n} \\ &= \operatorname{init} e_1^{\beta_1} \cdots e_n^{\beta_n} = \operatorname{init} e^{\boldsymbol{\beta}} \end{aligned}$$

so that the polynomials $e^{\boldsymbol{\alpha}}$ for $\boldsymbol{\alpha} \in \mathbb{N}^n$ are pairwise different.

Now suppose that

$$0 = \lambda_1 e^{\boldsymbol{\alpha}_1} + \cdots + \lambda_s e^{\boldsymbol{\alpha}_s}$$

with $s \geq 1$, $\boldsymbol{\alpha}_i \neq \boldsymbol{\alpha}_j$ for $i \neq j$ and $\lambda_i \neq 0$ for all $1 \leq i \leq s$. We can assume w.l.o.g. that

$$\operatorname{init} e^{\boldsymbol{\alpha}_1} > \operatorname{init} e^{\boldsymbol{\alpha}_2} > \cdots > \operatorname{init} e^{\boldsymbol{\alpha}_s}$$

since all of these terms are pairwise different. It follows that the initial term $\operatorname{init} e^{\boldsymbol{\alpha}_1}$ occures only in $e^{\boldsymbol{\alpha}_1}$ and in no ther of the $e^{\boldsymbol{\alpha}_i}$. From $\lambda_1 = 0$, in contradiction to $\lambda_1 \neq 0$. □

Second proof of the fundamental theorem. We denote the r-th elementary symmetric polynomial in n variables by $e_r^{(n)}$. Note that

$$\begin{aligned} e_r^{(n)} &= \sum_{\substack{I \subseteq \{1,\dots,n\} \\ |I|=r}} \prod_{i \in I} X_i \\ &= \sum_{\substack{I \subseteq \{1,\dots,n-1\} \\ |I|=r}} \prod_{i \in I} X_i + \sum_{\substack{I \subseteq \{1,\dots,n\} \\ |I|=r-1}} \left(\prod_{i \in I} X_i \right) X_n \qquad (9.1) \\ &= e_r^{(n-1)} + e_{r-1}^{(n)} X_n \,. \end{aligned}$$

Claim. A polynomial $f \in k[X_1, \dots, X_n]$ is symmetric if and only if f can be written as a polyonmial in $e_1^{(n)}, \dots, e_n^{(n)}$, i.e. we have that

$$k\left[e_1^{(n)}, \dots, e_n^{(n)}\right] = k[X_1, \dots, X_n]^{S_n} \,.$$

Proof of claim. Because the polynomials $e_1^{(n)}, \dots, e_n^{(n)} \in k[X_1, \dots, X_n]^{S_n}$ are symmetric it follows that $k[e_1^{(n)}, \dots, e_n^{(n)}] \subseteq k[X_1, \dots, X_n]^{S_n}$. We show the other inclusion by induction over n. For $n = 1$ we have that $k[e_1^{(1)}] = k[X_1] = k[X_1]^{S_1}$.

Let $n \geq 2$ and suppose that the claim holds for $n-1$. We show the claim for n by induction over the (total) degree $d \coloneqq \deg f$. If f is constant than the claim holds. So let $d \geq 1$ and suppose the claim holds for degrees $0, \dots, d-1$. By the Lemma 9.5 we may assume that f is homogenous. (The homogenous parts of lower degree are by induction hypothesis expressable as polynomials in $e_1^{(n)}, \dots, e_n^{(n)}$.)

Let

$$\Phi\colon k[X_1, \dots, X_n] \to k[X_1, \dots, X_{n-1}] \,, \quad f(X_1, \dots, X_n) \mapsto f(X_1, \dots, X_{n-1}, 0)$$

be the evaluation at $X_n = 0$. By (9.1) we have that

$$\begin{aligned} \Phi\left(e_r^{(n)}\right) &= e_r^{(n-1)} \quad \text{for all } 1 \leq r < n \,, \\ \Phi\left(e_n^{(n)}\right) &= 0 \,. \end{aligned}$$

Note that $\Phi(f) \in k[X_1, \dots, X_{n-1}]$ is symmetric: Because f is symmetric we have that

$$f = f(X_1, \dots, X_n) = f(X_{\sigma(1)}, \dots, X_{\sigma(n)})$$

for every $\sigma \in S_n$, und thus we have that

$$f(X_1, \dots, X_{n-1}, 0) = f(X_{\tau(1)}, \dots, X_{\tau(n-1)}, 0)$$

for every $\tau \in S_{n-1}$. Because $\Phi(f) \in k[X_1, \dots, X_{n-1}]$ is symmetric we can use the induction hypothesis (from the induction on n) to write

$$\Phi(f) = P\left(e_1^{(n-1)}, \dots, e_{n-1}^{(n-1)}\right)$$

for some polynomial $P \in k[Y_1, \dots, Y_{n-1}]$. Consider the symmetric polynomial

$$g \coloneqq P\left(e_1^{(n)}, \dots, e_{n-1}^{(n)}\right) \in k[X_1, \dots, X_n] \,.$$

Because Φ is a homomorphism of k-algebras we find that

$$\begin{aligned} \Phi(g) &= \Phi\left(P\left(e_1^{(n)}, \dots, e_{n-1}^{(n)}\right)\right) \\ &= P\left(\Phi\left(e_1^{(n)}\right), \dots, \left(e_{n-1}^{(n)}\right)\right) \\ &= P\left(e_1^{(n-1)}, \dots, e_{n-1}^{(n-1)}\right) = \Phi(f) \end{aligned}$$

and therefore that $\Phi(f-g) = 0$. Note that $\ker \Phi = (X_n)$ by the commutativity of the following diagram:

$$\begin{tikzcd} k[X_1, \dots, X_n] \arrow[rr, "\Phi"] \arrow[dr, "p \mapsto \overline{p}"'] & & k[X_1, \dots, X_{n-1}] \\ & k[X_1, \dots, X_n]/(X_n) \arrow[ur, "\sim", "\overline{p} \mapsto p(X_1, \dots, X_n, 0)"'] & \end{tikzcd}$$

It therefore follows from $\Phi(f-g) = 0$ that $X_n \mid (f-g)$. Because $f-g$ is symmetric (because both f and g are symmetric) it follows that $X_i \mid (f-g)$ for all $1 \leq i \leq n$, and therefore that $X_1 \cdots X_n \mid (f-g)$. We can thus consider the polynomial

$$h \coloneqq \frac{f-g}{X_1 \cdots X_n} = \frac{f-g}{e_n^{(n)}} \,.$$

(This quotient is well-defined because $k[X_1, \dots, X_n]$ is an integral domain.)

Claim. The polynomial h is symmetric.

Proof. From $he_n^{(n)} = f - g$ it follows for every $\sigma \in S_n$ that

$$(\sigma.h)e_n^{(n)} = (\sigma.h)(\sigma.e_n^{(n)}) = \sigma.(he_n^{(n)}) = \sigma(f-g) = \sigma.f - \sigma.g = f - g \,.$$

Hence it follows that $\sigma.h = (f-g)/e_n^{(n)} = h$. □

Claim. We have that $\deg g \leq \deg f$ and therefore that $\deg h < \deg f$.

Proof. ? □

By induction hypothesis (of the induction on d) we can write h as a polynomial in $e_1^{(n)}, \dots, e_n^{(n)}$. Because g is also a polynomial in $e_1^{(n)}, \dots, e_n^{(n)}$ it further follows that $f = e_n^{(n)}h + g$ is a polynomial in $e_1^{(n)}, \dots, e_n^{(n)}$. □

We now prove that the polynomials $e_1^{(n)}, \dots, e_n^{(n)}$ are algebraically independent by induction over n. It holds for $n = 1$ because $e_1^{(1)} = X_1$.

Now suppose $n \geq 2$ and that the elements $e_1^{(n-1)}, \dots, e_{n-1}^{(n-1)}$ are algebraically independent. Suppose that

$$F\left(e_1^{(n)}, \dots, e_n^{(n)}\right) = 0$$

for some polynomial $F \in k[Y_1, \dots, Y_n]$ with $F \neq 0$ of minimal possible degree. Then

$$\begin{aligned} 0 &= \Phi\left(F\left(e_1^{(n)}, \dots, e_{n-1}^{(n)}, e_n^{(n)}\right)\right) \\ &= F\left(\Phi\left(e_1^{(n)}\right), \dots, \Phi\left(e_{n-1}^{(n)}\right), \Phi\left(e_n^{(n)}\right)\right) \\ &= F\left(e_1^{n-1}, \dots, e_{n-1}^{(n-1)}, e_n^{(n-1)}\right) = F\left(e_1^{n-1}, \dots, e_{n-1}^{(n-1)}, 0\right). \end{aligned}$$

From the induction hypothesis it follows that $F(Y_1, \dots, Y_{n-1}, 0) = 0$, and therefore that $Y_n \mid F$. So there exists some polynomial $\hat{F} \in k[Y_1, \dots, Y_n]$ with $F = Y_n \hat{F}$. Note that $\hat{F} \neq 0$ since $F \neq 0$, and that $\deg \hat{F} < \deg F$. We then have

$$0 = F\left(e_1^{(n)}, \dots, e_n^{(n)}\right) = e_n^{(n)} \hat{F}\left(e_1^{(n)}, \dots, e_n^{(n)}\right).$$

Because $k[X_1, \dots, X_n]$ is an integral domain it now further follows from $e_n^{(n)} \neq 0$ that

$$\hat{F}\left(e_1^{(n)}, \dots, e_n^{(n)}\right) = 0.$$

This contradits the minimality of F. □

Remark 9.12. Each of the proofs gives us an algorithm how to express a symmetric polynomial in terms of $e_1, \dots, e_n$.

Remark 9.13. The first proof shows that the fundemental theorem does not only hold if k is a field, but for every nonzero commutative ring R. It does in particular hold for $k = \mathbb{Z}$.

The second proof can be slightly modified to also work for R: Instead of using that $R[X_1, \dots, X_n]$ is an integral domain (which holds if and only if R itself is an intgeral domain), it sufficies to realize that the polynomial $X_1 \cdots X_n = e_n$ is a non-zero divisor.

Example 9.14. Let $p(t) = t^n + a_{n-1}t^{n-1} + \dots + a_1 t + a_0 \in k[t]$ be a polynomial, and let $\lambda_1, \dots, \lambda_n$ be the roots of $p(t)$ is an algebraic closure $\overline{k}$ of k. Then

$$a_i = (-1)^{n-i} e_{n-i}(\lambda_1, \dots, \lambda_n)$$

for all i by Lemma 9.9. It follows from the fundamental theorem that every symmetric polynomial in the roots $\lambda_1, \dots, \lambda_n$ can already be expressed as a polynomial in the coefficients $a_0, \dots, a_{n-1}$:

Consider for example the *discriminant*

$$\Delta(p) = \prod_{i<j} (\lambda_i - \lambda_j)^2 = (-1)^{n(n-1)/2} \prod_{i \neq j} (\lambda_i - \lambda_j)$$

The polynomial $D(X_1, \dots, X_n) \coloneqq \prod_{i<j}(X_i - X_j)^2$ is symmetric, which is why there exists a (unique) polynomial $f \in k[Y_1, \dots, Y_n]$ with $D = f(e_1, \dots, e_n)$. Then

$$\Delta(p) = D(\lambda_1, \dots, \lambda_n) = f(e_1(\lambda_1, \dots, \lambda_n), \dots, e_n(\lambda_1, \dots, \lambda_n)) = f(a_{n-1}, \dots, a_0)\,.$$

This shows that $\Delta(p)$ can be expressed as a polynomial in the coefficients of p.

Note that $\Delta(p) = \prod_{i<j}(\lambda_i - \lambda_j)^2$ vanishes if and only if f a multiple root in $\overline{k}$. Altogether we have thus found that there exists a polynomial expression in the coefficients of p, namely $f(a_{n-1}, \dots, a_0)$, by which we can describe if f has multiple roots in an algebraic closure $\overline{k}$ of k.

Consider for example the case $n = 2$. Then

$$D(X_1, X_2) = (X_1 - X_2)^2 = (X_1 + X_2)^2 - 4X_1X_2 = e_1^2 - 4e_2\,,$$

and therefore $f(Y_1, Y_2) = Y_1^2 - 4Y_2$. For $p(t) = t^2 + at + b$ we therefore have that

$$\Delta(p) = f(a, b) = a^2 - 4b\,.$$

Our above discussion shows that $\Delta(p) = 0$ if and only if p has a multiple root in $\overline{k}$. Note that by the usual solution formula for quadratic equations, the roots λ_1, $\lambda_2 \in \overline{k}$ of $p(t)$ are given by

$$\lambda_{1,2} = \frac{-a \pm \sqrt{a^2 - 4b}}{2} = \frac{-a \pm \Delta(p)}{2} = -\frac{1}{2}a \pm \frac{\sqrt{\Delta(p)}}{2}\,.$$

We can see explicitly that the roots $\lambda_1 - \lambda_2 = \pm\sqrt{\Delta(p)}$, and that λ_1, λ_2 are therefore distinct if and only if $\lambda_1 \neq \lambda_2$. The previous discussion shows that $\Delta(p)$ can be generalized to polynomials of arbitrary degree.

9.15. Let R be a ring. Then every sequence of elements $a_0, a_1, a_2, \ldots \in R$ can be considered as coefficients of a (formal) power series

$$\sum_{r=0}^{\infty} a_r t^r \in R[\![t]\!]\,.$$

This power series is the *generating series* or *generating function* of the sequence $(a_n)_{n\in\mathbb{N}}$.

In the following we will consider the generating series $E(t)$, $H(t)$, $P(t)$ of families of symmetric polynomials $(e_r)_{r\in\mathbb{N}}$, $(h_r)_{r\in\mathbb{N}}$, $(p_r)_{r\in\mathbb{N}}$, and then use identities involving these generating series $E(t)$, $H(t)$, $P(t)$ to derive formulas for their coefficients, i.e. the symmetric polynomials e_r, h_r, p_r.

For this we will start with the elementary symmetric polynomials e_r and their generating series:

Definition 9.16. For every $n \in \mathbb{N}$ the power series $E(t) \in k[X_1, \dots, X_n][\![t]\!]$ is the generating series of the sequence $(e_r)_{r\in\mathbb{N}}$, that is

$$E(t) \coloneqq \sum_{r=0}^{\infty} e_r t^r\,.$$

Lemma 9.17. One has the equality of power series

$$E(t) = \prod_{i=1}^{n} (1 + X_i t) \,.$$

Proof. The coefficient of t^r on the right hand side of the equation is given by

$$\sum_{\substack{I \subseteq \{1,\dots,n\} \\ |I| = r}} \prod_{i \in I} X_i \,,$$

which is precisely e_r. □

10. Complete Homogeneous Symmetric Polynomials

Definition 10.1. For all $r \in \mathbb{N}$ the *r-th complete homogeneous symmetric polynomial* (in n-variables) is the sum of all monomials of $k[X_1, \dots, X_n]$ of degree r, that is

$$h_r \coloneqq \sum_{\substack{\boldsymbol{\alpha} \in \mathbb{N}^n \\ |\boldsymbol{\alpha}| = r}} X_1^{\alpha_1} \cdots X_n^{\alpha_n}$$

Definition 10.2. For every $n \in \mathbb{N}$ the power series $H(t) \in k[X_1, \dots, X_n][\![t]\!]$ is the generating series of the sequence $(h_r)_{r \in \mathbb{N}}$, that is

$$H(t) \coloneqq \sum_{r=0}^{\infty} h_r t^r \,.$$

Lemma 10.3. One has the equality of power series

$$H(t) = \prod_{i=1}^{n} \frac{1}{1 - X_i t} \,.$$

Proof. Note that the inverse of $1 - X_i t$ is for every i given by the geometric series

$$Q_i \coloneqq 1 + X_i t + X_i^2 t^2 + X_i^3 t^3 + \cdots \in k[X_1, \dots, X_n][\![t]\!] \,,$$

so that

$$\prod_{i=1}^{n} \frac{1}{1 - X_i t} = \prod_{i=1}^{n} Q_i = Q_1 \cdots Q_n \,.$$

The coefficient of t^r in $Q_1 \cdots Q_n$ is given by $\sum_{|\boldsymbol{\alpha}| = r} X_1^{\alpha_1} \cdots X_n^{\alpha_n} = h_r$. □

10.4. By comparing the closed expressions of the power series $E(t)$ and $H(t)$ from from Lemma 9.17 and Lemma 10.3 we find that

$$E(-t) H(t) = 1 = H(-t) E(t) \,.$$

By comparing the s-th coefficients of these power series we arrive at the following relation between the elementary symmetric polynomials e_r and the complete homogeneous symmetric polynomials h_r:

Corollary 10.5. For all $s \geq 1$ we have that

$$h_s - e_1 h_{s-1} + e_2 h_{s-2} - \dots + (-1)^{s-1} e_{s-1} h_1 + (-1)^s e_s = 0$$

as well as

$$e_s - h_1 e_{s-1} + h_2 e_{s-2} - \dots + (-1)^{s-1} h_{s-1} e_1 + (-1)^s h_s = 0\,.$$

10.6. From the fundamental theorem of symmetric functions we know that the complete homogeneous symmetric polynomials h_i can be expressed uniquely as polynomials in the elementary symmetric polynomials e_i, so that there exist unique polynomials $P_1, \dots, P_n \in k[Y_1, \dots, Y_n]$ with

$$h_i = P_i(e_1, \dots, e_n)$$

for all $i = 1, \dots, n$.

By rearranging the first formula of Corollary 10.5 to the equality

$$h_s = e_1 h_{s-1} - e_2 h_{s-2} + \dots - (-1)^{s-1} e_{s-1} h_1 - (-1)^s e_s$$

we can recursively express the h_i in terms of the e_i, starting off with $e_1 = h_1$ for $s = 1$, and thus inductively determine the polynomials $P_1, \dots, P_n$.

Note that the second formula of Corollary 10.5 results from the first by swapping h_i and e_i. We can therefore swap the h_i and e_i in the previous paragraph to find that the e_i can be expressed in terms of the h_i, and that this can be done in exactly the same way as the h_i are expressed in terms of the e_i. In other words, we have that

$$e_i = P_i(h_1, \dots, h_n)$$

for all $i = 1, \dots, n$.

This seems to suggest that the elementary symmetric polynomials $e_1, \dots, e_n$ and the homomogeneous symmetric polynomials $h_1, \dots, h_n$ are somehow dual to each other. To make this notion of duality more precise note that by the fundamental theorem of symmetric functions there exists a unique k-algebra homomorphism

$$\Phi \colon k[X_1, \dots, X_n]^{S_n} \to k[X_1, \dots, X_n]^{S_n}$$

with $\Phi(e_i) = h_i$ for every $i = 1, \dots, n$. (This follows from combining the universal property of the polynomial ring $k[Y_1, \dots, Y_n]$ with the k-algebra isomorphism $k[Y_1, \dots, Y_n] \to k[X_1, \dots, X_n]^{S_n}$, $Y_i \mapsto e_i$.) We then have that

$$\Phi(h_i) = \Phi(P_i(e_1, \dots, e_n)) = P_i(\Phi(e_1), \dots, \Phi(e_n)) = P_i(h_1, \dots, h_n) = e_n\,.$$

Hence the homomorphism Φ swaps e_i with h_i for every $i = 1, \dots, n$. It follows that $\Phi^2(e_i) = e_i$ for every $i = 1, \dots, n$, and therefore that $\Phi^2 = \mathrm{id}$ because $k[X_1, \dots, X_n]^{S_n}$ is generated by $e_1, \dots, e_n$. Thus we find the following:

Corollary 10.7. There exists an unique k-algebra homomorphism

$$\Phi\colon k[X_1,\dots,X_n]^{S_n} \to k[X_1,\dots,X_n]^{S_n}$$

with $\Phi(e_i) = h_i$ for every $i = 1,\dots,n$, and Φ is an involutive automorphism.

Corollary 10.8. The homogeneous symmetric polynomials $h_1,\dots,h_n$ generate the k-algebra $k[X_1,\dots,X_n]^{S_n}$ and are algebraically independent.

Remark 10.9. As for the fundamental theorem of symmetric functions these results remain valid we replace k with any non-zero commutative ring.

11. Power Symmetric Polynomials

Definition 11.1. For all $n, r \in \mathbb{N}$ the r*-th power symmetric polynomial*, or r*-th power sum* in n-variables is

$$p_r \coloneqq X_1^r + \cdots + X_n^r\,.$$

Definition 11.2. For all $n \in \mathbb{N}$ the power series $P(t) \in k[X_1,\dots,X_n]\llbracket t\rrbracket$ is the generating series of the sequence $(p_r)_{r\geq 1}$, that is

$$P(t) \coloneqq \sum_{r=0}^{\infty} p_{r+1} t^r\,.$$

(Note the shift compared to E and H.)

Lemma 11.3. One has the equality of power series

$$P(t) = \sum_{i=1}^{n} \frac{X_i}{1 - X_i t}\,.$$

More generally, one has that for every $s \geq 0$ that

$$\sum_{r=0}^{\infty} p_{r+s} t^r = \sum_{i=1}^{n} \frac{X_i^s}{1 - X_i t}\,.$$

Proof. We have that

$$\begin{aligned}
\sum_{i=1}^{n} \frac{X_i^s}{1 - X_i t} &= \sum_{i=1}^{n} X_i^s (1 + X_i t + X_i^2 t^2 + X_i^3 t^3 + \cdots) \\
&= \sum_{i=1}^{n} (X_i^s + X_i^{s+1} t + X_i^{s+2} t^2 + X_i^{s+3} t^3 + \cdots) \\
&= p_s + p_{s+1} t + p_{s+2} t^2 + p_{s+3} t^3 + \cdots
\end{aligned}$$

□

11.4. From the explicit formulas for $E(t)$ and $P(t)$ from Lemma 9.17 and Lemma 11.3 it follows that

$$E'(t) = \sum_{i=1}^{n} X_i \prod_{j\neq i}(1+X_j t) = \sum_{i=1}^{n} \frac{X_i}{1+X_i t} \prod_{j=1}^{n}(1+X_j t) = P(-t)E(t)\,.$$

The power series $E'(t)$ is given by

$$E'(t) = \sum_{r=1}^{\infty} r e_r t^{r-1} = \sum_{r=0}^{\infty}(r+1)e_{r+1}t^r\,,$$

so by comparing the $(r-1)$-th coefficient we arrive at the *Newton's identities*.

Corollary 11.5 (Newton's identities)**.** For every $r \geq 1$ one has that

$$re_r = p_1 e_{r-1} - p_2 e_{r-2} + \cdots + (-1)^{r-2} p_{r-1} e_1 + (-1)^{r-1} p_r\,,$$

and equivalently

$$p_r - e_1 p_{r-1} + \cdots + (-1)^{r-1} e_{r-1} p_1 + (-1)^r r e_r = 0\,.$$

11.6. We can proceed similiar as in 11.4 for the genarating functions $H(t)$ and $P(t)$: It follows from the explicit formulas for $H(t)$ and $P(t)$ from Lemma 10.3 and Lemma 11.3 that

$$H'(t) = \sum_{i=1}^{n} \frac{X_i}{(1-X_i t)^2} \prod_{j\neq i} \frac{1}{1-X_j t} = \sum_{i=1}^{n} \frac{X_i}{1-X_i t} \prod_{j=1}^{n} \frac{1}{1-X_j t} = P(t)H(t)\,.$$

Since the power series $H'(t)$ is given by

$$H'(t) = \sum_{k\geq 1} k h_k t^{k-1}$$

we get the following result by comparing the r-th coefficient:

Corollary 11.7. For all $r \geq 1$ we have that

$$rh_r = p_1 h_{r-1} + p_2 h_{r-2} + \cdots + p_{r-1} h_1 + p_r.$$

11.8. We have seen that the symmetric polynomials $e_1, \ldots, e_n$ and $h_1, \ldots, h_n$ each generate $k[X_1, \ldots, X_n]^{S_n}$ and are algebraically independent. It is now only natural to ask if this also holds true for the power sums $p_1, \ldots, p_n$. The next theorem shows that this holds under additional assumptions.

Theorem 11.9. Let k be a field with either $\operatorname{char}(k) = 0$ or $\operatorname{char}(k) > n$. Then $p_1, \ldots, p_n$ generate $k[X_1, \ldots, X_n]^{S_n}$ and are algebraically independent.

Proof. Since $2, \dots, n$ are invertible in k one can use the Newton identities (Corollary 11.5) to recursively express the elementary symmetric polynomials $e_1, \dots, e_n$ in terms of the power sums $p_1, \dots, p_n$, starting off with $e_1 = p_1$. It follows that $p_1, \dots, p_n$ generate $k[X_1, \dots, X_n]^{S_n}$ as a k-algebra.

To show that $p_1, \dots, p_n$ are algebraically independent we need to show that the monomials in $p_1, \dots, p_n$, i.e. the polynomials

$$p^{\boldsymbol{\alpha}} = p_1^{\alpha_1} \cdots p_n^{\alpha_n} \quad \text{with} \quad \boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$$

are linearly independent. For this it sufficies to show for every $N \geq 1$ that the monomials in $p_1, \dots, p_n$ of degree $\leq N$ form a k-basis of the k-linear space of symmetric polynomials of degree $\leq N$, which we will denote by V_N.

We also denote the number of (not necessarily distinct) monomials in $p_1, \dots, p_n$ of degree $\leq N$ by P_N, i.e. P_N is the number of multi-indices $\boldsymbol{\alpha} \in \mathbb{N}^n$ with $\deg p^{\boldsymbol{\alpha}} \leq N$.

Note that for every $\boldsymbol{\alpha} \in \mathbb{N}^n$ we have that

$$\begin{aligned} \deg p^{\boldsymbol{\alpha}} &= \deg p_1^{\alpha_1} \cdots p_n^{\alpha_n} \\ &= \alpha_1 \deg p_1 + \cdots + \alpha_n \deg p_n \\ &= \alpha_1 \cdot 1 + \alpha_2 \cdot 2 + \cdots + \alpha_n \cdot n \\ &= \alpha_1 \deg e_1 + \cdots + \alpha_n \deg e_n \\ &= \deg e_1^{\alpha_1} \cdots e_n^{\alpha_n} = e^{\boldsymbol{\alpha}} \,, \end{aligned}$$

so that P_N is also the number of monomials in $e_1, \dots, e_n$ of degree $\leq N$. Note that these monomials in the e_i are pairwise distinct because the e_i are algebraically independent. Hence P_N is also the number of monomials in $e_1, \dots, e_n$ of degree $\leq N$. With the fundamental theorem of symmetric functions it follows that $\dim V_N = P_N$.

Because $k[X_1, \dots, X_n]^{S_n}$ is generated as a k-algebra by the homogeneous elements $p_1, \dots, p_n$ it we find that V_N is spanned as a k-linear subspace of $K[X_1, \dots, X_n]^{S_n}$ by the monomials in $p(n)_1, \dots, p_n$ of degree $\leq N$, of which they are $\leq P_N$ many distinct ones. It therefore follows from $\dim V_N = P_N$ that V_N is a k-basis von V_N. □

Remark 11.10. Note that the above theorem cannot hold for $k = \mathbb{Z}$: To see this, note that in $\mathbb{Q}[X_1, X_2]^{S_2}$ we have that

$$e_2 = \frac{1}{2} p_1^2 - \frac{1}{2} p_2 \,.$$

If $\mathbb{Z}[X_1, X_2]^{S_2}$ would be generated by p_1, p_2 as a $\mathbb{Z}$-algebra (i.e. ring) then there would exists some polynomial $F \in \mathbb{Z}[Y_1, Y_2]$ with $e_2 = F(p_1, p_2)$. But this would then contradict the algebraic independence of p_1, p_2 in $\mathbb{Q}[X_1, X_2]^{S_2}$, since $F(X_1, X_2) \neq \frac{1}{2} X_1^2 - \frac{1}{2} X_2$.

11.11. We have seen that the elementary symmetric polynomials $e_1, \dots, e_n$ and the complete homogeneous symmetric polynomials $h_1, \dots, h_n$ are dual to each other in the sense that there exists a involutive algebra automorphism Φ of $k[X_1, \dots, X_n]^{S_n}$ which swaps e_i and h_i for every $i = 1, \dots, n$. We can determine the action of Φ on the power sums $p_1, \dots, p_n$.

Applying Φ to Newton's identities (Corollary 11.5) and comparing the result with Corollary 11.7 seems to suggest that

$$\Phi(p_r) = (-1)^{r-1} p_r$$

for all $r = 1, \dots, n$. We can show this by induction on r:

For $r = 1$ we have that

$$\Phi(p_1) = \Phi(e_1) = h_1 = p_1 = (-1)^{r-1} p_1 \,.$$

For $r > 1$ we apply Φ to the Newton identity

$$r e_r = p_1 e_{r-1} - p_2 e_{r-2} + \cdots + (-1)^{r-2} p_{r-1} e_1 + (-1)^{r-1} p_r \,,$$

which by induction results in the identity

$$r h_r = p_1 h_{r-1} + p_2 h_{r-2} + \cdots + p_{r-1} h_1 + (-1)^{r-1} \Phi(p_r) \,.$$

By comparing this to Corollary 11.7 it follows that $\Phi(p_r) = (-1)^{r-1} p_r$.

12. Partitions

Definition 12.1. Let $n \in \mathbb{N}$. A partition of n is a tupel $\lambda = (\lambda_1, \dots, \lambda_s)$ of natural numbers $\lambda_i \in \mathbb{N}$ with $n = \sum_{i=1}^{s} \lambda_i$ and

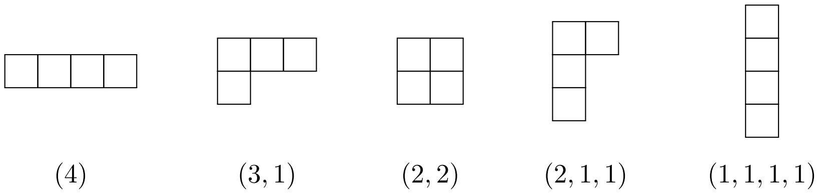
$$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_s > 0 \,.$$

Then $|\lambda| \coloneqq \sum_{i=1}^{n} \lambda_i$, the λ_i are the *parts of* λ and $\ell(\lambda) \coloneqq s$ is the *length of* λ.

Example 12.2. The partitions of 4 are (4), $(3,1)$, $(2,2)$, $(2,1,1)$, $(1,1,1,1)$.

12.3. Partitions are often displayed in terms of *Young diagrams.* The Young diagram corresponding to a partition λ is an array of boxes, left adjusted, such that the i-th row consists of λ_i boxes.

Example 12.4. The Young diagrams of the partitions of 4 are as follows:



(4) $(3,1)$ $(2,2)$ $(2,1,1)$ $(1,1,1,1)$

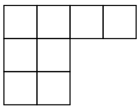
12.5. Note that transposing the Young diagram of a partition λ of n gives again the Young-diagram of a partition λ' of n. If $\lambda = (\lambda_1, \dots, \lambda_s)$ then $\lambda' = (\lambda'_1, \dots, \lambda'_t)$ for $t = \lambda_1$ with $\lambda'_i = |\{j \mid \lambda_j \geq i\}|$.

Definition 12.6. The partition λ' is the *transposed* of the partition λ.

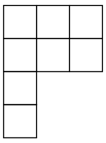
Definition 12.7. An *infinite partition* is a decreasing sequence $\lambda_1, \lambda_2, \ldots \in \mathbb{N}$ with $\lambda_i = 0$ for all but finitely many i. For a partition $(\lambda_1, \ldots, \lambda_s)$ the *infinite partition associated to* λ is given by

$$\hat{\lambda} = (\lambda_1, \ldots, \lambda_s, 0, 0, \ldots)\,.$$

Example 12.8. The partitions $\lambda = (4,2,2)$ and $\lambda' = (3,3,1,1)$ are transposed to each other.



$(4,2,2)$



$(3,3,1,1)$

Definition 12.9. For $n \in \mathbb{N}$ we write

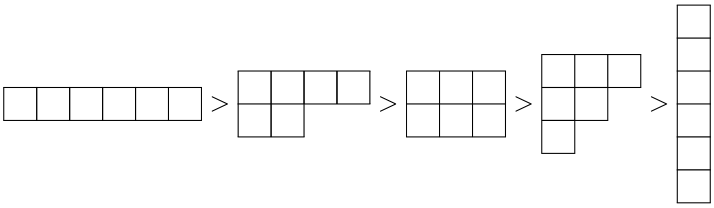
$$\mathrm{Par}(n) \coloneqq \{\text{partitions of } n\}$$

and we set

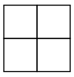
$$\mathrm{Par} \coloneqq \bigcup_{n \in \mathbb{N}} \mathrm{Par}(n)\,.$$

Definition 12.10. If $\lambda, \mu \in P(n)$ then $\lambda \geq \mu$ if $\sum_{i=1}^{r} \hat{\lambda}_i \geq \sum_{i=1}^{r} \hat{\mu}_i$ for all r.

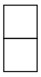
Example 12.11. The following are partitions of 6:



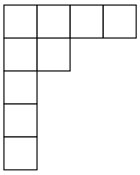
The partitions



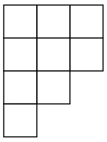
and



are not comparable because the first is a partition of 4 while the second is a partititon of 2. The partitions



and



are also not comparable because $4 > 3$ but $4 + 2 + 1 = 7 < 8 = 3 + 3 + 2$.

Lemma 12.12. For every $n \in \mathbb{N}$, $\leq$ defines a partial ordering on $\mathrm{Par}(n)$.

Proof. The relation $\leq$ is reflexive.

Let $\lambda, \mu \in \mathrm{Par}(n)$ with $\lambda \geq \mu$ and $\lambda \leq \mu$. Because $\lambda \geq \mu$ we have $\hat{\lambda}_1 \geq \hat{\mu}_1$ and because $\lambda \leq \mu$ we have $\hat{\lambda}_1 \leq \hat{\mu}_1$. Thus we have $\hat{\lambda}_1 = \hat{\mu}_1$. In the same way we find that $\hat{\lambda}_1 + \hat{\lambda}_2 = \hat{\mu}_1 + \hat{\mu}_2$, and with $\hat{\lambda}_1 = \hat{\mu}_1$ we get that $\hat{\lambda}_2 = \hat{\mu}_2$. It follows inductively that $\hat{\lambda}_i = \hat{\mu}_i$ for every i. We then have that $\hat{\lambda} = \hat{\mu}$, and therefore that $\lambda = \mu$. This shows that $\leq$ is antisymmetric.

Let $\lambda, \mu, \nu \in \mathrm{Par}(n)$ with $\lambda \geq \mu$ and $\mu \geq \nu$. For all $r \geq 1$ we then have

$$\sum_{i=1}^{r} \hat{\lambda}_i \geq \sum_{i=1}^{r} \hat{\mu}_i \quad \text{and} \quad \sum_{i=1}^{r} \hat{\mu}_i \geq \sum_{i=1}^{r} \hat{\nu}_i$$

and therefore

$$\sum_{i=1}^{r} \hat{\lambda}_i \geq \sum_{i=1}^{r} \hat{\nu}_i \,,$$

so that $\lambda \geq \nu$. This shows that $\leq$ is transitive. □

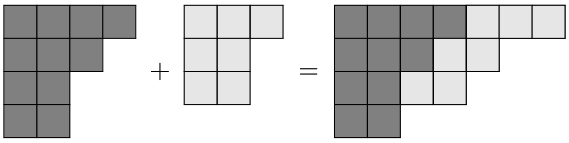
Definition 12.13. For any two infinite partitions λ, μ their *sum* $\lambda + \mu$ is given by

$$(\lambda + \mu)_i = \lambda_i + \mu_i$$

for all i. For any two partitions $\lambda, \mu \in \mathrm{Par}$ their *sum* $\lambda + \mu$ is the partition with $\widehat{\lambda + \mu} = \hat{\lambda} + \hat{\mu}$, i.e. the partitition with $\ell(\lambda + \mu) = \max(\ell(\lambda), \ell(\mu))$ and

$$(\lambda + \mu)_i = \begin{cases} \lambda_i + \mu_i & \text{if } i \leq \ell(\lambda), \ell(\mu)\,, \\ \lambda_i & \text{if } i \leq \ell(\lambda),\ i > \ell(\mu)\,, \\ \mu_i & \text{if } i \leq \ell(\mu),\ i > \ell(\lambda)\,. \end{cases}$$

Example 12.14. For $\lambda = (4, 3, 2, 2)$ and $\mu = (3, 2, 2)$ we have $\lambda + \mu = (7, 5, 4, 2)$. The addition of two partitions can also be visualized "putting together" their Young diagrams row-wise:



13. Monomial Symmetric Polynomials

Definition 13.1. For a partition $\lambda = (\lambda_1, \dots, \lambda_r)$ the corresponding *monomial symmetric polynomial* is given by

$$m_\lambda \coloneqq X_1^{\lambda_1} \cdots X_r^{\lambda_r} + \text{ all distinct permutations of this monomial}.$$

Remark 13.2. The monomial symmetric polynomial m_λ can also be defined in a more formal way:

Instead of adding up all distinct permutations of the monomial $X_1^{\lambda_1} \cdots X_r^{\lambda_r}$ we can also take all distinct permutations of the tupel λ and add up the corresponding monomials. To formalize this we let S_r act on $\mathbb{N}^r$ by permuting the entries, i.e.

$$\pi.(a_1, \dots, a_r) = (a_{\pi^{-1}(1)}, \dots, a_{\pi^{-1}(r)})$$

for all $\pi \in S_r$, $(a_1, \dots, a_r) \in \mathbb{N}^r$. The set of all distinct permutations of λ is precisely the orbit of λ under this action. For the stabilizer subgroup $U \subseteq S_n$ there exists an isomorphism of G-sets

$$S_r/U \to S_r\lambda, \quad \overline{\pi} \mapsto \pi.\lambda$$

where $S_r.\lambda$ denotes the orbit of λ. Thus we can write

$$m_\lambda = \sum_{\overline{\pi} \in S_r/U} X_1^{\lambda_{\pi^{-1}(1)}} \cdots X_r^{\lambda_{\pi^{-1}(r)}} = \sum_{\overline{\pi} \in S_r/U} X_{\pi(1)}^{\lambda_1} \cdots X_{\pi(r)}^{\lambda_r} \,.$$

13.3. Note that every multi-index $\boldsymbol{\alpha} \in \mathbb{N}^n$ can be reordered uniquely to a partition λ of length $\ell(\lambda) = n$. Then m_λ is the “smallest” symmetric polynomial containing the monomial $X^{\boldsymbol{\alpha}} = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$. The following result should therefore not be too surprising:

Proposition 13.4. The monomial symmetric polynomials

$$m_\lambda \quad \text{with} \quad \lambda \in \mathrm{Par}, \ \ell(\lambda) = n$$

form a k-basis of $k[X_1, \dots, X_n]^{S_n}$.

Notation 13.5. Every multi-index $\boldsymbol{\alpha} \in \mathbb{N}^n$ can be permuted to a unique partition $\lambda \in \mathrm{Par}$ of length n. We will refer to λ as the *partition associated to* $\boldsymbol{\alpha}$.

We will sometimes want to consider a partition $\lambda = (\lambda_1, \dots, \lambda_n)$ as a multi-index. When doing so, we will write $\boldsymbol{\lambda}$ instead of just λ. (So technically speaking both $\boldsymbol{\lambda}$ and λ are the same thing.) Note that λ is then the partition associated to $\boldsymbol{\lambda}$.

Proof. Note that for every monomial $X_1^{\alpha_1} \cdots X_n^{\alpha}$ the polynomial

$$X_1^{\alpha_1} \cdots X_n^{\alpha} + \text{all distinct permutations of this monomial}$$

is precisely the monomial symmetric polynomial m_λ of the partition λ associated to the multiindex $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n)$.

Let $f \in k[X_1, \dots, X_n]^{S_n}$ be a symmetric polynomial. Then for every monomial $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ occuring in f, all of its permutations must also occur in f, all of them with the same coefficient c. By the above observation all of these monomials can be grouped together to the symmetric polynomial cm_λ, where λ is the partition associated to $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n)$.

Since $f - cm_\lambda$ is again symmetric one can then inductively continue this process of grouping together permutated monomials to ultimately express f as a linear combination of monomial symmetric polynomials. (Note that no new monomials are introduced during this process, so that it eventually terminates.)

The beginning observation also shows that a partition λ is uniquely determined by any of the monomials $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ occuring in m_λ. It follows that for any two distinct partitions $\lambda \neq \mu$ their monomial symmetric polynomials m_λ, m_μ have no common monomonials. As the collection of all monomials $X^{\boldsymbol{\alpha}}$, $\boldsymbol{\alpha} \in \mathbb{N}^n$ is linearly independent, it follows that the collection of monomial symmetric polynomials m_λ, $\lambda \in \mathrm{Par}$ is also linearly independent. □

13.6. Note that the proof of Proposition 13.4 gives an easy way to express a symmetric polynomial $f \in k[X_1, \dots, X_n]^{S_n}$ in terms of the monomial symmetric polynomials: Simply group together all monomial which are permutated to each other.

We will use this to describe the product $m_\lambda m_\mu$ for two partitions $\lambda, \mu \in \mathrm{Par}$ of length n as a linear combination of the basis m_ν, $\nu \in \mathrm{Par}$:

The monomials $X^{\boldsymbol{\alpha}} = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ occuring in m_λ are those for the multi-indices $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n)$ with associated partition λ, and the monomials $X^{\boldsymbol{\beta}}$ occuring in m_μ are those for the multi-indices $\boldsymbol{\beta}$ with associated partition μ.

In follows that all monomials $X^{\boldsymbol{\gamma}}$ occuring in $m_\lambda m_\mu$ are of the form $\boldsymbol{\gamma} = \boldsymbol{\alpha} + \boldsymbol{\beta}$ for some $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$ as above. Given such a $\boldsymbol{\gamma}$ and corresponding $\boldsymbol{\alpha}, \boldsymbol{\beta}$, let $\nu \in \mathrm{Par}$ be the partition associated to $\boldsymbol{\gamma}$.

Claim. The partition ν satisfies $\nu \leq \lambda + \mu$.

Proof. Let $\lambda = (\lambda_1, \dots, \lambda_n)$, $\mu = (\mu_1, \dots, \mu_n)$ and $\nu = (\nu_1, \dots, \nu_n)$. By definition of $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ there exist permutations $\sigma, \tau \in S_n$ with

$$\boldsymbol{\alpha} = (\lambda_{\sigma(1)}, \dots, \lambda_{\sigma(n)}) \quad \text{and} \quad \boldsymbol{\beta} = (\mu_{\tau(1)}, \dots, \mu_{\tau(n)})$$

and by definition of ν there exists some permutation $\omega \in S_n$ with

$$\nu = (\nu_1, \dots, \nu_n) = (\alpha_{\omega(1)} + \beta_{\omega(1)}, \dots, \alpha_{\omega(n)} + \beta_{\omega(n)})$$

For every $r = 1, \dots, n$ we therefore have that

$$\begin{aligned} \sum_{i=1}^r \nu_r = \sum_{i=1}^r (\alpha_{\omega(i)} + \beta_{\omega(i)}) = \sum_{i=1}^r \alpha_{\omega(i)} + \sum_{i=1}^r \beta_{\omega(i)} &= \sum_{i=1}^r \lambda_{\sigma(\omega(i))} + \sum_{i=1}^r \mu_{\tau(\omega(i))} \\ &= \sum_{i=1}^r \lambda_{\sigma'(i)} + \sum_{i=1}^r \mu_{\tau'(i)} \end{aligned}$$

for the permutations $\sigma' := \sigma\omega$ and $\tau' := \tau\omega$. Because the entries of the partitions λ and μ are decreasing we have that $\sum_{i=1}^r \lambda_{\sigma'(i)} \leq \sum_{i=1}^r \lambda_i$ and $\sum_{i=0}^r \mu_{\tau'(i)} \leq \sum_{i=1}^r \mu_i$, so that

$$\sum_{i=1}^r \nu_i \leq \sum_{i=1}^r \lambda_i + \sum_{i=1}^r \mu_i = \sum_{i=1}^r (\lambda_i + \mu_i) = \sum_{i=1}^r (\lambda + \mu)_i \,.$$

As this holds for every $r = 1, \dots, n$, this shows that $\nu \leq \mu + \lambda$. □

We have shown that for every monomial $X^{\boldsymbol{\gamma}}$ in $m_\lambda m_\mu$ the partition ν associated to $\boldsymbol{\gamma}$ satisfies $\nu \leq \lambda + \mu$. Thus we find that $m_\lambda m_\mu$ is already a linear combination of those m_ν for which $\nu \leq \mu + \lambda$, i.e. that

$$m_\lambda m_\mu = \sum_{\nu \leq \lambda + \mu} a_\nu m_\nu \,.$$

for suitable coecffients $a_\nu \in k$.

We can also determine the coefficients $a_{\lambda+\mu}$: As in the first proof of the fundamental theorem of symmetric functions we introduce an ordering on the set of monomials in $k[X_1, \dots, X_n]$ by $X_1^{\alpha_1} \cdots X_n^{\alpha_n} > X_1^{\beta_1} \cdots X_n^{\beta_n}$ if they exists some i with $\alpha_1 = \beta_1, \dots, \alpha_n = \beta_n$ and $\alpha_i > \beta_i$. For every polynomial non-zero $f \in k[X_1, \dots, X_n]$ we then denote by $\operatorname{init} f$ the inital term of f, that is the biggest monomial occuring in f together with its coefficient. Then

- $\operatorname{init}(f \cdot g) = (\operatorname{init} f) \cdot (\operatorname{init} g)$ for all $f, g \in k[X_1, \dots, X_n]$ with $f, g \neq 0$, and
- $\operatorname{init} m_\nu = X^{\boldsymbol{\nu}}$ for every partition $\nu \in \mathrm{Par}$ of length n.

With this we find that

$$\operatorname{init}(m_\lambda m_\mu) = (\operatorname{init} m_\lambda)(\operatorname{init} m_\mu) = X^{\boldsymbol{\lambda}} X^{\boldsymbol{\mu}} = X^{\boldsymbol{\lambda}+\boldsymbol{\mu}} = X^{\boldsymbol{\lambda}+\boldsymbol{\mu}} \,.$$

Hence the monomial $X^{\boldsymbol{\lambda}+\boldsymbol{\mu}}$ occurs in $m_\lambda m_\mu$ with coefficient 1. The partition associated to $\boldsymbol{\lambda}+\boldsymbol{\mu}$ is $\lambda + \mu$, so the coefficient of $m_{\lambda+\mu}$ in $m_\lambda m_\mu$ is 1, i.e. $a_{\lambda+\mu} = 1$.

Altogether we have proven the following result:

Lemma 13.7. Let $\lambda, \mu \in \mathrm{Par}$ be partitions of length $\ell(\lambda), \ell(\mu) = n$. Then

$$m_\lambda m_\mu = m_{\lambda+\mu} + \sum_{\nu < \lambda + \mu} a^\nu_{\lambda,\mu} m_\nu$$

for suitable $a^\nu_{\lambda,\mu} \in k$.

Remark 13.8. Note that the above results about monomial symmetric polynomials also hold when the field k is replaced by an arbitrary non-zero commutative ring.

14. Other Symmetric Polynomials Associated to Partitions

Definition 14.1. For a partition $\lambda = (\lambda_1, \dots, \lambda_r)$ the corresponding *elementary symmetric polynomial* is given by

$$e_\lambda \coloneqq e_{\lambda_1} \cdots e_{\lambda_r} \,,$$

the corresponding *complete symmetric polynomial* is given by

$$h_\lambda \coloneqq h_{\lambda_1} \cdots h_{\lambda_r} \,,$$

the corresponding *power symmetric polynomial* is given by

$$p_\lambda \coloneqq p_{\lambda_1} \cdots p_{\lambda_r} \,.$$

14.2. We know from the fundamental theorem of symmetric functions that the elementary symmetric polynomials $e_1, \dots, e_n$ generate $k[X_1, \dots, X_n]^{S_n}$ as a k-algebra and are algebraically independent. This is equivalent to saying that the monomials in $e_1, \dots, e_n$, i.e.

$$e^{\boldsymbol{\alpha}} = e_1^{\alpha_1} \cdots e_n^{\alpha_n} \quad \text{with} \quad \boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n)$$

form a k-basis of $k[X_1, \dots, X_n]^{S_n}$. Note that $e^{\boldsymbol{\alpha}}$ coincides with e_λ for the partition

$$\lambda = (\underbrace{n, \dots, n}_{\alpha_n}, \underbrace{n-1, \dots, n-1}_{\alpha_{n-1}}, \dots, \underbrace{1, \dots, 1}_{\alpha_1}) \,.$$

Also note that the above formula gives a bijection

$$\{\text{multi-indices } \boldsymbol{\alpha} \in \mathbb{N}^n\} \longleftrightarrow \{\text{partitions } \lambda \in \mathrm{Par} \text{ with } \lambda_1 \leq n\} \,.$$

With this we arrive at the following reformulation of the fundamental theorem of symmetric functions:

Corollary 14.3. The symmetric polynomials

$$e_\lambda \quad \text{with} \quad \lambda \in \mathrm{Par} \,, \lambda_1 \leq n$$

form a k-basis of $k[X_1, \dots, X_n]^{S_n}$.

Remark 14.4. We can show the same statements for the polynomials h_λ since $h_1, \dots, h_n$ generate $k[X_1, \dots, X_n]^{S_n}$ as a k-algebra and are algebraically independent. If k is a field with $\mathrm{char}(k) = 0$ or $\mathrm{char}(k) > n$ we can also show the same for the polynomials p_λ.

Invariant Rings and Zariski Density

15. Invariants for Matrix Actions

Definition 15.1. Let V be a finite-dimensional representation of a group G. The k-algebra $\mathcal{P}(V)^G$ is the *ring of invariants* or *invariant ring* of V.

Example 15.2. Let S_n acts on k^n by permuting the coordinates. When we identify $\mathcal{P}(k^n)$ with $k[X_1, \dots, X_n]$ (as explained in 7.11) then the invariant ring $\mathcal{P}(k^n)^{S_n}$ coincides with the ring of symmetric polynomials $k[X_1, \dots, X_n]^{S_n}$. The fundamental theorem of symmetric functions shows that $\mathcal{P}(k^n)^{S_n}$ is again a polynomial ring in n variables and gives an explicit set of free k-algebra generators $e_1, \dots, e_n$.

Conventions 15.3. For this section we require all occuring fields to be infinite.

15.4. One of the main concerns of *classical invariant theory* is to understand the invariant ring $\mathcal{P}(V)^G$ of a representation V of a group G. Over the course of the next two sections we will determine the invariant rings of the actions of $\mathrm{GL}_n(k)$ and $\mathrm{SL}_n(k)$ on $\mathrm{M}_n(k)$ by left multiplication and by conjugation. The content of this section is mostly taken from [KP96, §1.2, §2.3].

We will make use of the following *Zariski density properties*, which we will prove in the next section:

Proposition 15.5 (Zariski density properties)**.** Let $h\colon \mathrm{M}_n(k) \to k$ be polynomial.

a) If $h|_{\mathrm{GL}_n(k)} = 0$ then $h = 0$.

b) Let $h(D) = 0$ for every diagonalizable matrix $D \in \mathrm{M}_n(k)$, then $h = 0$.

Proposition 15.6. Let the group $\mathrm{GL}_n(k)$ act on $\mathrm{M}_n(k)$ by left multiplication. Then the invariant ring $\mathcal{P}(\mathrm{M}_n(k))^{\mathrm{GL}_n(k)}$ is given by $\mathcal{P}(\mathrm{M}_n(k))^{\mathrm{GL}_n(k)} = k$.

Proof. For $f \in \mathcal{P}(\mathrm{M}_n(k))^{\mathrm{GL}_n(k)}$ we have that

$$f(S) = f(S \cdot I) = f(S.I) = f(I)$$

for every $S \in \mathrm{GL}_n(k)$. It follows for the polyonomial map $g\colon \mathrm{M}_n(k) \to k$ given by $g \coloneqq f - f(I)$ satisfies $g|_{\mathrm{GL}_n(k)} = 0$. It follows from the first Zariski density property that $g = 0$. This shows that $f(A) = f(I)$ for all $A \in \mathrm{M}_n(k)$, so that f is constant. □

Theorem 15.7. Let $\mathrm{SL}_n(k)$ act on $\mathrm{M}_n(k)$ by left multiplication. Then the map

$$\det\colon \mathrm{M}_n(k) \to k$$

generates the invariant ring $\mathcal{P}(\mathrm{M}_n(k))^{\mathrm{SL}_n(k)}$ as a k-algebra and is algebraically independent, i.e. the map

$$k[T] \to \mathcal{P}(\mathrm{M}_n(k))^{\mathrm{SL}_n(k)}\,, \quad p(T) \mapsto p(\det)$$

is a well-defined isomorphism of k-algebras.

Proof. The determinant function is polynomial, as seen in Example 7.7. For all $S \in \mathrm{SL}_n(k)$, $A \in \mathrm{M}_n(k)$ we have that

$$(S.\det)(A) = \det\left(S^{-1}.A\right) = \det\left(S^{-1}\right)\det(A) = \det(A)\,,$$

which shows that det is $\mathrm{SL}_n(k)$-invariant.

We show that det is algebraically independent: Let $p \in k[X]$ with $p(\det) = 0$. Then

$$p(\det(A)) = p(\det)(A) = 0$$

for all $A \in \mathrm{M}_n(k)$ because the k-algebra structure of $\mathcal{P}(\mathrm{M}_n(k))$ is defined pointwise. Since det is surjective it follows that $p(\lambda) = 0$ for every $\lambda \in k$. Because k is infinite it follows that $p = 0$.

We show that det generates $\mathcal{P}(\mathrm{M}_n(k))^{\mathrm{SL}_n(k)}$ as a k-algebra: Let $f \in \mathcal{P}(\mathrm{M}_n(k))^{\mathrm{SL}_n(k)}$. Note that for $A, B \in \mathrm{GL}_n(k)$ with $\det A = \det B$ we have that $BA^{-1} \in \mathrm{SL}_n(k)$ and therefore

$$f(A) = f\left((BA^{-1}).A\right) = f(BA^{-1}A) = f(B)\,.$$

It follows for every $A \in \mathrm{GL}_n(k)$ that

$$f(A) = f\left(\begin{bmatrix} \det A & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix}\right). \tag{15.1}$$

Note that the right hand side of this equation is a polynomial in $\det A$.

More specifically, let $p \in k[X_{11}, \dots, X_{nn}]$ with

$$f(A) = p(A_{11}, \dots, A_{nn})$$

for every $A = (A_{ij})_{i,j=1,\dots,n} \in \mathrm{M}_n(k)$. Let $\varphi\colon k[X_{11}, \dots, X_{nn}] \to k[T]$ be the k-algebra homomorphism with

$$\varphi(X_{ij}) = \begin{cases} 0 & \text{if } i \neq j\,, \\ 1 & \text{if } i = j \neq 1\,, \\ T & \text{if } i = j = 1\,. \end{cases}$$

for all $i, j = 1, \dots, n$. Then for the polynomial $q \coloneqq \varphi(p) \in k[T]$ and the corresponding polynomial function $g \coloneqq q(\det) \in \mathcal{P}(V)^{\mathrm{SL}_n(k)}$ we can reformulate (15.1) to

$$f(A) = f\left(\begin{bmatrix} \det A & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix}\right) = q(\det A) = q(\det)(A) = g(A) \tag{15.2}$$

for every $A \in \mathrm{GL}_n(k)$.

We have constructed $g = q(\det) \in k[\det]$ with $f|_{\mathrm{GL}_n(k)} = g|_{\mathrm{GL}_n(k)}$. With the first Zariski density property it follows from $(f-g)|_{\mathrm{GL}_n(k)} = 0$ that $f - g = 0$ and therefore that $f = g$. □

15.8. Recall that the characteristic polynomial of a matrix $A \in \mathrm{M}_n(k)$ is given by

$$\chi_A(t) = \det(tE_n - A)$$

where $E_n \in \mathrm{M}_n(k)$ is the identity matrix. Then

$$\chi_A(t) = t^n - s_1(A)t^{n-1} + s_2(A)t^{n-2} + \cdots + (-1)^n s_n(A)$$

with $s_1, \dots, s_n \in \mathcal{P}(\mathrm{M}_n(k))$ and $s_1 = \mathrm{tr}$, $s_n = \det$. In the case that A is a diagonal matrix $A = \mathrm{diag}(d_1, \dots, d_n)$ we have that

$$\chi_A(t) = \prod_{i=1}^{n}(t - d_i) = t^n - e_1(d_1, \dots, d_n)t^{n-1} + \cdots + (-1)^n e_n(d_1, \dots, d_n)$$

for the elementary symmetric polynomials $e_1, \dots, e_n$, and therefore

$$s_i(\mathrm{diag}(d_1, \dots, d_n)) = e_i(d_1, \dots, d_n)$$

for all $i = 1, \dots, n$.

Theorem 15.9. Let $\mathrm{GL}_n(k)$ act on $\mathrm{M}_n(k)$ by conjugation. Then the invariant ring $\mathcal{P}(\mathrm{M}_n(k))^{\mathrm{GL}_n(k)}$ is generated by $s_1, \dots, s_n$ as a k-algebra and the s_i are algebraically independent, i.e. the map

$$k[T_1, \dots, T_n] \to \mathcal{P}(\mathrm{M}_n(k))^{\mathrm{GL}_n(k)}, \quad p(T_1, \dots T_n) \mapsto p(s_1, \dots, s_n)$$

is a well-defined isomorphism of k-algebras.

Proof. The polynomial functions $s_1, \dots, s_n \colon \mathrm{M}_n(k) \to k$ are $\mathrm{GL}_n(k)$-invariant because the characteristic polynomial of a matrix is invariant under conjugation.

Let $p \in k[X_1, \dots, X_n]$ with $p(s_1, \dots, s_n) = 0$. For all $\lambda_1, \dots, \lambda \in k$ it follows that

$$\begin{aligned} 0 &= p(s_1, \dots, s_n)(\mathrm{diag}(\lambda_1, \dots, \lambda_n)) \\ &= p(s_1(\mathrm{diag}(\lambda_1, \dots, \lambda_n)), \dots, s_n(\mathrm{diag}(\lambda_1, \dots, \lambda_n))) \\ &= p(e_1(\lambda_1, \dots, \lambda_n), \dots, e_n(\lambda_1, \dots, \lambda_n)) \\ &= p(e_1, \dots, e_n)(\lambda_1, \dots, \lambda_n), \end{aligned}$$

which shows that the polynomial $p(e_1, \dots, e_n)$ vanishes everywhere. It follows that $p(e_1, \dots, e_n) = 0$ because k is infinite, und thus $p = 0$ because $e_1, \dots, e_n$ are algebraically independent. This shows that $s_1, \dots, s_n$ are algebraically independent.

Let $f \in \mathcal{P}(\mathrm{M}_n(k))^{\mathrm{GL}_n(k)}$. If $D \in \mathrm{M}_n(k)$ diagonalizable with eigenvalues $\lambda_1, \dots, \lambda_n$ then D is conjugated to the diagonal matrix $\mathrm{diag}(\lambda_1, \dots, \lambda_n)$, so that

$$f(D) = f(\mathrm{diag}(\lambda_1, \dots, \lambda_n)). \tag{15.3}$$

Note that the right hand side is a polynomial in $\lambda_1, \dots, \lambda_n$. More specifically, let $p \in k[X_{11}, \dots, X_{nn}]$ with

$$f(A) = p(A_{11}, \dots, A_{nn})$$

for every matrix $A = (A_{ij})_{i,j=1,\dots,n} \in \mathrm{M}_n(k)$. Let $\varphi\colon k[X_{11}, \dots, X_{nn}] \to k[\tilde{T}_1, \dots, \tilde{T}_n]$ be the k-algebra homomorphism with

$$\varphi(X_{ij}) = \begin{cases} \tilde{T}_i & \text{if } i = j\,, \\ 0 & \text{otherwise}\,, \end{cases}$$

for all $i, j = 1, \dots, n$. For the polynomial $\tilde{q} \coloneqq \varphi(p)$ we can then reformulate (15.3) to

$$f(D) = f(\operatorname{diag}(\lambda_1, \dots, \lambda_n)) = \tilde{q}(\lambda_1, \dots, \lambda_n)\,. \tag{15.4}$$

Claim. The polynomial $\tilde{q}$ is symmetric.

Proof. We need to show that $\tilde{q} = \sigma.\tilde{q}$ for every $\sigma \in S_n$. Since k is infinite is sufficies to show that

$$\tilde{q}(\lambda_1, \dots, \lambda_n) = (\sigma.\tilde{q})(\lambda_1, \dots, \lambda_n)$$

for all $\lambda_1, \dots, \lambda_n \in k$. Note that

$$(\sigma.\tilde{q})(\lambda_1, \dots, \lambda_n) = \tilde{q}(\lambda_{\sigma(1)}, \dots, \lambda_{\sigma(n)})$$

because S_n acts by k-algebra automorphisms on $k[\tilde{T}_1, \dots, \tilde{T}_n]$, which is generated by $\tilde{T}_1, \dots, \tilde{T}_n$, and

$$(\sigma.\tilde{T}_i)(\lambda_1, \dots, \lambda_n) = \tilde{T}_{\sigma(i)}(\lambda_1, \dots, \lambda_n) = \lambda_{\sigma(i)} = \tilde{T}_i(\lambda_{\sigma(1)}, \dots, \lambda_{\sigma(n)})\,.$$

Hence we have to show that

$$\tilde{q}(\lambda_1, \dots, \lambda_n) = \tilde{q}(\lambda_{\sigma(1)}, \dots, \lambda_{\sigma(n)})$$

for all $\lambda_1, \dots, \lambda_n \in k$. By construction of $\tilde{q}$ this is equivalent to

$$f(\operatorname{diag}(\lambda_1, \dots, \lambda_n)) = f(\operatorname{diag}(\lambda_{\sigma(1)}, \dots, \lambda_{\sigma(n)})) \tag{15.5}$$

for all $\lambda_1, \dots, \lambda_n \in k$. Note thas the two diagonal matrices $\operatorname{diag}(\lambda_1, \dots, \lambda_n)$ and $\operatorname{diag}(\lambda_{\sigma(1)}, \dots, \lambda_{\sigma(n)})$ we have that

$$\operatorname{diag}(\lambda_{\sigma(1)}, \dots, \lambda_{\sigma(n)}) = P_\sigma^{-1} \operatorname{diag}(\lambda_1, \dots, \lambda_n) P_\sigma$$

where $P_\sigma \in \mathrm{GL}_n(k)$ denotes the permutation matrix of σ, i.e. the matrix P_σ with $P_\sigma(e_i) = e_{\sigma(i)}$ for all i. This holds because

$$\begin{aligned} P_\sigma^{-1} \operatorname{diag}(\lambda_1, \dots, \lambda_n) P_\sigma e_i &= P_\sigma^{-1} \operatorname{diag}(\lambda_1, \dots, \lambda_n) e_{\sigma(i)} \\ &= \lambda_{\sigma(i)} P_\sigma^{-1} e_{\sigma(i)} = \lambda_{\sigma(i)} e_i = \operatorname{diag}(\lambda_{\sigma(1)}, \dots, \lambda_{\sigma(n)}) e_i \end{aligned}$$

for all i. The desired equality (15.5) thus follows from the $\mathrm{GL}_n(k)$-invariance of f. □

Since the elementary symmetric polynomials $e_1, \dots, e_n$ generate the k-algebra of symmetric polynomials $k[\tilde{T}_1, \dots, \tilde{T}_n]^{S_n}$ there exists a polynomial $q \in k[T_1, \dots, T_n]$ with

$$\tilde{q} = q(e_1, \dots, e_n)\,.$$

For the polynomial function $g \coloneqq q(s_1, \dots, s_n)$ we can then further reformulate (15.4) to

$$\begin{aligned} f(D) &= f(\operatorname{diag}(\lambda_1, \dots, \lambda_n)) = \tilde{q}(\lambda_1, \dots, \lambda_n) \\ &= q(e_1, \dots, e_n)(\lambda_1, \dots, \lambda_n) \\ &= q(e_1(\lambda_1, \dots, \lambda_n), \dots, e_n(\lambda_1, \dots, \lambda_n)) \\ &= q(s_1(\operatorname{diag}(\lambda_1, \dots, \lambda_n)), \dots, s_n(\operatorname{diag}(\lambda_1, \dots, \lambda_n))) \\ &= q(s_1, \dots, s_n)(\operatorname{diag}(\lambda_1, \dots, \lambda_n)) \\ &= g(\operatorname{diag}(\lambda_1, \dots, \lambda_n)) = g(D)\,. \end{aligned}$$

We have thus constructed a polynomial function $g = q(s_1, \dots, s_n) \in k[s_1, \dots, s_n]$ with $f(D) = q(D)$ for every diagonalizable matrix $D \in \mathrm{M}_n(k)$. By the second Zariski density property it follows from

$$(f - g)(D) = 0 \quad \text{for every diagonalizable matrix } D \in \mathrm{M}_n(k)$$

that $f - g = 0$, and thus $f = g = q(s_1, \dots .s_n)$. This shows that $\mathcal{P}(\mathrm{M}_n(k))^{\mathrm{GL}_n(k)}$ is generated by $s_1, \dots, s_n$. □

15.10. Another family of $\mathrm{GL}_n(k)$-invarant polynomial functions $\mathrm{M}_n(k) \to k$ (where $\mathrm{GL}_n(k)$ acts on $\mathrm{M}_n(k)$ by conjugation) are the *power traces*: The m-th *power traces* is given by

$$\mathrm{tr}_m \colon \mathrm{M}_n(k) \to k, \quad A \mapsto \mathrm{tr}(A^m)\,.$$

for every $m \in \mathbb{N}$. The $\mathrm{GL}_n(k)$-invariance of the trace powers tr_m follows from the $\mathrm{GL}_n(k)$-invariance of the trace, as we have for all $S \in \mathrm{GL}_n(k)$, $A \in \mathrm{M}_n(k)$ that

$$\begin{aligned} (S.\,\mathrm{tr}_m)\,(A) = \mathrm{tr}_m\left(S^{-1}.A\right) = \mathrm{tr}_m\left(S^{-1}AS\right) = \mathrm{tr}\left(S^{-1}AS\right)^m &= \mathrm{tr}\left(S^{-1}A^mS\right) \\ &= \mathrm{tr}(A^m) = \mathrm{tr}_m(A)\,. \end{aligned}$$

Note that for all $\lambda_1, \dots, \lambda_n \in k$ we have that

$$\mathrm{tr}_m(\operatorname{diag}(\lambda_1, \dots, \lambda_n)) = \lambda_1^m + \cdots + \lambda_n^m = p_m(\lambda_1, \dots, \lambda_n)$$

for every $m \in \mathbb{N}$, where p_m denotes the m-th power symmetric polynomials. Since k is a field with $\mathrm{char}(k) = 0$ or $\mathrm{char}(k) > n$ we know that the k-algebra of symmetric polynomials $k[\tilde{T}_1, \dots, \tilde{T}_n]^{S_n}$ is generated by the polynomials $p_1, \dots, p_n$, and that they are algebraically independent.

By replacing s_i with tr_i and e_i with p_i in the proof of Theorem 15.9 we thus arrive at a proof of the following theorem:

Theorem 15.11. Let the group $\mathrm{GL}_n(k)$ act on $\mathrm{M}_n(k)$ by conjugation. If $\mathrm{char}(k) = 0$ or $\mathrm{char}(k) > n$ then the k-algebra $\mathcal{P}(\mathrm{M}_n(k))^{\mathrm{GL}_n(k)}$ is generated by the power traces $\mathrm{tr}_1, \dots, \mathrm{tr}_n$ and they are algebraically independent, i.e. the map

$$k[T_1, \dots, T_n] \to \mathcal{P}(\mathrm{M}_n(k))^{\mathrm{GL}_n(k)}, \quad p(T_1, \dots T_n) \mapsto p(\mathrm{tr}_1, \dots, \mathrm{tr}_n)$$

is a well-defined isomorphism of k-algebras.

16. Zariski Dense Subsets

16.1. Parts of this section are taken from [KP96, §1.3].

Conventions 16.2. For this section let k be an infinite field.

Definition 16.3. Let V be a finite-dimensional k-vector space. A subset $X \subseteq V$ is *Zariski dense* (*over* k) if for every polynomial map $f \colon V \to k$ we have that

$$f|_X = 0 \implies f = 0\,.$$

If $X \subseteq Y \subseteq V$ then X *is Zariski dense in* Y (*over* k) if for every polynomial function $f \colon V \to k$ we have that

$$f|_X = 0 \implies f|_Y = 0\,.$$

Example 16.4. Let V be a finite-dimensional k-vector space.

a) Any infinite subset $X \subseteq k$ is Zariski dense: Let $f \colon V \to k$ be a polynomial function with $f|_X = 0$. There exists some polynomial $p \in k[X]$ with $f(\lambda) = p(\lambda)$ for all $\lambda \in k$ because f is polynomial. It follows from $f|_X = 0$ that every $x \in X$ is a zero of p, which shows that p has infinitley many zeroes. This can only be the case for $p = 0$, and thus $f = 0$.

b) Let $U \subsetneq V$ be a proper k-linear subspace. Then U is not Zariski dense in V over k: To see this let $v_1, \dots, v_m, v_{m+1}, \dots, v_n$ be a k-basis of V such that $v_1, \dots, v_m$ is a k-basis of U. Then $m < n$ because U is a proper subspace of V. Let $\pi \colon V \to k$ be the projection onto the last coordinate, i.e.

$$\pi\left(\lambda_1 v_1 + \dots + \lambda_n v_n\right) = \lambda_n$$

for all $\lambda_1, \dots, \lambda_n \in k$. We then have that $\pi|_U = 0$ but $\pi \neq 0$, which shows that U is not Zariski dense in V over k.

c) Let k be a finite field. We have seen in Remark 7.12 that every function $f \colon V \to k$ is a polynomial function. It follows that the only Zariski-dense subset $X \subseteq V$ is $X = V$ itself.

Warning 16.5. The previous examples show that the notion of Zariski density depend on the choice of the underlying field k: It follows from the first example that $\mathbb{R} \subseteq \mathbb{C}$ is Zariski dense over $\mathbb{C}$, while it follows from the second example that $\mathbb{R} \subseteq \mathbb{C}$ is not Zariski dense over $\mathbb{R}$.

Lemma 16.6. Let V be a finite-dimensional k-vector space and let $h\colon V \to k$ be a non-zero polynomial function. Then the non-vanishing set

$$V_h \coloneqq \{v \in V \mid h(v) \neq 0\}$$

is Zariski dense in V.

Proof. Let $f\colon V \to k$ be a polynomial function with $f|_{V_h} = 0$. Then

$$(fh)(v) = f(v)h(v) = 0$$

for all $v \in V$, and thus $fh = 0$. The k-algebra $\mathcal{P}(V) \cong k[X_1, \dots, X_{(\dim V)}]$ is an integral domain. It therefore follows from $fh = 0$ and $h \neq 0$ that $f = 0$. □

Corollary 16.7 (First Zariski density property)**.** The subset $\mathrm{GL}_n(k) \subseteq \mathrm{M}_n(k)$ is Zariski dense.

Proof. The group $\mathrm{GL}_n(k)$ is the non-vanishing set of $\det\colon \mathrm{M}_n(k) \to k$. □

Lemma 16.8. Let V be a finite-dimensional representation of a group G and let $f\colon V \to k$ be a G-invariant polynomial function. Suppose that $X \subseteq V$ is a subset such that that the orbit

$$G.X = \{g.x \mid g \in G, x \in X\}$$

is Zariski-dense in V. If $f|_X = 0$ then $f = 0$.

Proof. It follows from the G-invariance of f that $f|_{G.X} = 0$ because

$$f(g.x) = \left(g^{-1}.f\right)(x) = f(x) = 0$$

for all $g \in G$, $x \in X$. It follows that $f = 0$ because $G.X$ is Zariski dense in V. □

Proposition 16.9. If k is algebraically closed then the set of diagonalizable matrices,

$$\mathrm{Diag}_n(k) \coloneqq \{A \in \mathrm{M}_n(k) \mid A \text{ is diagonalizable}\},$$

is Zariski-dense in $\mathrm{M}_n(k)$.

Proof. Let $f\colon \mathrm{M}_n(k) \to k$ with $f|_{\mathrm{Diag}_n(k)} = 0$ and let $A \in \mathrm{M}_n(k)$. The matrix A is triangularizable over k because k is algebraically closed, so there exists some $S \in \mathrm{GL}_n(k)$ such that SAS^{-1} is an upper triangular matrix with diagonal entries $b_1, \dots, b_n \in k$ (not necessarily pairwise distinct).

We want to "deform" the matrix A to make it diagonalizable:

Let $a_1, \dots, a_n \in k$ be pairwise different (such a_i exist because k is infinite), and consider the map $M\colon k \to \mathrm{M}_n(k)$ given by

$$M(z) \coloneqq S^{-1}\left(SAS^{-1} + z\begin{bmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{bmatrix}\right)S$$

for all $z \in k$. Then $M(0) = A$, so one may think of $M(z)$ as a “deformation” of A along a parameter $z \in k$. Note that $M(z)$ has the eigenvalues $b_1 + a_1 z, \dots, b_n + a_n z$ because

$$
\begin{aligned}
SM(z)S^{-1} = SAS^{-1} + z \begin{bmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{bmatrix} &= \begin{bmatrix} b_1 & \cdots & * \\ & \ddots & \vdots \\ & & b_n \end{bmatrix} + z \begin{bmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{bmatrix} \\
&= \begin{bmatrix} b_1 + za_1 & \cdots & * \\ & \ddots & \vdots \\ & & b_n + za_n \end{bmatrix} .
\end{aligned}
$$

Any two eigenvalues $b_i + a_i z$ and $b_j + a_j z$ of $M(z)$ coincide for only one value of z, namely for $z = (b_j - b_i)/(a_i - a_j)$. It follows that $M(z)$ has pairwise different eigenvalues, and is therefore digonalizable, for all but finitely many $z \in k$.

It follows from $f|_{\mathrm{Diag}_n(k)} = 0$ that $(f \circ M)(z) = 0$ for all but finitely many $z \in k$, and therefore that $f \circ M = 0$. For $z = 0$ we find that

$$
0 = (f \circ M)(0) = f(M(0)) = f(A) .
$$

This shows that $f(A) = 0$ for every $A \in \mathrm{M}_n(k)$, i.e. that $f = 0$. □

Remark 16.10. The above proof actually shows that the set of matrices with pairwise different eigenvalues is Zariski dense if k is algebraically closed.

Remark 16.11. Proposition 16.9 can also be shown by using Lemma 16.6:

Recall from Example 9.14 that there exists a polynomial $\Delta \in k[Y_1, \dots, Y_n]$ such that a monic polynomial $X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in k[X]$ has a multiple root in k (which is algebraically closed) if and only if $\Delta(a_{n-1}, \dots, a_0) = 0$. If the characteristic polynomial of $A \in \mathrm{M}_n(k)$ is given $\chi_A(X) = X^n + s_{n-1}(A)X^{n-1} + \cdots + s_1(A)X + s_0(A)$ the the $s_i \colon \mathrm{M}_n(k) \to k$ are polynomial functions and it follows that

$$
d \colon \mathrm{M}_n(k) \to k, \quad A \mapsto \Delta(s_{n-1}(A), \dots, s_0(A))
$$

is a polynomial function. For every matrix $A \in \mathrm{M}_n(k)$ we have that

$$
\begin{aligned}
& d(A) = 0 \\
\iff & \chi_A \text{ has a multiple root} \\
\iff & A \text{ has a eigenvalue with (algebraic) multiplicity} \geq 2 ,
\end{aligned}
$$

and therefore that

$$
d(A) \neq 0 \iff A \text{ has pairwise different eigenvalues} .
$$

The set of matrices with pairwise different eigenvalues is non-empty and the non-vanishing set of d, and thus Zariski dense by Lemma 16.6.

Instead of using the fundamental theorem of symmetric functions to justify the existence of the polynomial Δ as done in Example 9.14 one can also use the following explicit construction:

- For every two polynomials $f, g \in k[X]$ with $f = a_n X^n + \cdots + a_1 X + a_0$ and $g = b_m X^m + \cdots + b_1 X + b_0$ their *Sylvester matrix* is the $((n+m) \times (n+m))$-matrix $S(f,g)$ such that
  - for $j = 1, \dots, m$ the j-th column contains the coefficients $a_n, \dots, a_0$ starting in the j-the row, and
  - for $j = m+1, \dots, m+n$ the $(m+j')$-th column contains the coefficients $b_m, \dots, b_0$ starting in the j'-th row.

  If for example $f = a_4 X^4 + a_3 X^3 + a_2 X^2 + a_1 X + a_0$ and $g = b_3 X^3 + b_2 X^2 + b_1 X + b_0$ then the Sylvester Matrix $S(f,g)$ is the (7×7)-matrix given by

$$S(f,g) = \begin{bmatrix} a_4 & & & b_3 & & & \\ a_3 & a_4 & & b_2 & b_3 & & \\ a_2 & a_3 & a_4 & b_1 & b_2 & b_3 & \\ a_1 & a_2 & a_3 & b_0 & b_1 & b_2 & b_3 \\ a_0 & a_1 & a_2 & & b_0 & b_1 & b_2 \\ & a_0 & a_1 & & & b_0 & b_1 \\ & & a_0 & & & & b_0 \end{bmatrix}.$$

  For $y = (y_{n-1}, y_{n-2}, \dots, y_0) \in k^n$ we denote by $y(X) \in k[X]$ the polynomial

$$y(X) \coloneqq y_{n-1} X^{n-1} + \cdots + y_1 X + y_0 \,.$$

  We then have for all $y \in k^n$, $z \in k^m$ that

$$S(f,g) \cdot \begin{bmatrix} y \\ z \end{bmatrix} = 0 \iff f(X) \cdot y(X) + g(X) \cdot z(X) = 0 \,,$$

  so

$$\ker S(f,g) = \left\{ \begin{bmatrix} y \\ z \end{bmatrix} \in \begin{bmatrix} k^n \\ k^m \end{bmatrix} = k^{n+m} \,\middle|\, y(X) f(X) + z(X) g(Z) = 0 \right\}$$

  It then follows that $\deg(\gcd(f,g)) = m + n - \operatorname{rank} S(f,g)$. It follows that $S(f,g)$ is invertible if and only if $\deg(\gcd(f,g)) = 0$, i.e. if and only if f, g are coprime.

- If $f \in K[X]$ is a polynomial of degree $\leq n$ then f has a multiple root in k if and only if f, f' are not coprime, i.e. if and only if $\Delta(f) \neq 0$ for

$$\Delta(f) \coloneqq \det S(f, f') \,,$$

  where Δ is polynomial in f.

For $f = X^2 + aX + b$ we have that $f' = 2X + a$ and therefore

$$\Delta(f) = \det S(f, f') = \det \begin{bmatrix} 1 & 2 & \\ a & a & 2 \\ b & & a \end{bmatrix} = a^2 + 4b - 2a^2 = 4b - a^2 \,,$$

and for $f = X^3 + aX^2 + bX + c$ we have that $f' = 3X^2 + 2aX + b$ and therefore

$$\begin{aligned}\Delta(f) = \det S(f, f') &= \det \begin{bmatrix} 1 & & 3 & & \\ a & 1 & 2a & 3 & \\ b & a & b & 2a & 3 \\ c & b & & b & 2a \\ & c & & & b \end{bmatrix} \\ &= 4a^3c - a^2b^2 - 18abc + 4b^3 + 27c^2 \,.\end{aligned}$$

Corollary 16.12 (Second Zariski density property for algebraically closed fields)**.** Let k be an algebraically closed field and let $\mathrm{GL}_n(k)$ act on $\mathrm{M}_n(k)$ by conjugation. Let $f \in \mathrm{M}_n(k) \to k$ be a $\mathrm{GL}_n(k)$-invariant polynomial function and let $D \subseteq \mathrm{M}_n(k)$ be the subset of diagonal matrices. If $f|_D = 0$ then $f = 0$.

Proof. This follows from Lemma 16.8 because the orbit $\mathrm{GL}_n(k).D = \mathrm{Diag}_n(k)$ is Zariski dense in $\mathrm{M}_n(k)$ by Proposition 16.9. □

Extension of scalars

16.13. The first of the Zariski density properties stated in Proposition 15.5 has been proven by Corollary 16.7, but we have only shown the second Zariski density property for algebraically closed fields.

To show that the second Zariski density property holds for arbitrary infinite fields we now examine how Zariski density changes under extension of scalars.

Conventions 16.14. In the following let L/k be a field extension. For every k-vector space V we denote by $V_L = L \otimes_k V$ the extension of scalars of V, and regard V as a k-linear subspace of V_L (see Appendix A1 for a short introduction to extension of scalars). If V is finite-dimensional then we abbreviate $\mathcal{P}(V) = \mathcal{P}_k(V)$ and $\mathcal{P}(V_L) = \mathcal{P}_L(V_L)$.

Lemma 16.15. Let V, W be k-vector spaces and let $X \subseteq V$ and $Y \subseteq W$ be Zariski dense. Then $X \times Y \subseteq V \times W$ is again Zariski dense.

Proof. Let $f \colon V \times W \to k$ be a polynomial function with $f|_{X \times Y} = 0$. We then have that

$$f(x, y) = 0 \qquad \text{for all } x \in X,\, y \in Y \,.$$

For fixed $x \in X$ the map $f(x, -) \colon W \to k$ is polynomial with $f(x, -)|_Y = 0$, so it follows that $f(x, -) = 0$ because Y is Zariski dense in W. This shows that

$$f(x, w) = 0 \qquad \text{for all } x \in X,\, w \in W.$$

For fixed $w \in W$ the map $f(-, w) \colon V \to k$ is polynomial with $f(-, w)|_X = 0$, so it follows that $f(-, w) = 0$ because X is Zariski dense in V. This shows that

$$f(v, w) = 0 \qquad \text{for all } v \in V,\, w \in W \,,$$

and therefore that $f = 0$. □

Corollary 16.16. The subset $k^n \subseteq L^n$ is Zariski dense over L.

Proof. This follows from Lemma 16.15 because $k \subseteq L$ is Zariski dense over L (because k is infinite). □

Corollary 16.17. Let V be a finite-dimensional k-vector space. Then V is Zariski dense in V_L over L.

Proof. Let $v_1, \dots, v_n$ be a k-basis of V. Then $1 \otimes v_1, \dots, 1 \otimes v_n$ is an L-basis of V_L. The isomorphism of L-vector spaces $\varphi\colon L^n \to V_L$ with $\varphi(e_i) = 1 \otimes v_i$ maps $k^n \subseteq L^n$ onto $\varphi(k^n) = V$. The statement now follows from Corollary 16.16 because φ is a polynomial isomorphism, since both φ and φ^{-1} are linear and therefore polynomial. □

Proposition 16.18. Let V be a finite-dimensional k-vector space.

a) Every k-polynomial map $f\colon V \to k$ extends uniquely to an L-polynomial map $\overline{f}\colon V_L \to L$ with
$$\overline{f}(1 \otimes v) = f(v)$$
for all $v \in V$.

b) The map $i\colon \mathcal{P}(V) \to \mathcal{P}(V_L)$, $f \mapsto \overline{f}$ is a homomorphism of k-algebras, which extends to an isomorphism of L-algebras
$$I\colon \mathcal{P}(V)_L \xrightarrow{\sim} \mathcal{P}(V_L)$$

c) Let $v_1, \dots, v_n$ be a k-basis of V and let $\varphi_1, \dots, \varphi_n \in \mathcal{P}(V)$ be the corresponding coordinate functions. Let $\psi_1, \dots, \psi_n \in \mathcal{P}(V_L)$ be the coordinate functions corresponding to the basis $1 \otimes v_1, \dots, 1 \otimes v_n$ of V_L.

Let $\Phi\colon \mathcal{P}(V) \to k[X_1, \dots, X_n]$ be the unique isomorphism of k-algebras with $\Phi(\varphi_i) = X_i$ for all i, and let $\Psi\colon \mathcal{P}(V_L) \to L[X_1, \dots, X_n]$ be the unique isomorphism of L-algebras with $\Psi(\psi_i) = X_i$ for all i.

Then the following diagram commutes:

$$\begin{tikzcd}
 & \mathcal{P}(V) \arrow[dl, "\text{can}"'] \arrow[dr, "i"] \arrow[dd, "\Phi"] & \\
\mathcal{P}(V)_L \arrow[rr, "I"] \arrow[dd, "\Phi_L"'] & & \mathcal{P}(V_L) \arrow[dd, "\Psi"] \\
 & k[X_1, \dots, X_n] \arrow[dl, "\text{can}"'] \arrow[dr, hook] & \\
k[X_1, \dots, X_n]_L \arrow[rr, "\sim"] & & L[X_1, \dots, X_n]
\end{tikzcd}$$

(16.1)

Proof. Let $v_1, \dots, v_n$ be a k-basis of V.

There exists a polynomial $p \in k[X_1, \dots, X_n]$ with

$$f(\lambda_n v_1 + \dots + \lambda_n v_n) = p(\lambda_1, \dots, \lambda_n)$$

for all $\lambda_1, \dots, \lambda_n \in k$ because the the map f is k-polynomial. We can regard p as a polynomial $p \in L[X_1, \dots, X_n]$. With respect to the L-basis $1 \otimes v_1, \dots, 1 \otimes v_n$ of V_L the polynomial p then defines an L-polynomial map $\overline{f} \colon V_L \to L$ given by

$$\overline{f}(\lambda_1(1 \otimes v_1) + \dots + \lambda_n(1 \otimes v_n)) = p(\lambda_1, \dots, \lambda_n)$$

for all $\lambda_1, \dots, \lambda_n \in L$. We have for every $v \in V$ with $v = \sum_{i=1}^n \lambda_i v_i$ that

$$\overline{f}(1 \otimes v) = \overline{f}(\lambda_1(1 \otimes v_1) + \dots + \lambda_n(1 \otimes v_n)) = p(\lambda_1, \dots, \lambda_n) = f(v) \,.$$

The uniqueness of $\overline{f}$ follows from the Zariski density of $V \subseteq V_L$ over L.

Note that the diagram

$$\begin{tikzcd}
\mathcal{P}(V) \arrow[r, "i"] \arrow[d, "\Phi"'] & \mathcal{P}(V_L) \arrow[d, "\Psi"] \\
k[X_1, \dots, X_n] \arrow[r, hook] & L[X_1, \dots, X_n]
\end{tikzcd}$$

commutes by the above construction of i. It follows that

$$i \colon \mathcal{P}(V) \xrightarrow{\Phi} k[X_1, \dots, X_n] \hookrightarrow L[X_1, \dots, X_n] \xrightarrow{\Psi^{-1}} \mathcal{P}(V_L)$$

is a composition of k-algebra homomorphisms, and thus a k-algebra homomorphism itself. It follows (from Lemma A1.31) that i extends uniquely to an L-algebra homomorphism $I \colon \mathcal{P}(V)_L \to \mathcal{P}(V_L)$ such that the diagram

$$\begin{tikzcd}
\mathcal{P}(V)_L \arrow[r, dashed, "I"] & \mathcal{P}(V_L) \\
\mathcal{P}(V) \arrow[u, "\mathrm{can}"] \arrow[ur, "i"'] &
\end{tikzcd}$$

commutes.

For the commutativity of the diagram (16.1) we note that on elements we get the following diagram, which does commute:

$$\begin{tikzcd}
 & \varphi_i \arrow[dl, mapsto] \arrow[dr, mapsto] \arrow[dd, mapsto] & \\
1 \otimes \varphi_i \arrow[rr, mapsto] \arrow[dd, mapsto] & & \psi_i \arrow[dd, mapsto] \\
 & X_i \arrow[dl, mapsto] \arrow[dr, mapsto] & \\
1 \otimes X_i \arrow[rr, mapsto] & & X_i
\end{tikzcd}$$

It follows that the diagram (16.1) commutes because the occuring maps are all algebra homomorphisms and these elements generate their respective algebras (as L-algebras for the upper four in the front, and as k-algebras for the two in the back).

It remains to show that I is an isomorphism. This follows from the commutativity of the diagram (16.1) because

$$I\colon \mathcal{P}(V)_L \xrightarrow{\Phi_L} k[X_1,\dots,X_n]_L \xrightarrow{\sim} L[X_1,\dots,X_n] \xrightarrow{\Phi^{-1}} \mathcal{P}(V_L)$$

is a composition of isomorphisms. □

Definition 16.19. Let V be a finite-dimensional k-vector space.

a) For $X \subseteq V$ the *vanishing ideal of* X is given by

$$\mathcal{I}_k(X) \coloneqq \{f \in \mathcal{P}_k(V) \mid f(x) = 0 \text{ for all } x \in X\}\,.$$

We also write $\mathcal{I}(X)$ instead of $\mathcal{I}_k(X)$ if the field k is clear from the context.

b) For every point $a \in V$ we set

$$\mathfrak{m}_a \coloneqq \mathcal{I}(\{a\}) = \{f \in \mathcal{P}(V) \mid f(a) = 0\}\,.$$

Lemma 16.20. Let V be a finite-dimensional k-vector space.

a) For every subset $X \subseteq V$ the vanishing ideal $\mathcal{I}(X)$ is an ideal in $\mathcal{P}(V)$.

b) If $X \subseteq Y \subseteq V$ then $\mathcal{I}(Y) \subseteq \mathcal{I}(X)$. Furthermore, X is Zariski-dense in Y if and only if $\mathcal{I}(X) = \mathcal{I}(Y)$.

c) Let $\{X_i\}_{i\in I}$ be a collection of subsets $X_i \subseteq V$. Then

$$\mathcal{I}\left(\bigcup_{i\in I} X_i\right) = \bigcap_{i\in I} \mathcal{I}(X_i)\,.$$

Lemma 16.21. For $a = (a_1,\dots,a_n) \in k^n$ the ideal $\mathfrak{m}_a$ is maximal and given by

$$\mathfrak{m}_a = (X_1 - a_1,\dots,X_n - a_n)\,,$$

where we identify $\mathcal{P}(k^n)$ with $k[X_1,\dots,X_n]$ as explained in 7.11.

Proof. The ideal $\mathfrak{m} \coloneqq (X_1 - a_1,\dots,X_n - a_n)$ is maximal:

We consider first the case $a_1 = \dots = a_n = 0$. Then $\mathfrak{m} = (X_1,\dots,X_n)$ has a k-basis given by all monomials $X_1^{\alpha_1}\cdots X_n^{\alpha_n} \neq 1$. It follows that the k-algebra $k[X_1,\dots,X_n]/\mathfrak{m}$ has a basis given by the single element $\overline{1}$, and is therefore one-dimensional. It follows that $k[X_1,\dots,X_n]/\mathfrak{m} \cong k$ as k-algebras. Then $\mathfrak{m}$ is maximal because k is a field.

For general $a \in k^n$ we observe that there exists an automorphism of k-algebras $\Phi\colon k[X_1,\dots,X_n] \to k[X_1,\dots,X_n]$ with $\Phi(X_i) = X_i + a_i$ for all $i = 1,\dots,n$. Then $\Phi(\mathfrak{m}) = (X_1,\dots,X_n)$ is maximal as shown above so $\mathfrak{m}$ itself is also maximal.

The maximal ideal $\mathfrak{m}$ is contained in the vanishing ideal $\mathfrak{m}_a$ because $X_i - a_i \in \mathfrak{m}_a$ for every $i = 1,\dots,n$. It follows that $\mathfrak{m}_a = \mathfrak{m}$ or $\mathfrak{m}_a = \mathcal{P}(V)$ because the ideal $\mathfrak{m}$ is maximal. The case $\mathfrak{m}_a = \mathcal{P}(V)$ cannot occur because $\mathfrak{m}_a$ is a proper ideal, as it does not contain $1 \in \mathcal{P}(V)$. Hence $\mathfrak{m}_a = \mathfrak{m}$. □

Corollary 16.22. Let V be a finite-dimensional k-vector space and $X \subseteq V \subseteq V_L$. Then

$$\mathcal{I}_k(X)_L = \mathcal{I}_L(X)\,,$$

where we identify $\mathcal{P}(V)_L$ with $\mathcal{P}(V_L)$ as explained in Proposition 16.18.

Proof. By choosing a basis of V we may identify in a consistent way

- the k-vector space V with k^n,
- the L-vector space V_L with L^n,
- the k-algebra $\mathcal{P}(V)$ with $k[X_1, \dots, X_n]$,
- the L-algebras $\mathcal{P}(V)_L$ and $\mathcal{P}(V_L)$ with $L[X_1, \dots, X_n]$

by Proposition 16.18. For every point $a \in k^n$ we then have that

$$\begin{aligned}\mathcal{I}_k(\{a\})_L &= L \otimes_k \mathcal{I}_k(\{a\}) \\ &= L \otimes_k (X_1 - a_1, \dots, X_n - a_n)_{k[X_1,\dots,X_n]} \\ &= (X_1 - a_1, \dots, X_n - a_n)_{L[X_1,\dots,X_n]} \\ &= \mathcal{I}_L(\{a\})\,.\end{aligned}$$

For every subset $X \subseteq W$ we therefore have that

$$\begin{aligned}\mathcal{I}_k(X)_L = L \otimes_k \mathcal{I}_k(X) = L \otimes_k \mathcal{I}_k\left(\bigcup_{x \in X} \{x\}\right) = L \otimes_k \left(\bigcap_{x \in X} \mathcal{I}_k(\{x\})\right) \\ = \bigcap_{x \in X} (L \otimes_k \mathcal{I}_k(\{x\})) = \bigcap_{x \in X} \mathcal{I}_k(\{x\})_L = \bigcap_{x \in X} \mathcal{I}_L(\{x\}) = \mathcal{I}_L(X)\,.\end{aligned}$$

This proves the claim. □

Corollary 16.23. Let V be a finite-dimensional k-vector space and let

$$X \subseteq Y \subseteq V \subseteq V_L\,.$$

If X is Zariski dense in Y over k then X is also Zariski dense in Y over L.

Proof. We have that $\mathcal{I}_k(X) = \mathcal{I}_k(Y)$ because X is Zariski dense in Y over k. It follows that

$$\mathcal{I}_L(X) = \mathcal{I}_k(X)_L = \mathcal{I}_k(Y)_L = \mathcal{I}_L(Y)\,,$$

which shows that X is Zariski dense in Y over L. □

Lemma 16.24 (Transitivity of Zariski density)**.** Let V be a finite-dimensional k-vector space and let $X \subseteq Y \subseteq Z \subseteq V$. If X is Zariski-dense in Y and Y is Zariski-dense in Z, then X is Zariski-dense in Z.

Proof. It follows for every polynomial function $f \colon V \to k$ from $f|_X = 0$ that $f|_Y = 0$ and thus $f|_Z = 0$. □

16.25. Let V be a finite-dimensional k-vector space. To prove the last part of the upcoming proposition we need to slightly generalize our notion of polynomial maps:

For a subset $X \subseteq V$ a function $X \to k$ is *polynomial* if it is the restriction of a polynomial function $V \to k$. If X is Zariski dense in $Y \subseteq V$ and $f \colon Y \to k$ is a polynomial function with $f|_X = 0$ it then follows that $f = 0$.

For a subset $X \subseteq V$ a function $f \colon X \to k$ is *rational* if there exists polynomial functions $g, h \colon X \to k$ with $h(x) \neq 0$ for every $x \in X$ and

$$f(x) = \frac{g(x)}{h(x)}$$

for every $x \in X$. Note that a rational function $f = g/h$ vanishes if and only if its numerator g vanishes. If X is Zariski dense in $Y \subseteq V$ and $f \colon Y \to k$ is rational with $f|_X = 0$, it thus follows that $f = 0$.

Both the polynomial functions $X \to k$ and rational functions $X \to k$ form k-algebras via pointwise addition and scalar multiplication of functions. We will come back to this generalization of polynomial functions in subsection 21.

Warning 16.26. While every polynomial function $f \colon X \to k$ can be extended to a polynomial function $V \to k$ the same does not hold for rational functions. Consider for example the subset $\mathrm{GL}_n(k) \subseteq \mathrm{M}_n(k)$ and the rational function $f \colon \mathrm{GL}_n(k) \to k$ given by

$$f(A) \coloneqq \frac{1}{\det(A)} \,.$$

Suppose that f could be extended to a rational function $\hat{f} \colon \mathrm{M}_n(k) \to k$. Then the function $g \colon \mathrm{M}_n(k) \to k$ given by $g(A) = \hat{f}(A)\det(A) - 1$ is also rational and satisfies $g|_{\mathrm{GL}_n(k)} = 0$. It then follows that $g = 0$ because $\mathrm{GL}_n(k)$ is Zariski dense in $\mathrm{M}_n(k)$, and therefore that $\hat{f}(A)\det(A) = 1$ for all $A \in \mathrm{M}_n(k)$. But this is not possible.

(This shows more generally that f cannot be extended to a rational function $X \to k$ for any subset $X \subseteq \mathrm{M}_n(k)$ with $\mathrm{GL}_n(k) \subsetneq X$.)

Proposition 16.27. For the subsets $\mathrm{GL}_n(k), \mathrm{GL}_n(L), \mathrm{SL}_n(k), \mathrm{SL}_n(L)$ of $\mathrm{M}_n(L)$ we have that

a) $\mathrm{GL}_n(k)$ is Zariski dense in $\mathrm{M}_n(L)$ over L,

b) $\mathrm{GL}_n(k)$ is Zariski dense in $\mathrm{GL}_n(L)$ over L,

c) $\mathrm{SL}_n(k)$ is Zariski dense in $\mathrm{SL}_n(L)$ over L.

Proof.

a) We have already seen that $\mathrm{GL}_n(k)$ is Zariski dense in $\mathrm{M}_n(k)$ over k. It follows that $\mathrm{GL}_n(k)$ is Zariski dense in $\mathrm{M}_n(k)$ over L by Corollary 16.23, with $\mathrm{M}_n(k)$ being Zariski dense in $\mathrm{M}_n(L)$ over L by Corollary 16.16. It follows from the transitivity of Zariski density that $\mathrm{GL}_n(k)$ is Zariski dense in $\mathrm{M}_n(L)$ over L.

b) This follows from part a) of this proposition.

c) Let $f\colon \mathrm{M}_n(L) \to L$ be a polynomial function with $f|_{\mathrm{SL}_n(k)} = 0$. Consider the map

$$p\colon \mathrm{GL}_n(L) \to \mathrm{SL}_n(L)\,, \quad A \mapsto \begin{bmatrix} \det(A)^{-1} & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix} \cdot A\,,$$

which divides the first row of A by $\det(A)$. For every $A \in \mathrm{SL}_n(L)$ we have that $p(A) = A$, so we may think of p as a (rational) retraction of $\mathrm{GL}_n(L)$ onto $\mathrm{SL}_n(L)$. Note that p restricts to a map $p|_{\mathrm{GL}_n(k)}\colon \mathrm{GL}_n(k) \to \mathrm{SL}_n(k)$.

The map p is rational in every coordinate, so it follows that the composition $f|_{\mathrm{SL}_n(L)} \circ p\colon \mathrm{GL}_n(L) \to L$ is rational. For every $A \in \mathrm{GL}_n(k)$ we have that $p(A) \in \mathrm{SL}_n(k)$ and therefore

$$(f|_{\mathrm{SL}_n(L)} \circ p)(A) = f(p(A)) = 0\,.$$

It follows that $(f|_{\mathrm{SL}_n(L)} \circ p)(A) = 0$ for every $A \in \mathrm{GL}_n(L)$ because $\mathrm{GL}_n(k)$ is Zariski-dense in $\mathrm{GL}_n(L)$ over L. It then follows for every $A \in \mathrm{SL}_n(L)$ that

$$f(A) = f(p(A)) = (f|_{\mathrm{SL}_n(L)} \circ p)(A) = 0\,.$$

This shows that $f|_{\mathrm{SL}_n(L)} = 0$. □

Corollary 16.28. Let $\mathrm{GL}_n(k), \mathrm{GL}_n(L), \mathrm{SL}_n(k), \mathrm{SL}_n(L)$ act on $\mathrm{M}_n(k)$, resp. $\mathrm{M}_n(L)$ by conjugation. Let $f\colon \mathrm{M}_n(k) \to k$ be a k-polynomial function and let $\overline{f}\colon \mathrm{M}_n(L) \to L$ be the unique L-polynomial extension of f (as described in Proposition 16.18).

a) If f is $\mathrm{GL}_n(k)$-invariant then $\overline{f}$ is $\mathrm{GL}_n(L)$-invariant.

b) If f is $\mathrm{SL}_n(k)$-invariant then $\overline{f}$ is $\mathrm{SL}_n(L)$-invariant.

Proof. We consider the map $\Phi\colon \mathrm{M}_n(L) \times \mathrm{M}_n(L) \to L$ given by

$$\Phi(A, B) = \overline{f}(AB) - \overline{f}(BA)$$

for all $A, B \in \mathrm{M}_n(L)$. We then have that

$$f \text{ is } \mathrm{GL}_n(k)\text{-invariant} \iff \Phi|_{\mathrm{GL}_n(k) \times \mathrm{M}_n(k)} = 0$$

and similarly that

$$\overline{f} \text{ is } \mathrm{GL}_n(L)\text{-invariant} \iff \Phi|_{\mathrm{GL}_n(L) \times \mathrm{M}_n(L)} = 0$$

Both $\mathrm{GL}_n(k) \subseteq \mathrm{GL}_n(L)$ and $\mathrm{M}_n(k) \subseteq \mathrm{M}_n(L)$ are Zariski dense over L, so it follows from Lemma 16.15 that $\mathrm{GL}_n(k) \times \mathrm{M}_n(k) \subseteq \mathrm{GL}_n(L) \times \mathrm{M}_n(L)$ is Zariski dense over L. It therefore follows that

$$\Phi|_{\mathrm{GL}_n(k) \times \mathrm{M}_n(k)} = 0 \implies \Phi|_{\mathrm{GL}_n(L) \times \mathrm{M}_n(L)} = 0\,.$$

This shows part a).

By replacing GL_n by SL_n in the above argumentation we find that part b) holds. □

Proposition 16.29 (Second Zariski density property)**.** Let k be an infinite field and let $\mathrm{GL}_n(k)$ act on $\mathrm{M}_n(k)$ by conjugation. Let $f\colon \mathrm{M}_n(k) \to k$ be a $\mathrm{GL}_n(k)$-invariant polynomial function and let $D \subseteq \mathrm{M}_n(k)$ be the subset of diagonal matrices. If $f|_D = 0$ then $f = 0$.

Proof. Let L be an algebraic closure of k and let $\mathrm{GL}_n(L)$ acts on $\mathrm{M}_n(L)$ by conjugation. Let $\overline{f}\colon \mathrm{M}_n(L) \to L$ be the unique L-polynomial extension of f . Then $\overline{f}$ is $\mathrm{GL}_n(L)$-invariant by Corollary 16.28.

Let $D_k \subseteq \mathrm{M}_n(k)$ and $D_L \subseteq \mathrm{M}_n(L)$ be the subsets of diagonal matrices. It follows from $f|_{D_k} = 0$ that $\overline{f}|_{D_k} = 0$, from which it further follows that $\overline{f}|_{D_L} = 0$ because D_k is Zariski-dense in D_L over L by Corollary 16.16. It follows from the second Zariski density property for algebraically closed fields that $\overline{f} = 0$ and therefore that $f = 0$. □

Proposition 16.30. Let $\mathrm{GL}_n(k)$ and $\mathrm{SL}_n(k)$ act on $\mathrm{M}_n(k)$ by conjugation. Then

$$\mathcal{P}(\mathrm{M}_n(k))^{\mathrm{GL}_n(k)} = \mathcal{P}(\mathrm{M}_n(k))^{\mathrm{SL}_n(k)} .$$

Proof. Suppose first that k is algebraically closed. If A, B are $\mathrm{GL}_n(k)$-conjugated then they are already $\mathrm{SL}_n(k)$-conjugated because for $S \in \mathrm{GL}_n(k)$ with $SAS^{-1} = B$ there exists some $\alpha \in k$ with $\alpha^n = 1/\det(S)$, and for $T := S/\alpha \in \mathrm{SL}_n(k)$ we then have that TAT^{-1}. It follows that the actions of $\mathrm{GL}_n(k)$ and $\mathrm{SL}_n(k)$ on $\mathrm{M}_n(k)$ have the same orbits. This proves the proposition for k algebraically closed.

Let k be any infinite field. We need to show that every $\mathrm{SL}_n(k)$-invariant polynomial map $f\colon \mathrm{M}_n(k) \to k$ is already $\mathrm{GL}_n(k)$-invariant. Let L be an algebraic closure of k and let $\overline{f}\colon \mathrm{M}_n(L) \to L$ be the unique L-linear extension of f. Then $\overline{f}$ is $\mathrm{SL}_n(L)$-invariant by Corollary 16.28. The map $\overline{f}$ is therefore already $\mathrm{GL}_n(L)$-invariant as shown above. Then f, which is now the restriction of $\overline{f}$ to $\mathrm{M}_n(k)$, is $\mathrm{GL}_n(k)$-invariant. □

17. Finiteness Results on Invariant Rings

17.1. We now return to the topic of invariant rings. Throughout the previous sections we have determined the following examples:

Group	**Repre-sentation**	**Action**	**Invariant Ring (up to iso.)**	**generators**
S_n	k^n	permutation of coordinates	$k[X_1, \dots, X_n]$	$e_1, \dots, e_n$, $h_1, \dots, h_n$, $p_1, \dots, p_n$ (for suitable k)
$\mathrm{GL}_n(k)$ $\mathrm{SL}_n(k)$	$\mathrm{M}_n(k)$	conjugation	$k[X_1, \dots, X_n]$	$s_1, \dots, s_n$, $\mathrm{tr}_1, \dots, \mathrm{tr}_n$ (for suitable k)
$\mathrm{GL}_n(k)$	$\mathrm{M}_n(k)$	(left) mult.	k	$\emptyset$
$\mathrm{SL}_n(k)$			$k[X]$	det

We finish this chapter by giving two finiteness results on the invariant ring $\mathcal{P}(V)^G$, one by Hilbert and one by E. Noether. The main results of this section are taken from [KP96, §1.6] and generalize some aspects of the above examples.

Conventions 17.2. In the following k denotes an infinite field.

17.3. Let V be finite-dimensional representation of a group G. The main observation behind both theorems is that the invariant ring $\mathcal{P}(V)^G$ inherits a grading from $\mathcal{P}(V)$:

If $f \in \mathcal{P}(V)$ is homogenous of degree $d \geq 0$, then for every $g \in G$ the polynomial map $g.f \in \mathcal{P}(V)$ is again polynomial of degree d because

$$(g.f)(\lambda v) = f(g^{-1}.(\lambda v)) = f(\lambda g^{-1}.v) = \lambda^d f(g^{-1}.v) = \lambda^d (g.f)(v)$$

for all $\lambda \in k$, $v \in V$. It follows for the grading $\mathcal{P}(V) = \bigoplus_{d \geq 0} \mathcal{P}(V)_d$ that $\mathcal{P}(V)_d$ is a subrepresentation for every $d \geq 0$. From this it follows that

$$\mathcal{P}(V)^G = \left(\bigoplus_{d \geq 0} \mathcal{P}(V)_d \right)^G = \bigoplus_{d \geq 0} \mathcal{P}(V)^G_d \,.$$

with $\mathcal{P}(V)^G_d = \mathcal{P}(V)^G \cap \mathcal{P}(V)_d$. That $\mathcal{P}(V)^G_d \mathcal{P}(V)^G_{d'} \subseteq \mathcal{P}(V)^G_{d+d'}$ is a combination of

$$\mathcal{P}(V)_d \mathcal{P}(V)_{d'} \subseteq \mathcal{P}(V)_{d+d'} \quad \text{and} \quad \mathcal{P}(V)^G \mathcal{P}(V)^G \subseteq \mathcal{P}(V)^G \,.$$

17.1. A Theorem by Hilbert

Theorem 17.4 (Hilbert)**.** Let V be a finite-dimensional representation of a group G. If $\mathcal{P}(V)$ is completely reducible (as a representation of G) then the coordinate ring $\mathcal{P}(V)^G$ is finitely generated as a k-algebra.

Example 17.5. Let V is a finite-dimensional representation of a finite groups G, and suppose that $\operatorname{char}(k) \nmid |G|$. Then $\mathcal{P}(V)^G = \bigoplus_{d \geq 0} \mathcal{P}(V)^G_d$ is a decomposition into finite-dimensional subrepresentations and it follows from Maschke's theorem that $\mathcal{P}(V)^G$ decomposes into irreducible subrepresentations. The invariant ring $\mathcal{P}(V)^G$ is then a finitely-generated k-algebra by Hilbert's theorem.

17.6. The proof of Hilbert's theorem uses two main tools: The so-called *irrelevant ideal* $\bigoplus_{d \geq 1} \mathcal{P}(V)^G_d$ and the *Reynolds operator* $\mathcal{P}(V) \to \mathcal{P}(V)^G$, whose existence relies on the complete reducibility of $\mathcal{P}(V)$.

Basics on Homogeneous Ideals

Definition 17.7. Let $A = \bigoplus_{d \geq 0} A_d$ be a graded k-algebra. An ideal $I \trianglelefteq A$ is *homogeneous* or *graded* if it is of the form $I = \bigoplus_{d \geq 0} I_d$ for linear subspaces $I_d \subseteq A_d$.

Remark 17.8. One of the nice things about graded ideals (which we will not need) is that when $A = \bigoplus_{d \geq 0} A_d$ is a graded k-algebra and $I \trianglelefteq A$ is a homogeneous two-sided ideal with homogeneous parts $I = \bigoplus_{d \geq 0} I_d$, then the quotient algebra A/I inherts a grading from A which is given by $(A/I)_d = A_d / I_d$ for all $d \geq 0$. The canonical projection $A \to A/I$ is then a homomorphism of graded k-algebras.

Lemma 17.9. Let $A = \bigoplus_{d\geq 0} A_d$ be a graded k-algebra and let $I \trianglelefteq A$ be an ideal.

a) The subset $\bigoplus_{d\geq 0}(I \cap A_d)$ is again an ideal in A.

b) The following conditions are equivalent:

   1) The ideal I is homogenous.

   2) The ideal I satisfies $I = \bigoplus_{d\geq 0}(I \cap A_d)$.

   3) The ideal I contains for every $x \in I$ all homogeneous parts of x.

   4) The ideal I is generated by homogeneous elements.

c) If the ideal I is homogenous and finitely generated then it is already finitely generated by homogeneous elements.

Proof.

a) We have for the k-linear subspace $J := \bigoplus_{d\geq 0}(I \cap A_d) = \sum_{d\geq 0}(I \cap A_d) \subseteq A$ that

$$\begin{aligned} AJ = \left(\sum_{d\geq 0} A_d\right)\left(\sum_{d'\geq 0}(I \cap A_{d'})\right) &= \sum_{d,d'\geq 0}[A_d(I \cap A_{d'})] \\ \subseteq \sum_{d,d'\geq 0}[A_d I \cap A_d A_{d'}] \subseteq \sum_{d,d'\geq 0}[I \cap A_{d+d'}] &\subseteq \sum_{d\geq 0}(I \cap A_d) = J\,. \end{aligned}$$

b) 1) $\implies$ 2) For the homogeneous parts $I = \bigoplus_{d\geq 0} I_d$ we have that $I \cap A_d = I_d$ for every $d \geq 0$ and thus $I = \bigoplus_{d\geq 0}(I \cap A_d)$.

   2) $\implies$ 1) For the k-linear subspaces $I_d := I \cap A_d$ we have that $I = \bigoplus_{d\geq 0} I_d$.

   1) $\implies$ 3) If $x = \sum_{d\geq 0} x_d$ is the decomposition into homogeneous parts then $x_d \in I_d \subseteq I$ for every $d \geq 0$.

   3) $\implies$ 4) If I is homogeneous with generating set $(x_i)_{i\in I}$ then we can replace each generator x_i by its homogeneous parts to obtain a homogeneous generating set for I.

   4) $\implies$ 2) Suppose that I is generated by a family $(x_i)_{i\in I}$ of homogeneous elements. Then $J = \bigoplus_{d\geq 0}(I\cap A_d)$ is again an ideal in A by part a) and $\bigoplus_{d\geq 0}(I\cap A_d)$ contains all x_i. It follows that $J \subseteq I \subseteq J$ and thus $I = J$.

c) We see from the proof of the implication 3) $\implies$ 4) that every finite generating set of I leads to a finite generating set of I which consists of homogeneous elements. □

Definition 17.10. For a graded k-algebra $A = \bigoplus_{d\geq 1}$ the two-sided ideal

$$A_+ := \bigoplus_{d\geq 1} A_d$$

is the *irrelevant ideal.*

Proposition 17.11. Let $A = \bigoplus_{d \geq 0} A_d$ be a graded k-algebra which is commutative. Let $(x_i)_{i \in I}$ be a family of elements $x_i \in A$ which are homogeneous of degree ≥ 1. Then the following are equivalent:

a) The irrelevant ideal A_+ is generated by the $(x_i)_{i \in I}$ over A.

b) The family $(x_i)_{i \in I}$ generates A as an A_0-algebra.

c) The elements of the form $\prod_i x_i^{n_i}$ (with $n_i = 0$ for all but finitely many $i \in I$) generate A is an A_0-module.

d) For every degree $d \geq 0$ the A_0-module A_d is generated by the elements of the form $\prod_i x_i^{n_i}$ which are of degree d.

Proof.

a) $\implies$ b) Let $A' = A_0[x_i \,|\, i \in I]$ be the A_0-subalgebra of A generated by the x_i. We show by induction over the degree d that $A_d \subseteq A'$ for all $d \geq 0$. For $d = 0$ we have that $A_d = A_0 \subseteq A'$ by definition of A'.

Suppose that $d \geq 1$ and that $A_0, \dots, A_{d-1} \subseteq A'$, i.e. A' contains all elements of degree $\leq d-1$. Let $x \in A_d$. Then $x \in A_+$, so we may write $x = \sum_{i \in I} a_i x_i$ for some coefficients $a_i \in A$. Every coefficient a_i decomposes into homogeneous parts $a_i = \sum_{d' \geq 0} a_{i,d'}$, so we have that

$$x = \sum_{i \in I} a_i x_i = \sum_{i \in I} \sum_{d' \geq 0} a_{i,d'} x_i = \sum_{d' \geq 0} \sum_{i \in I} a_{i,d'} x_i \,.$$

If x_i is homogeneous of degree $d_i \geq 1$, then we find in degree $d' = d$ that

$$x = \sum_{i \in I} a_{i,d-d_i} x_i \,.$$

The coefficients $a_{i,d-d_i}$ are homogeneous of degree $d - d_i \leq d-1$ and therefore contained in A' by induction hypothesis. The elements x_i are contained in A' by definition of A'. It follows that $x = \sum_{i \in I} a_{i,d-d_i} x_i \in A'$.

b) $\iff$ c) This holds because $A_0[x_i \,|\, i \in I]$, the A_0-subalgebra generated by the x_i, is generated by the products $\prod_{i \in I} x_i^{n_i}$ as an A_0-module.

c) $\iff$ d) This follows because from the homogeneity of the elements $\prod_{i \in I} x_i^{n_i}$ and the directness of the sum $A = \bigoplus_{d \geq} A_d$.

d) $\implies$ a) Let J be the A-ideal generated by the x_i, i.e. $J = \sum_{i \in I} A x_i$. Then $J \subseteq A_+$ because the element x_i are homogeneous of degree ≤ 1 and therefore contained in the A-ideal A_+.

To see the other inclusion note that the elements of the form $\prod_{i \in i} x_i^{n_i}$ of degree $d \geq 1$ are contained in J: Because this element has degree ≥ 1 there exists some $j \in I$ with $n_j \geq 1$ and it follows that

$$\prod_{i \in I} x_i^{n_i} = \prod_{i \in I} x_i^{n_i - \delta_{i,j}} \cdot x_j \in A x_j \subseteq J \,.$$

It follows that J contains the A_0-generators of A_d, which is why

$$A_d \subseteq A_0 J \subseteq AJ = J \,.$$

This shows that $A_d \subseteq J$ for all $d \geq 1$ and therefore that $A_+ \subseteq J$. □

Corollary 17.12. Let $A = \bigoplus_{d \geq 0} A_d$ be a graded k-algebra which is commutative. Then A is finitely generated by homogeneous elements as an A_0-algebra if and only if the irrelevant ideal A_+ is finitely generated.

Remark 17.13. Let $A = \bigoplus_{d \geq 0} A_d$ be graded k-algebra which is commutative with $A_0 = k$. Then A_+ is a maximal ideal in A, and it is the unique homogeneous ideal with this property. This can be seen as follows:

1) If L is a field which is also a graded k-algebra $L = \bigoplus_{d \geq 0} L_d$, then L is already concentrated in degree 0: Otherwise there would exist some non-zero $a \in L$ which is homogeneous of degree $d \geq 1$. For $b = 1/a$ we then have the decomposition into homogeneous parts $b = \sum_{d \geq 0} b_d$. We have that

$$1 = ba = \sum_{d' \geq 0} b_{d'} a$$

with $1 \in L_0$ and $b_{d'} a \in L_{d'+d}$ for all $d' \geq 0$. It follows that $d = 0$ and $b_{d'} = 0$ for all $d' \geq 1$.

(We have shown more generally that for an M-graded algebra $A = \bigoplus_{m \in M} A_m$, where M is cancellative additive monoid, the inverse of a homogeneous unit of degree $m \in M$ is again homogenous, but of degree $-m$. Since we are only working with $\mathbb{N}$-graded algebras, all units must have degree 0.)

2) If $\mathfrak{m} \trianglelefteq A$ is an ideal which is both maximal and homogeneous then $\mathfrak{m}$ is already of the form

$$\mathfrak{m} = \mathfrak{m}_0 \oplus A_1 \oplus A_2 \oplus \cdots$$

for a maximal ideal $\mathfrak{m}_0 \trianglelefteq A_0$:

The quotient $A/\mathfrak{m}$ is a field which (as mentioned in Remark 17.8) inherits a grading from A given by $(A/\mathfrak{m})_d = A_d/\mathfrak{m}_d$ for all $d \geq 0$. It follows from the previous step that $(A/\mathfrak{m})_d = 0$ for all $d \geq 1$ and therefore that $\mathfrak{m}_d = A_d$ for all $d \geq 1$. That $\mathfrak{m}_0 \trianglelefteq A_0$ is a maximal ideal then follows from $A_0/\mathfrak{m}_0 \cong A/\mathfrak{m}$ being a field.

3) Since A_0 is a field it follows that $\mathfrak{m}_0 = 0$, and therefore that $\mathfrak{m} = \bigoplus_{d \geq 1} A_d = A_+$.

The claim also holds for $\mathbb{Z}$-graded commutative algebras because the first step can still be generalized to this case. A proof of this can be found in [NV04, Remark 1.3.10].

17.14. If V is a finite-dimensional representation of a group G then $\mathcal{P}(V)^G_0 = k$, so it follows from Corollary 17.12 that $\mathcal{P}(V)^G$ is finitely generated as a k-algebra if and only if the irrelevant ideal $\bigoplus_{d \geq 1} \mathcal{P}(V)^G_d$ is finitely generated over $\mathcal{P}(V)^G$. To show this we would like to use that every ideal $I \trianglelefteq \mathcal{P}(V)$ is finitely generated because $\mathcal{P}(V)$

is noetherian. To establish a suitable connection between the ideal of $\mathcal{P}(V)$ and the ideals of $\mathcal{P}(V)^G$ we will now construct a projection $\mathcal{P}(V) \to \mathcal{P}(V)^G$, the so called Reynolds operator, whose existence relies on the complete reducibility of $\mathcal{P}(V)$ as a representation of G.

The Reynolds Operator

Proposition 17.15. Let V be completely reducible representation of a group G.

a) There exists a unique decomposition $V = V^G \oplus N$ into subrepresentations.

b) The only morphism of representations $N \to V^G$ is the zero morphism.

c) There exists a unique G-equivariant projection $\pi\colon V \to V^G$, i.e. morphism of representations with $\pi(x) = x$ for every $x \in V^G$.

Proof. Let $V = \bigoplus_{i \in I} V_i$ be a decomposition into irreducible subrepresentations $V_i \subseteq V$ and let

$$J = \{ j \in I \mid V_j \text{ is a trivial representation} \} .$$

We set $N = \bigoplus_{i \in I \smallsetminus J} V_i$. For every $j \in J$ we have that $V_j^G = V_j$ and for every $i \in I \smallsetminus J$ we have that $V_i^G = 0$ because V_i^G is a proper subrepresentation of V_i with V_i being irreducible. It follows that

$$V^G = \left(\bigoplus_{i \in I} V_i \right)^G = \bigoplus_{i \in I} V_i^G = \bigoplus_{j \in J} V_j ,$$

and therefore that

$$V = \bigoplus_{i \in I} V_i = \left(\bigoplus_{j \in J} V_j \right) \oplus \left(\bigoplus_{i \in I \smallsetminus J} V_i \right) = V^G \oplus N .$$

This shows the existence for part a).

We show that part b) holds for the decomposition $V = V^G \oplus N$ constructed above: Let $f\colon N \to V^G$ be a morphism of representations. For every $i \in I \smallsetminus J$ the restriction $f|_{V_i}\colon V_i \to V$ is either injective or 0 because V_i is irreducible. If $f|_{V_i}$ were injective then V_i would be isomorphic to a subrepresentation of V^G and would therefore be a trivial representation, contradicting $i \notin J$. It follows that $f|_{V_i} = 0$ for every $i \in I \smallsetminus J$, and therefore that $f = 0$. This shows part b) for the given decomposition $V = V^G \oplus N$.

Let $\pi\colon V \to V^G$ be the projection along N. Then π is a k-linear projection by construction and G-equivariant because $V = V^G \oplus N$ is a decomposition into subrepresentations. This shows the existence for part c).

It follows that every G-equivariant projection $\pi'\colon V \to V^G$ satisfies the conditions

$$\pi'|_{V^G} = \mathrm{id}_{V^G} \quad \text{and} \quad \pi|_N = 0 ,$$

and π' is already uniquely determined by this conditions because $V = V^G \oplus N$. This shows that the uniqueness for part c).

The uniqueness for part a) follows from the uniqueness of π because $N = \ker \pi$. □

Definition 17.16. If V is a completely reducible representation of a group G then the unique G-equivariant projection $\pi\colon V \to V^G$ is the *Reynolds operator* of V.

Example 17.17. If G is a finite group with $\operatorname{char}(k) \nmid |G|$, then every finite-dimensional representation V of G is completely reducible by Maschke's theorem. The Reynolds operator $V \to V^G$ is then given by the projection onto invariants

$$\pi\colon V \to V^G, \quad v \mapsto \frac{1}{|G|} \sum_{g \in G} g.v$$

as introduced in Remark 5.11 because π is a G-equivariant projection onto V^G.

Lemma 17.18. Let A be a k-algebra and let G be a group acting on A by algebra automorphisms such that A is completely reducible as a representation. Then the Reynolds operator $\pi\colon A \to A^G$ is a homomorphism of left and right A^G-modules.

Proof. For every $h \in A^G$ the map $\hat{h}\colon A \to A$, $a \mapsto ha$ is G-equivariant because

$$g.\hat{h}(a) = g.(ha) = (g.h)(g.a) = h(g.a) = \hat{h}(g.a)$$

for all $g \in G$, $a \in A$. It follows that the map

$$H\colon A \to A^G, \quad a \mapsto h\pi(a) - \pi(ha) = \hat{h}(\pi(a)) - \pi(\hat{h}(a))$$

is a morphism of representations. It follows from part b) of Proposition 17.15 that H is uniquely determined by the restriction $H|_{A^G}$ (because for the direct complement N with $A = A^G \oplus N$ we have that $H|_N = 0$). For every $a \in A^G$ we have that

$$H(a) = h\pi(a) - \pi(ha) = ha - ha = 0$$

and therefore $H = 0$. This shows that $\pi(ha) = h\pi(a)$ for all $a \in A$.

This shows that π is a homomorphism of left A^G-modules. In can be shown in the same way that π is a homomorphism of right A^G-modules. □

The Proof Itself

Proof of Hilbert's theorem. Let $A \coloneqq \mathcal{P}(V)$. We have that $A_0^G = k$ so by Corollary 17.12 we need to show that the irrelevant ideal $\mathfrak{m} \coloneqq \bigoplus_{d \geq 1} A_d^G$ is finitely generated over A^G.

Because $\mathcal{P}(V)$ is completely reducible as a representation of G we can consider the Reynolds operator $\pi\colon A \to A^G$. Then π is a homomorphism of right A^G-modules by Lemma 17.18, so that we have that

$$\pi(h) = h \quad \text{and} \quad \pi(fh) = \pi(f)h$$

for all $f \in A$, $h \in A^G$. For every ideal $I \trianglelefteq A^G$ we denote by AI the A-ideal generated by I and note that

$$\pi(AI) = \pi(A)\pi(I) = A^G I = I\,. \tag{17.1}$$

We therefore have that $\mathfrak{m} = \pi(A\mathfrak{m})$. The ideal $A\mathfrak{m}$ is finitely generated because $A = \mathcal{P}(V)$ is noetherian, so there exist $f_1, \ldots, f_n \in \mathfrak{m}$ with $A\mathfrak{m} = Af_1 + \cdots + Af_n$. It follows that

$$\mathfrak{m} = \pi(Af_1 + \cdots + Af_n) = \pi(A)\pi(f_1) + \cdots + \pi(A)\pi(f_n) = A^G f_1 + \cdots + A^G f_n\,,$$

which shows that $\mathfrak{m}$ is finitely generated over A^G. □

Remark 17.19. The ideal $\mathcal{P}(V)\mathcal{P}(V)^G_+$ from the proof of Hilbert's theorem, i.e. the ideal in $\mathcal{P}(V)$ generated by all homogeneous invariants of positive degree, is known as the *Hilbert ideal.* The proof of Hilbert's theorem can roughly be described as follows:

$$\begin{aligned} &\text{The } k\text{-algebra } \mathcal{P}(V) \text{ is noetherian} \\ \Longrightarrow\ &\text{the Hilbert ideal } \mathcal{P}(V)\mathcal{P}(V)^G_+ \text{ is finitely generated} \\ \xRightarrow[\text{Reynolds}]{}\ &\text{the irrelevant ideal } \textstyle\bigoplus_{d\geq 1} \mathcal{P}(V)^G_d \text{ is finitely generated} \\ \Longrightarrow\ &\text{the } k\text{-algebra } \mathcal{P}(V)^G \text{ is finitely generated.} \end{aligned}$$

17.2. A Theorem by Noether

17.20. Example 17.5 shows that the invariant ring $\mathcal{P}(V)^G$ is finitely generated whenever G is finite with $\operatorname{char}(k) \nmid |G|$, but we do not have any restrictions on the needed generators. The following theorem by E. Noether ([Noe15]) gives a bound on the degree of the generators[1]:

Theorem 17.21 (Noether)**.** Let V be a finite-dimensional representation of a finite group G over a field k of characteristic $\operatorname{char}(k) = 0$. Then the invariant ring $\mathcal{P}(V)^G$ is generated as a k-algebra by the invariants of degree $\leq |G|$.

Proof. We may assume w.l.o.g. that $V = k^n$ and thus identify $\mathcal{P}(V)$ with the polynomial ring $k[X_1, \ldots, X_n] =: A$. For every $g \in G$ and every multi-index $\mu = (\mu_1, \ldots, \mu_n)$ let

$$m_\mu := \sum_{g\in G} g.(X_1^{\mu_1} \cdots X_n^{\mu_n}) \in A^G\,.$$

The elements m_μ, $\mu \in \mathbb{N}^n$ form a k-generating set of A^G. This can be seen in (at least) two similar ways:

[1] To quote Noether herself: “Im folgenden soll ein ganz elementarer [...] Endlichkeitsbesweis der Invarianten *endlicher* Gruppen gebracht werden, der zugleich eine *wirkliche Angabe des vollen Systems* liefert; während der gewöhnliche, auf das Hilbertsche Theorem von der Modulbasis [...] sich stützende Beweis nur Existenzbeweis ist.” (Taken from [Noe15].)

- The Reynolds operator
$$R\colon A \to A^G, \quad f \mapsto \frac{1}{|G|}\sum_{g\in G} g.f$$
is k-linear and surjective. The monomials $X_1^{\mu_1}\cdots X_n^{\mu_n}$ with $\mu \in \mathbb{N}^n$ form a k-basis of A, so it follows that the images $R(X_1^{\mu_1}\cdots X_n^{\mu_n})$ form a k-generating set of A^G. Up to the coefficient $|G| \in k^\times$ these are precisely the m_μ.

- We may write $f \in A^G \subseteq A$ as $f = \sum_\mu f_\mu X_1^{\mu_1}\cdots X_n^{\mu_n}$. Then
$$\begin{aligned} f = R(f) &= \frac{1}{|G|}\sum_{g\in G} g.f = \frac{1}{|G|}\sum_{g\in G} g.\left(\sum_\mu f_\mu X_1^{\mu_1}\cdots X_n^{\mu_n}\right) \\ &= \frac{1}{|G|}\sum_\mu f_\mu \sum_{g\in G} g.(X_1^{\mu_1}\cdots X_n^{\mu_n}) = \frac{1}{|G|}\sum_\mu f_\mu m_\mu \,. \end{aligned}$$

The elements m_μ, $\mu \in \mathbb{N}^n$ are homogeneous of degree $|\mu| = \mu_1 + \cdots + \mu_n$. For $h := |G|$ we thus need to show that A^G is generated as a k-algebra by those m_μ with $|\mu| \leq h$.

Let $G = \{g_1, \dots, g_h\}$. For every $j \geq 0$ let $p_j = \sum_{i=1}^h Y_i^j \in k[Y_1, \dots, Y_h]$ be the j-th power symmetric polynomial. For the elements
$$y_i := (g_i.X_1)Z_1 + \cdots + (g_i.X_n)Z_n \in A[Z_1, \dots, Z_n]$$
with $i = 1, \dots, h$ we then have that
$$\begin{aligned} p_j(y_1, \dots, y_n) &= \sum_{i=1}^h y_i^j = \sum_{i=1}^h [(g_i.X_1)Z_1 + \cdots + (g_i.X_n)Z_n]^j \\ &= \sum_{i=1}^h \sum_{|\mu|=j} \binom{j}{\mu_1, \dots, \mu_n} [(g_i.X_1)Z_1]^{\mu_1} \cdots [(g_i.X_n)Z_n]^{\mu_n} \\ &= \sum_{i=1}^h \sum_{|\mu|=j} \binom{j}{\mu_1, \dots, \mu_n} (g_i.X_1)^{\mu_1} \cdots (g_i.X_n)^{\mu_n} Z_1^{\mu_1} \cdots Z_n^{\mu_n} \\ &= \sum_{|\mu|=j} \binom{j}{\mu_1, \dots, \mu_n} \left[\sum_{i=1}^h (g_i.X_1)^{\mu_1} \cdots (g_i.X_n)^{\mu_n}\right] Z_1^{\mu_1} \cdots Z_n^{\mu_n} \\ &= \sum_{|\mu|=j} \binom{j}{\mu_1, \dots, \mu_n} \left[\sum_{i=1}^h g_i.(X_1^{\mu_1} \cdots X_n^{\mu_n})\right] Z_1^{\mu_1} \cdots Z_n^{\mu_n} \\ &= \sum_{|\mu|=j} \binom{j}{\mu_1, \dots, \mu_n} m_\mu Z_1^{\mu_1} \cdots Z_n^{\mu_n} \,. \end{aligned}$$

This shows that m_μ is, up to the factor

$$C_\mu := \binom{|\mu|}{\mu_1, \dots, \mu_n} ,$$

the coefficient of the monomial $Z_1^{\mu_1} \cdots Z_n^{\mu_n}$ in $p_j(y_1, \dots, y_n)$.

We know that for every $j > h$ the j-th power symmetric polynomial p_j can be expressed as a k-polynomial in the power symmetric polynomials $p_1, \dots, p_h$. It follows that the coefficients of $p_j(y_1, \dots, y_n)$ are k-polynomials in the coefficients of $p_1(y_1, \dots, y_n), \dots, p_h(y_1, \dots, y_n)$. This shows that $C_\mu m_\mu$ can be expressed as a k-polynomial in the terms $C_\nu m_\nu$ with $|\nu| \leq h$. Because the factor C_μ is invertible in k it follows that m_μ is a k-polynomial in the m_ν with $|\nu| \leq h$. □

Remark 17.22. Let V be a finite-dimensional representation of a finite group G. The *Noether number* $\beta(V, G)$ is the minimal degree $d \geq 0$ such that the invariant ring $\mathcal{P}(V)^G$ is generated as a k-algebra by the elements of degree $\leq d$. We also set

$$\beta(G) := \max\{\beta(V, G) \mid V \text{ is a finite-dimensional representation of } G \text{ over } k\} .$$

Noether's theorem shows that $\beta(G) \leq |G|$ if $\operatorname{char}(k) = 0$, which is known as the *Noether bound*. This result can be strengthened in various ways:

- It has since then been proven by Fogarty [Fog01] that Noether's theorem holds under the weaker assumption that $|G|$ is invertible in k.
- Fleischmann [Fle00] showed the more general result that if $H \trianglelefteq G$ is a normal subgroup whose index $[G : H]$ is invertible in k, then $\beta(V, G) \leq \beta(V, H) \cdot [G : H]$. (For $G = H$ we get the above result.)
- In the case of $\operatorname{char}(k) = 0$ it was proven by Schmid [Sch91] that $\beta(G) \leq \beta(H)[G : H]$ for every subgroup $H \leq G$, and that $\beta(G) \leq \beta(H)\beta(G/H)$ if $H \trianglelefteq G$ is normal.
- Schmid also showed for $\operatorname{char}(k) = 0$ that $\beta(G) < |G|$ if G is not cyclic, and that $\beta(\mathbb{Z}/n) = n$ if k contains a primitive n-th root of unity. ([Sch91] seems to only consider the case that k is algebraically closed, but according to [Weh06, Theorem 3.7] the bound $\beta(G) < |G|$ is shown for $\operatorname{char}(k) = 0$.)
- According to [Weh06, Remark 3.6] and [DK15, Remark 3.2.5] it is not know if $\beta(G) \leq \beta(H)[G : H]$ holds for every subgroup $H \leq G$ if $\operatorname{char}(k) \nmid [G : H]$.

Another Proof

17.23. Noether herself gives in [Noe15] two proofs of her theorem. The proof presented above is the second one. We also give an overview of the first proof, simply because the author spent some time on trying to understand it and does not want his effort go to waste.

The main tool in this proof is the *fundamental theorem of vector invariants for the symmetric group*. We use the formulation from [Fle00], where the result is attributed to [Wey46] (the author thinks that this maybe can be found in [Wey46, II.3]).

Theorem 17.24 (Fundamental theorem of vector invariants for the symmetric group)**.** Let k be a field with $\mathrm{char}(k) = 0$. Let $n, m \geq 1$ and let S_n act on

$$V := \underbrace{k^m \times \cdots \times k^m}_{n}$$

by permutation of the entries, i.e. the action is given by

$$\sigma.\left(y^{(1)}, \ldots, y^{(n)}\right) = \left(y^{(\sigma^{-1}(1))}, \ldots, y^{(\sigma^{-1}(n))}\right) .$$

for all $\sigma \in S_n$, $y^{(1)}, \ldots, y^{(n)} \in k^m$. We identify $\mathcal{P}(V)$ with the polynomial ring $k[X_{ij} \,|\, i = 1, \ldots, m, j = 1, \ldots, n]$ such that X_{ij} gives the i-th coordinates of the j-th vector, i.e.

$$X_{ij}(y^{(1)}, \ldots, y^{(n)}) = y_i^{(j)}$$

for all i, j; the action of S_n on $\mathcal{P}(V)$ is then given by

$$\sigma.X_{ij} = X_{i\sigma(j)}$$

for all $\sigma \in S_n$ and i, j. Then the invariant ring $\mathcal{P}(V)^{S_n}$ is generated by the coefficients of the monomials $Y_1^{\alpha_1} \cdots Y_n^{\alpha_n}$ in the expression

$$\prod_{j=1}^{n} \left(1 + \sum_{i=1}^{m} X_{ij} Y_i\right) ,$$

and this generators are homogeneous of degree $\leq n$.

Example 17.25. We examine the fundamental theorem for some special cases:

a) Consider the case $m = 1$. Then $V = k^n$ (consisting of row vectors), the action of S_n on k^n is the usual permutation action via $\sigma.e_i = e_{\sigma(i)}$ and the invariant ring $\mathcal{P}(k^n)^{S_n} = k[X_1, \ldots, X_n]^{S_n}$ is the ring of symmetric polynomials. We have that

$$\prod_{j=1}^{n} (1 + X_i Y) = 1 + e_1(X_1, \ldots, X_n)Y + \cdots + e_n(X_1, \ldots, X_n)Y^n ,$$

so the theorem states that $k[X_1, \ldots, X_n]^{S_n}$ is generated by the elementary symmetric polynomials. This is precisely the fundamental theorem of symmetric functions.

b) Consider the case $n = 1$. Then $V = k^m$ (cosisting of column vectors) and the action of $S_n = S_1$ on k^m is just the trivial one. Then $\mathcal{P}(k^m)^{S_1} = k[X_1, \ldots, X_m]$. We have that

$$1 + \sum_{i=1}^{m} X_i Y_i = 1 + X_1 Y_1 + \cdots + X_m Y_m ,$$

so the theorem states that $k[X_1, \ldots, X_m]$ is generated by $X_1, \ldots, X_m$.

c) Consider the case $n = m = 2$, so that $\mathcal{P}(k^2 \times k^2) = k[X_{11}, X_{12}, X_{21}, X_{22}]$. We then have that

$$\begin{aligned}&\prod_{j=1}^{2}\left(1+\sum_{i=1}^{2} X_{ij}Y_i\right)\\ &= (1 + X_{11}Y_1 + X_{21}Y_2)(1 + X_{12}Y_1 + X_{22}Y_2)\\ &= 1 + (X_{11} + X_{12})Y_1 + (X_{21} + X_{22})Y_2\\ &\quad + X_{11}X_{12}Y_1^2 + (X_{11}X_{22} + X_{12}X_{21})Y_1Y_2 + X_{21}X_{22}Y_2^2\,,\end{aligned}$$

so the theorem states that $k[X_{11}, X_{12}, X_{21}, X_{22}]^{S_2}$ is generated by

$$X_{11} + X_{12}\,, \quad X_{21} + X_{22}\,, \quad X_{11}X_{12}\,, \quad X_{21}X_{22}\,, \quad X_{11}X_{22} + X_{12}X_{21}\,.$$

Here $X_{11}+X_{12}$ and $X_{12}X_{12}$ are the elementary symmetric polynomials in the upper coordinates, $X_{21} + X_{22}$ and $X_{21}X_{22}$ are the elementary symmetric polynomials in the lower coordinates, and $X_{11}X_{22} + X_{12}X_{21}$ is a new kind of invariant. (If one identifies $k^2 \times k^2$ with $\mathrm{M}(2 \times 2, k)$ then $X_{11}X_{22} + X_{12}X_{21}$ is the permanent.)

Noether's first proof of her theorem. We assume w.l.o.g. that $V = k^n$. Let $h \coloneqq |G|$ and $G = \{g_1, \dots, g_h\}$. For every $x \in k^n$ let $x^{(i)} \coloneqq g_i.x$ for every $i = 1, \dots, h$. For $f \in \mathcal{P}(k^n)$ we then have that $f(x) = f(x^{(i)})$ for every $i = 1, \dots, h$ and therefore

$$f(x) = \frac{1}{h}\sum_{i=1}^{h} f(x^{(i)})\,.$$

(This can be seen as a use of the Reynolds operator.) Note that the right hand side of this equation is a symmetric polynomial in the vectors $x^{(1)}, \dots, x^{(h)}$. We therefore define the maps

$$F\colon \underbrace{k^n \times \cdots \times k^n}_{h} \to k\,, \quad (y^{(1)}, \dots, y^{(n)}) \mapsto \frac{1}{h}\sum_{i=1}^{h} f(y^{(i)})$$

and

$$P\colon k^n \to k^n \times \cdots \times k^n\,, \quad x \mapsto (x^{(1)}, \dots, x^{(n)})\,.$$

Both maps are polynomial with F being symmetric, P being homogeneous of degree 1, and $f = F \circ P$. (One may think about $P(x)$ as recording the permuations of x under the action of G.)

We can now apply the fundamental theorem of vector invariants of the symmetric group to F: We identify $\mathcal{P}((k^n)^{\times h})$ with $B \coloneqq k[Y_{ij} \mid i = 1, \dots, n, j = 1, \dots, h]$. In $B[Z_1, \dots, Z_n]$ we then have the identity

$$\prod_{j=1}^{h}\left(1+\sum_{i=1}^{n} Y_{ij}Z_i\right) = 1 + \sum_{\substack{\alpha,\alpha_1,\dots,\alpha_n \geq 0\\ \alpha+\alpha_1+\cdots+\alpha_n = h\\ \alpha \neq h}} G_{\alpha,\alpha_1,\dots,\alpha_n} Z_1^{\alpha_1} \cdots Z_n^{\alpha_n}$$

with the coefficients $G_{\alpha,\alpha_1,\dots,\alpha_n} \in B$ being generators of the invariant ring B^{S_h} and homogeneous of degree $\leq h$. We can now express F as a polynomial in the $G_{\alpha,\alpha_1,\dots,\alpha_n}$.

This then expresses $f = F \circ P$ as a polynomial in the invariants $G_{\alpha,\alpha_1,\dots,\alpha_n} \circ P$, each of which is a homogeneous invariant of degree $\leq h$ (because $G_{\alpha,\alpha_1,\dots,\alpha_n}$ and P are homogeneous of degree d and 1). To see that the $G_{\alpha,\alpha_1,\dots,\alpha_n} \circ P \colon k^n \to k$ are indeed G-invariants note that the tupels $P(x)$ and $P(g.x)$ differ only in the order of they entries, which then implies that $G_{\alpha,\alpha_1,\dots,\alpha_n}(P(x)) = G_{\alpha,\alpha_1,\dots,\alpha_n}(P(g.x))$. □

17.26. We use the notation of Remark 17.22. Let k be a field of characteristic 0.

If V is a finite-dimensional k-vector space then S_n acts on $V^{\times n}$ by permutation of the entries, and the fundamental theorem of vector invariants for the symmetric group shows that

$$\beta(V^{\times n}, S_n) \leq n\,.$$

The above proof of Noether's theorem explains how this implies the Noether bound $\beta(G) \leq |G|$ for every finite group G.

The main idea to derive the Noether bound from the fundamental theorem is the following construction:

If V is a finite-dimensional representation of G then for $h \coloneqq |G|$ we can embedd the group $G = \{g_1, \dots, g_h\}$ into the symmetric group S_h by Cayley's theorem; one such embedding $\varphi \colon G \to S_h$ is given by

$$g_i \cdot g = g_{\varphi(g)^{-1}(i)}$$

for all $g \in G$ and $i = 1, \dots, n$ (this embedding corresponds to the regular right action of G on itself). Then S_h acts on $V^{\times h}$ by permutation of the entries via

$$\sigma.(v_1, \dots, v_h) = (v_{\sigma^{-1}(1)}, \dots v_{\sigma^{-1}(h)})$$

for all $\sigma \in S_h$, $i = 1, \dots, n$. We also have an embedding

$$\Phi \colon V \to V^{\times h}\,, \quad v \mapsto (g_1.v, \dots, g_h.v)\;.$$

These embeddings are compatible in the sense that

$$\begin{aligned}\varphi(g).\Phi(v) &= \varphi(g).(g_1.v, \dots, g_h.v) = \big(g_{\varphi(g)^{-1}(1)}.v, \dots, g_{\varphi(g)^{-1}(h)}.v\big) \\ &= ((g_1 \cdot g).v, \dots, (g_h \cdot g).v) = (g_1.(g.v), \dots, g_h.(g.v)) = \Phi(g.v)\,.\end{aligned}$$

So the action of G on V factors through the action of S_h on $V^{\times h}$, i.e. the following diagramm commutes:

$$\begin{tikzcd} G \times V \arrow[r] \arrow[d, "\varphi \times \Phi"'] & V \arrow[d, "\Phi"] \\ S_h \times V^{\times h} \arrow[r] & V^{\times h} \end{tikzcd}$$

In the case of $\mathrm{char}(k) = 0$ we see via the formula

$$f(x) = \frac{1}{|G|} \sum_{g \in G} f(g.x)$$

that every G-invariant polynomial function $f\colon V \to k$ extends to an S_h-invariant polynomial function $V^{\times h} \to k$. So by understanding these S_h-invariant polynomial functions we can also gain a better understanding of the G-invariant polynomial functions.

Zariski Closed Subsets

18. Basic Definitions

18.1. In this chapter we will give an introduction to the Zariski topology and affine algebraic varieties.

We will start by proving *Hilbert's Nullstellensatz* (or rather *Nullstellensätze*), which will give us some understanding of the vanishing sets of polynomials in multiple variables.

We will then introduce the *Zariski topology* of a finite-dimensional vector space V. We will show some basic properties of this topology and together with Hilbert's Nullstellensätze we will see how topological properties of V correspond to algebraic properties of the coordinate ring $\mathcal{P}(V)$.

Lastly we show that the Zariski closed subsets of V can be regarded as (geometric) spaces in their own right, so called *affine algebraic varieties.* We show how many of the notions and statements which have previuosly only been considered for finite-dimensional vector spaces generalize to affine algebraic varieties.

Conventions 18.2. In this section we require all fields to be infinite. We also fix a finite-dimesional k-vector space V.

Definition 18.3. For every subset $S \subseteq \mathcal{P}(V)$ the set

$$\mathcal{V}(S) \coloneqq \{x \in V \mid f(x) = 0 \text{ for all } x \in S\}$$

is the *zero set* or *vanishing set* or *algebraic set* or *Zariski closed subset* or *affine algebraic variety* associated to S.

Example 18.4.

a) For $X^2 + Y^2 - 1 \in \mathbb{R}[X, Y]$ the vanishing set $\mathcal{V}(X^2 + Y^2 - 1)$ is the unit circle.

b) For $XY \in k[X, Y]$ the vanishing set $\mathcal{V}(XY)$ union of the two coordinate axis.

c) We have that $\mathcal{V}(\emptyset) = \mathcal{V}(0) = V$.

d) We have that $\mathcal{V}(\mathcal{P}(V)) = \mathcal{V}(1) = \emptyset$.

Lemma 18.5. For all subsets $S, T \subseteq \mathcal{P}(V)$ with $S \subseteq T$ we have that $\mathcal{V}(S) \supseteq \mathcal{V}(T)$.

Lemma 18.6. For every subset $S \subseteq \mathcal{P}(V)$ we have that $\mathcal{V}(S) = \mathcal{V}(I)$ for the generated ideal $I \coloneqq (S)$.

Proof. It follows from $S \subseteq I$ that $\mathcal{V}(I) \subseteq \mathcal{V}(S)$. To show the other inclusion let $x \in \mathcal{V}(S)$. Then $g(x) = 0$ for every $g \in S$. Every $f \in I$ is of the form $f = \sum_{i=1}^{n} h_i g_i$ for some $h_i \in \mathcal{P}(V)$, $g_i \in S$ and it follows that $f(x) = 0$. This shows that $x \in \mathcal{V}(I)$ and therefore that $\mathcal{V}(S) \subseteq \mathcal{V}(I)$. □

Corollary 18.7. For every algebraic subset $X \subseteq V$ there exists an ideal $I \trianglelefteq \mathcal{P}(V)$ with $X = \mathcal{V}(I)$.

Proof. By definition of an algebraic set there exist a subset $S \subseteq \mathcal{P}(V)$ with $X = \mathcal{V}(S)$ and for the ideal $I \coloneqq (S)$ we have that $X = \mathcal{V}(I)$ by Lemma 18.6. □

Corollary 18.8. Every algebraic subset $X \subseteq V$ can be described by finitely many polynomial equations, i.e. there exist $f_1, \dots, f_n \in \mathcal{P}(V)$ with $X = \mathcal{V}(f_1, \dots, f_n)$.

Proof. There exists an ideal $I \trianglelefteq \mathcal{P}(V)$ with $X = \mathcal{V}(I)$ by Corollary 18.7. The k-algebra $\mathcal{P}(V) \cong k[X_1, \dots, X_{(\dim V)}]$ is notherian by Hilbert's basis theorem so there exist finitely many $f_1, \dots, f_n \in I$ with $I = (f_1, \dots, f_n)$. It follows from Lemma 18.6 that $X = \mathcal{V}(f_1, \dots, f_n)$. □

19. The Nullstellensätze

19.1. We can associate to every subset $X \subseteq V$ its vanishing ideal $\mathcal{I}(X) \trianglelefteq \mathcal{P}(V)$, and to every ideal $I \trianglelefteq \mathcal{P}(V)$ its vanishing set $\mathcal{V}(I) \subseteq V$, resulting in maps $\mathcal{I}, \mathcal{V}$ as follows:

$$\begin{tikzcd}\{\text{subsets } X \subseteq V\} \arrow[r, shift left, "\mathcal{I}"] & \{\text{ideals } I \trianglelefteq \mathcal{P}(V)\} \arrow[l, shift left, "\mathcal{V}"]\end{tikzcd}$$

In general the maps $\mathcal{I}, \mathcal{V}$ will neither be injective nor surjective. But we will see in this section that when we restrict our attention to suitable classes (or rather sets) of subsets $X \subseteq V$ and ideals $I \trianglelefteq \mathcal{P}(V)$ the maps $\mathcal{V}$ and $\mathcal{I}$ not only restrict to bijections, but that they become inverse to each other.

Lemma 19.2. For every subset $X \subseteq V$ and ideal $I \trianglelefteq \mathcal{P}(V)$ we have that

$$X \subseteq \mathcal{V}(I) \iff \mathcal{I}(X) \supseteq I\,.$$

Proof. Both conditions state that $f(x) = 0$ for all $f \in I$, $x \in X$. □

Lemma 19.3. Let $X \subseteq V$ be a subset and let $I \trianglelefteq \mathcal{P}(V)$ be an ideal. Then

a) $X \subseteq \mathcal{V}(\mathcal{I}(X))$,

b) $I \subseteq \mathcal{I}(\mathcal{V}(I))$,

c) $\mathcal{I}(\mathcal{V}(\mathcal{I}(X))) = \mathcal{I}(X)$,

d) $\mathcal{V}(\mathcal{I}(\mathcal{V}(I))) = \mathcal{V}(I)$.

Proof.

a) This is by Lemma 19.2 equivalent to $\mathcal{I}(X) \supseteq \mathcal{I}(X)$.

b) This is by Lemma 19.2 equivalent to $\mathcal{V}(I) \subseteq \mathcal{V}(I)$.

c) It follows from $X \subseteq \mathcal{V}(\mathcal{I}(X))$ that $\mathcal{I}(X) \supseteq \mathcal{I}(\mathcal{V}(\mathcal{I}(X)))$ because $\mathcal{I}$ is order-reversing. That $\mathcal{I}(X) \subseteq \mathcal{I}(\mathcal{V}(\mathcal{I}(X)))$ is equivalent to $\mathcal{V}(\mathcal{I}(X)) \supseteq \mathcal{V}(\mathcal{I}(X))$ by Lemma 19.2.

d) It follows from $I \subseteq \mathcal{I}(\mathcal{V}(I))$ that $\mathcal{V}(I) \supseteq \mathcal{V}(\mathcal{I}(\mathcal{V}(I)))$ because $\mathcal{V}$ is order-reversing. That $\mathcal{V}(I) \subseteq \mathcal{V}(\mathcal{I}(\mathcal{V}(I)))$ is equivalent to $\mathcal{I}(\mathcal{V}(I)) \supseteq \mathcal{I}(\mathcal{V}(I))$ by Lemma 19.2. □

Definition 19.4. An ideal $I \trianglelefteq \mathcal{P}(V)$ is a *vanishing ideal* if $I = \mathcal{I}(X)$ for some $X \subseteq V$.

Corollary 19.5. The maps $\mathcal{I}$, $\mathcal{V}$ restrict to the following mutually inverse bijections:

$$\begin{tikzcd}
\left\{\begin{matrix} \text{algebraic subsets} \\ X \subseteq V \end{matrix}\right\} \arrow[r, shift left, "\mathcal{I}"] & \left\{\begin{matrix} \text{vanishing ideals} \\ I \trianglelefteq \mathcal{P}(V) \end{matrix}\right\} \arrow[l, shift left, "\mathcal{V}"]
\end{tikzcd}$$

i.e. for every algebraic subset $X \subseteq V$ we have that

$$\mathcal{V}(\mathcal{I}(X)) = X\,,$$

and for every vanishing ideal $I \trianglelefteq \mathcal{P}(V)$ we have that

$$\mathcal{I}(\mathcal{V}(I)) = I\,.$$

Proof. The two identities are just reformulations of parts c), d) of Lemma 19.3. □

Lemma 19.6. An ideal $\mathfrak{m} \trianglelefteq \mathcal{P}(V)$ is of the form $\mathfrak{m} = \mathfrak{m}_a$ for some $a \in V$ if and only if it is both a maximal ideal and a vanishing ideal.

Proof. The ideal $\mathfrak{m}_a$ is maximal and it is a vanishing ideal because $\mathfrak{m} = \mathcal{I}(a)$.

Suppose on the other hand that $\mathfrak{m}$ is both a maximal ideal and a vanishing ideal. Then $\mathcal{I}(\mathcal{V}(\mathfrak{m})) = \mathfrak{m}$ by Corollary 19.5 because $\mathfrak{m}$ is a vanishing ideal. It then follows that $\mathcal{V}(\mathfrak{m}) \neq \emptyset$ because otherwise $\mathfrak{m} = \mathcal{I}(\emptyset) = \mathcal{P}(V)$, which contradicts $\mathfrak{m}$ being a proper ideal. It follows that there exists some $a \in \mathcal{V}(\mathfrak{m})$. Then

$$\mathfrak{m} = \mathcal{I}(\mathcal{V}(\mathfrak{m})) \subseteq \mathcal{I}(a) = \mathfrak{m}_a$$

and it follows that $\mathfrak{m} = \mathfrak{m}_a$ because both $\mathfrak{m}$ and $\mathfrak{m}_a$ are maximal. □

Corollary 19.7. The maps $\mathcal{I}, \mathcal{V}$ restrict to the following mutually inverse bijections:

$$\begin{tikzcd}
\left\{\begin{matrix} \text{algebraic subsets} \\ X \subseteq V \end{matrix}\right\} \arrow[r, shift left, "\mathcal{I}"] & \left\{\begin{matrix} \text{vanishing ideals} \\ I \trianglelefteq \mathcal{P}(V) \end{matrix}\right\} \arrow[l, shift left, "\mathcal{V}"] \\
\left\{\ \text{points } a \in V\ \right\} \arrow[u, phantom, sloped, "\subseteq"] \arrow[r, shift left, "\mathcal{I}"] & \left\{\begin{matrix} \text{vanishing ideals} \\ \mathfrak{m} \trianglelefteq \mathcal{P}(V) \\ \text{which are maximal} \end{matrix}\right\} \arrow[u, phantom, sloped, "\subseteq"] \arrow[l, shift left, "\mathcal{V}"]
\end{tikzcd}$$

Proof. This follows from Corollary 19.5 because by Lemma 19.6 the vanishing ideals which correspond to points $a \in V$ are precisely the vanishing ideals which are also maximal. □

Remark 19.8 (Galois connections)**.** We will use this opportunity to introduce the notion of a *Galois connections*, although we will not use it in the rest of the text. Let $(A, \leq)$, $(B, \leq)$ be two partially ordered sets.

a) An *antitone Galois connection* consists of two functions $f \colon A \to B$, $g \colon B \to A$ which are order-reversing, i.e. $f(a) \geq f(a')$ for all $a \leq a'$ and $g(b) \geq g(b')$ for all $b \leq b'$, such that
$$a \leq g(b) \iff f(a) \geq b \tag{19.1}$$
for all $a \in A$, $b \in B$; the condition (19.1) may also be expressed as
$$a \leq g(b) \iff b \leq f(a)\,.$$
Lemma 19.2 states that $\mathcal{I}, \mathcal{V}$ form a Galois connection (between suitable sets). Lemma 19.3 generalizes for an arbitrary Galois connection to

a') $a \leq g(f(a))$ for every $a \in A$,

b') $b \leq f(g(b))$ for every $b \in B$,

c') $f(g(f(a))) = f(a)$ for every $a \in A$,

d') $g(f(g(b))) = g(b)$ for every $b \in B$,

and Corollary 19.5 generalizes to f, g restricting to mutually inverse order-reversing bijections between the sets
$$\{f(a) \mid a \in A\} \qquad \text{and} \qquad \{g(b) \mid b \in B\}\,.$$
Note that the roles of f and g are symmetric, in the sense that $((A, \leq), (B, \leq), f, g)$ is an antitone Galois connection if and only if $((B, \leq), (A, \leq), g, f)$ is an antitone Galois connection. One may visualize an antitone Galois-connection as follows:
$$\begin{tikzcd} (A, \leq) \arrow[r, shift left, "f"] & (B, \leq) \arrow[l, shift left, "g"] \end{tikzcd}$$

b) Instead of *antitone* Galois connections, one can also consider *monotone* Galois connections. The condititiion of f, g being order-reversing is then replaced by the requirement of f, g being order-preserving, i.e. monotone, and the condititiion (19.1) is adjusted to
$$a \leq g(b) \iff f(a) \leq b\,.$$
Note that this requirement is not symmetric in f and g: If $((A, \leq), (B, \leq), f, g)$ is a monotone Galois connection then $((B, \leq), (A, \leq), g, f)$ is not necessarily a monotone Galois connection. This non-symmetry is reflected in the fact that f is referred to as the *left adjoint* and g is referred to as the *right adjoint* of this

(monotone) Galois connection. The consequences a'), c'), d') still hold, but b') has to be replaced by

$$f(g(b)) \leq b\,.$$

The maps f, g still restrict to mutually inverse bijections as above. One may visualize a monotone Galois connection with left adjoint f and right adjoint g as follows:

$$\begin{tikzcd}(A, \leq) \arrow[r, bend left, "f"] \arrow[r, phantom, "\perp"] & (B, \leq) \arrow[l, bend left, "g"]\end{tikzcd}$$

c) We have the following connections between antitone and monoton Galois connections:

$$\begin{tikzcd}(A, \leq) \arrow[r, bend left, "f"] \arrow[r, phantom, "\perp"] & (B, \leq) \arrow[l, bend left, "g"]\end{tikzcd} \quad\iff\quad \begin{tikzcd}(A, \leq) \arrow[r, shift left, "f"] & (B, \leq^{\mathrm{op}}) \arrow[l, shift left, "g"]\end{tikzcd}$$

Here $\leq^{\mathrm{op}}$ denotes the partial order given by

$$x \leq^{\mathrm{op}} y \iff x \geq y\,.$$

d) One can think about the partially ordered sets $(A, \leq)$ and $(B, \leq)$ as categories $\mathcal{A}, \mathcal{B}$ in the usual way, i.e. the objects of $\mathcal{A}$ (resp. $\mathcal{B}$) are the elements of A (resp. of B) and for all $x, y \in \mathcal{A}$ (resp. $x, y \in \mathcal{B}$) there exists a unique morphism $x \to y$ if $x \leq y$, and no morphism $x \to y$ otherwise.

A pair of order-preserving maps $f\colon A \to B$, $g\colon B \to A$ can be regarded as a pair of (covariant) functors $F\colon \mathcal{A} \to \mathcal{B}$ and $G\colon \mathcal{B} \to \mathcal{A}$, whose action on objects are given by the maps f, g and whose action on morphisms is the only possible one. Then f, g form a monotone Galois connection with f left adjoint to g if and only if the functor F is left adjoint to the functor G.

A pair of order-reversing maps $f\colon A \to B$, $g\colon B \to A$ can then be regarded as a pair of contravariant functors $F\colon \mathcal{A} \to \mathcal{B}$ and $G\colon \mathcal{B} \to \mathcal{A}$. Then f, g define an antitone Galois connection if the functors F, G are adjoint on the right.

This abstract viewpoint has some direct consequences for Galois connections:

- Left (resp. right) adjoints are unique up to isomorphism. The only isomorphisms in $\mathcal{A}, \mathcal{B}$ are the identies (by the anti-symmetry of $\leq$) so it follows that F is uniquely determined by G and vice versa. It follows that in a Galois connection f, g the map f is uniquely determined by g and vice versa.
- If f, g form a monotone adjoint Galois connection with f left adjoint to g then F is left adjoint to G and it follows that F preserves colimits and G preserves limits. It follows in particular that F preserves coproducts while G preserves products. Coproducts in $\mathcal{A}$ are just suprema in $(A, \leq)$, and products in $\mathcal{B}$ are just infima in $(B, \leq)$. It thus follows that f preserves suprema while g preserves infima.

If f, g form an antitone Galois connection between $(A, \leq)$ and $(B, \leq)$ then f, g form a monotone Galois connection between $(A, \leq)$ and $(B, \leq^{\mathrm{op}})$. It then follows from the above that both f and g turn suprema into infima.

For the maps $\mathcal{I}, \mathcal{V}$ this means that

$$\mathcal{I}\left(\bigcup_{i \in I} X_i\right) = \bigcap_{i \in I} \mathcal{I}(X_i)$$

for every family $(X_i)_{i \in I}$ of subsets $X_i \subseteq V$, which we have already seen in Lemma 16.20, and that

$$\mathcal{V}\left(\sum_{j \in J} I_j\right) = \bigcap_{i \in I} \mathcal{V}(I_j)$$

for every family $(I_j)_{j \in J}$ of ideal $I_j \trianglelefteq \mathcal{P}(V)$, which we will see in Lemma 20.2.

19.9. Suppose that we are given two subsets

$$A \subseteq \{\text{subsets } X \subseteq V\} \qquad \text{and} \qquad B \subseteq \{\text{ideals } I \trianglelefteq \mathcal{P}(V)\}$$

such that the maps $\mathcal{I}, \mathcal{V}$ restrict to bijections $A \to B$ and $B \to A$. Then A needs to be contained in the image of $\mathcal{V}$ while B needs to be contained in the image of $\mathcal{I}$. It then follows that the bijections $A \to B$ and $B \to A$ are just restrictions of the mutually bijections from Corollary 19.5.

The 1:1-correspondence given by Corollary 19.5 is therefore the most general 1:1-correspondence which can be constructed between subsets of V and ideal in $\mathcal{P}(V)$ by using the maps $\mathcal{V}, \mathcal{I}$. All other such correspondences must be restrictions of the one given by Corollary 19.5.

To better Corollary 19.5 we want to determine which kind of ideals can occur as vanishing ideals. We will show in the rest of this section that the vanishing ideals are precisely the radical ideals when k is algebraically closed.

Definition 19.10. Let R be a commutative ring.

a) An ideal $I \trianglelefteq R$ is a *radical ideal* if for all $x \in R$, $n \geq 0$ it follows from $x^n \in I$ that $x \in I$.

b) The *radical* of an ideal $I \trianglelefteq R$ is

$$\sqrt{I} := \{x \in R \mid x^n \in I \text{ for some } n \geq 0\}.$$

Lemma 19.11. Let R be a commutative ring and let $I \trianglelefteq R$ be an ideal. Then I is radical if and only if the ring R/I is reduced, i.e. has no non-zero commutative elements.

Proof. We have that

$$\begin{aligned} & R/I \text{ is reduced} \\ \iff & \forall x \in R/I : (x^n = 0 \text{ for some } n \geq 0 \implies x = 0) \\ \iff & \forall x \in R : (\overline{x}^n = 0 \text{ for some } n \geq 0 \implies \overline{x} = 0) \\ \iff & \forall x \in R : (x^n \in I \text{ for some } n \geq 0 \implies x \in I) \\ \iff & \text{the ideal } I \text{ is radical}. \end{aligned}$$

This proves the claim. □

Example 19.12. Let R be a commutative ring.

a) The unit ideal $(1) = R$ is always radical.

b) The zero ideal 0 is radical if and only if $R = R/0$ is reduced.

c) Every prime ideal $\mathfrak{p} \trianglelefteq\!\!\!\!\!\neq R$ is a radical ideal:

   If $x^n \in \mathfrak{p}$ for some $x \in R$, $n \geq 0$ then $n \geq 1$ because $x^0 = 1 \notin \mathfrak{p}$, and it then follows from $x^n \in \mathfrak{p}$ and $\mathfrak{p}$ being prime that $x \in \mathfrak{p}$.

   Alternatively we can observe that $R/\mathfrak{p}$ is an integral domain and is therefore reduced.

d) It can conversely be shown that every radical ideal is an intersection of prime ideals.

Lemma 19.13. Let R be a commutative ring and let $I \trianglelefteq R$ be an ideal.

a) The radical $\sqrt{I}$ is a radical ideal in R.

b) The radical $\sqrt{I}$ is the smallest radical ideal which contains I.

c) For an ideal $J \trianglelefteq R$ the following conditions are equivalent:
   1) The ideal J is radical.
   2) There exists some ideal $I \trianglelefteq R$ with $J = \sqrt{I}$.
   3) The ideal J satisfies $J = \sqrt{J}$.

Proof.

a) We have that $0 \in \sqrt{I}$ because $0^1 = 0 \in I$.

   For $f, g \in \sqrt{I}$ there exist $n, m \geq 0$ with $f^n, g^m \in I$ and thus $f^s, g^t \in I$ for all $s \geq n, t \geq m$. It follows that

$$(f+g)^{n+m} = \sum_{\ell=0}^{n+m} \binom{n+m}{\ell} f^\ell g^{n+m-\ell} \in I$$

   because for all $i = 0, \dots, n+m$ we have that $\ell \geq n$ or $n + m - \ell \geq m$. This shows that also $f + g \in \sqrt{I}$.

For $f \in \sqrt{I}$ there exists some $n \geq 0$ such that $f^n \in I$. For every $r \in R$ we then have that

$$(rf)^n = r^n f^n \in I$$

and thus $rf \in \sqrt{I}$.

For $x \in R$ with $x^n \in \sqrt{I}$ for some $n \geq 0$ there exists some $m \geq 0$ with $r^{mn} = (r^n)^m \in I$. It then follows that $x \in \sqrt{I}$. This shows that the ideal $\sqrt{I}$ is radical.

b) We have that $I \subseteq \sqrt{I}$ because $x = x^1 \in I$ for every $x \in I$, and every radical ideal $J \trianglelefteq R$ which contains I must also contain the elements of $\sqrt{I}$.

c) 1) $\implies$ 3): The smallest radical ideal containing J is just J itself, so $J = \sqrt{J}$.

3) $\implies$ 2): Choose $I = J$.

2) $\implies$ 1): This follows from part a). □

Lemma 19.14. For every subset $X \subseteq V$ the ideal $\mathcal{I}(X)$ is a radical ideal in $\mathcal{P}(V)$.

Proof. For $f \in \mathcal{P}(V)$ with $f^n \in \mathcal{I}(X)$ for some $n \geq 0$ we have that $f(x)^n = 0$ for every $x \in X$. Then $f(x) = 0$ for every $x \in X$ and thus $f \in \mathcal{I}(X)$. □

19.15. We will now show that the converse of Lemma 19.14 holds if k is algebraically closed. This will then answer our question which ideals $I \trianglelefteq \mathcal{P}(V)$ are vanishing ideals: It is precisely the radical ideals.

We proceed in three steps, each of which resulting in some kind of Nullstellensatz: We start off the weak Nullstellensatz, from which we then conclude the Nullstellensatz. By using the Rabinowitsch trick we then show the strong Nullstellensatz.

To show the weak Nullstellensatz we will need a results from commutative algebra, namely Zariski's lemma (Corollary A3.5).

Theorem 19.16 (Weak Nullstellensatz)**.** Let k be algebraically closed. Then every maximal ideal $\mathfrak{m} \subseteq k[X_1, \dots, X_n]$ is of the form

$$\mathfrak{m} = ((X_1 - a_1), \dots, (X_n - a_n)) = \mathfrak{m}_a$$

for some $a = (a_1, \dots, a_n) \in k^n$.

Proof. Let $R \coloneqq k[X_1, \dots, X_n]$. The quotient $L \coloneqq R/\mathfrak{m}$ is a field because the ideal $\mathfrak{m}$ is maximal and L is finitely generated as a k-algebra because R is a finitely generated k-algebra. It follows from Zariski's lemma that the field extension L/k is finite It follows that $L = k$ because k is algebraically closed.

Let $a_i \coloneqq \overline{X_i} \in L$ for every $i = 1, \dots, n$. Then the ideal $\mathfrak{m}_a = (X_1 - a_1, \dots, X_n - a_n)$ is a maximal (by Lemma 16.21) with $\mathfrak{m}_a \subseteq \mathfrak{m}$. It follows that $\mathfrak{m} = \mathfrak{m}_a$. □

Theorem 19.17. (Nullstellensatz) Let k be an algebraically closed field. For every proper ideal $I \ntrianglelefteq k[X_1, \dots, X_n]$ we have that $\mathcal{V}(I) \neq \emptyset$.

Proof. There exists a maximal ideal $\mathfrak{m} \precneqq k[X_1, \dots, X_n]$ with $I \subseteq \mathfrak{m}$ because I is a proper ideal. By the weak Nullstellensatz we have that $\mathfrak{m} = \mathfrak{m}_a$ for some $a \in k^n$. We then have that $\{a\} = \mathcal{V}(\mathfrak{m}_a) \subseteq \mathcal{V}(I)$. □

Remark 19.18.

a) The weak Nullstellensatz follows from the Nullstellensatz: If $\mathfrak{m} \precneqq k[X_1, \dots, X_n]$ is a maximal ideal then $\mathfrak{m}$ is in particular a proper ideal, so by the Nullstellensatz there exists some $a \in k^n$ with $a \in \mathcal{V}(\mathfrak{m})$. It follows that

$$\mathfrak{m} \subseteq \mathcal{I}(\mathcal{V}(\mathfrak{m})) \subseteq \mathcal{I}(a) = \mathfrak{m}_a$$

and thus $\mathfrak{m} = \mathfrak{m}_a$ because both $\mathfrak{m}, \mathfrak{m}_a$ are maximal.

The weak Nullstellensatz and Nullstellensatz are therefore equivalent.

b) For the case $n = 1$ both the weak Nullstellensatz and the Nullstellensatz become a well-known characterization of algebraically closed fields:

- The maximal ideals of $k[X]$ are precisely the ideals of the form (f) with $f \in k[X]$ irreducible because $k[X]$ is a principal ideal domain; the irreducible polynomial f is unique if we require it to be monic. The weak Nullstellensatz therefore states for $n = 1$ that the irreducible monic polynomials in $k[X]$ are precisely the polynomials $X - a$ with $a \in k$.
- The proper ideal in $k[X]$ are precisely the ideals of the form (f) with $f \in k[X]$ with $f = 0$ or f being non-constant. The Nullstellensatz therefore states for $n = 1$ that the only polynomials $f \in k[x]$ with no roots are the non-zero constant ones.

This also shows that both Nullstellensätze hold only if k is algebraically closed.

Consider for example the case $k = \mathbb{R}$ and $n = 1$. Then the ideal $(X^2 + 1) \trianglelefteq \mathbb{R}[X]$ is maximal but not of the form $X - a$ for some $a \in \mathbb{R}$, and $\mathcal{V}((X^2 + 1)) = \emptyset$.

c) The Nullstellensatz states that for all polynomials $f_1, \dots, f_s \in k[X_1, \dots, X_n]$ precisely one the following two things occurs:

- The polynomials $f_1, \dots, f_s$ have a common zero in k^n.
- There exists $g_1, \dots, g_n \in k[X_1, \dots, X_n]$ with $1 = g_1 f_1 + \dots + g_n f_n$.

Theorem 19.19 (Strong Nullstellensatz)**.** If k is algebraically closed then

$$\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$$

for every ideal $I \trianglelefteq k[X_1, \dots, X_n]$.

Proof. The ideal $\mathcal{I}(\mathcal{V}(I))$ is radical by Lemma 19.14 and contains I by Lemma 19.3 so it follows that $\sqrt{I} \subseteq \mathcal{I}(\mathcal{V}(I))$.

To show the other inclusion let $h \in \mathcal{I}(\mathcal{V}(I))$. We need to show that $h^m \in I$ for some $m \geq 0$. For $h = 0$ this is clear, so we assume that $h \neq 0$. Let $f_1, \dots, f_s \in I$ with $I = (f_1, \dots, f_s)$; such f_i exist because $k[X_1, \dots, X_n]$ is noetherian.

We use the *Rabinowitsch trick*: We adjoin a new variable Y to $k[X_1, \dots, X_n]$ and get $k[X_1, \dots, X_n, Y]$. Then $k[X_1, \dots, X_n]$ as a subring of $k[X_1, \dots, X_n, Y]$ so we can evaluate the polynomials $f \in k[X_1, \dots, X_n]$ at points $x \in k^{n+1}$. If $f_i(x) = 0$ for every $1 \leq i \leq s$ then $h(x) = 0$ which shows that the polynomials $f_1, \dots, f_s, 1 - hY$ have no common zeros.

It follows from the Nullstellensatz (see Remark 19.18) that there exist coefficients $p_1 \dots, p_s, q \in k[X_1, \dots, X_n, Y]$ with

$$1 = p_0(1 - Yh) + p_1 f_1 + \cdots + p_s f_s \,.$$

We can consider this as an identity in $k(X_1, \dots, X_n, Y)$ and replace Y by $1/h$, resulting in the equality

$$1 = p_1\left(X_1, \dots, X_n, \frac{1}{h}\right) f_1 + \cdots + p_s\left(X_1, \dots, X_n, \frac{1}{h}\right) f_s \,.$$

By multiplying both sides of this equation by a high enough power of h we get find that

$$h^m = q_1 f_1 + \cdots + q_s f_s \in I$$

for some $m \geq 0$ and polynomials $q_1, \dots, q_s \in k[X_1, \dots, X_n]$. □

Remark 19.20. The Rabinowitsch trick can be understood an an applicaiton of localization, as explained in [MO12]:

We want to show that some power of h is contained in I, which amounts to showing that the residue class $\overline{h}$ is nilpotent in $k[X_1, \dots, X_n]/I$. This happens only if $(k[X_1, \dots, X_n]/I)_{\overline{h}} = 0$. We have that

$$\begin{aligned} (k[X_1, \dots, X_n]/I)_{\overline{h}} &\cong (k[X_1, \dots, X_n]/I)[Y]/(\overline{h}Y - 1) \\ &\cong k[X_1, \dots, X_n, Y]/(I, hY - 1)\,, \end{aligned}$$

so we need to show that $(I, hY - 1)$ is not a proper ideal of $k[X_1, \dots, X_n, Y]$. By the Nullstellensatz this hols true if the polynomials of this ideal have no common roots, which holds because $h \in I$.

Remark 19.21. The strong Nullstellensatz implies the Nullstellensatz:

If $I \trianglelefteq\!\!\!\!\neq k[X_1, \dots, X_n]$ is a proper ideal with $\mathcal{V}(I) = \emptyset$ then $\sqrt{I} = \mathcal{I}(\mathcal{V}(I)) = \mathcal{I}(\emptyset) = (1)$ and thus $1 \in \sqrt{I}$. But then $1^m \in I$ for some $m \geq 0$ and thus $1 \in I$, which contradicts I being a proper ideal.

Together with part a) of Remark 19.18 this shows that all three forms of the Nullstellensatz are equivalent. There are also other equivalent theorems which are commonly known as “the Nullstellensatz”, but we will not encounter them here.

Corollary 19.22. If k is algebraically closed then an ideal $I \trianglelefteq k[X_1, \dots, X_n]$ is a vanishing ideal if and only if it is a radical ideal.

Proof. Every vanishing ideal is a radical ideal by Lemma 19.14, and every radical ideal is a vanishing ideal by the strong Nullstellensatz. □

Corollary 19.23. Let k be algebraically closed. Then the maps $\mathcal{I}, \mathcal{V}$ restrict to the following mutually inverse bijections:

$$\begin{tikzcd}
\left\{\begin{matrix}\text{algebraic subsets}\\ X \subseteq V\end{matrix}\right\} \arrow[r, shift left, "\mathcal{I}"] & \left\{\begin{matrix}\text{radical ideals}\\ I \trianglelefteq \mathcal{P}(V)\end{matrix}\right\} \arrow[l, shift left, "\mathcal{V}"] \\
\rotatebox{90}{$\subseteq$} & \rotatebox{90}{$\subseteq$} \\
\left\{\text{ points } a \in V \text{ }\right\} \arrow[r, shift left, "\mathcal{I}"] & \left\{\begin{matrix}\text{maximal ideals}\\ \mathfrak{m} \trianglelefteq \mathcal{P}(V)\end{matrix}\right\} \arrow[l, shift left, "\mathcal{V}"]
\end{tikzcd}$$

Proof. In the diagram of Corollary 19.7 we can replace “vanishing ideals” by “radical ideals” by Corollary 19.22, and we can replace “vanishing ideals [...] which are maximal” first by “radical ideals [...] which are maximal” and then by “maximal ideal” because every maximal ideal is already a radical ideal (because it is prime). □

Remark 19.24. It follows from part d) of Lemma 19.3 that the composition

$$\mathcal{I} \circ \mathcal{V} \colon \{\text{ideals } I \trianglelefteq \mathcal{P}(V)\} \to \{\text{ideals } I \trianglelefteq \mathcal{P}(V)\}$$

is idempotent and monotone with $I \subseteq (\mathcal{I} \circ \mathcal{V})(I)$ for all $I \trianglelefteq \mathcal{P}(V)$. The composition $\mathcal{I} \circ \mathcal{V}$ is therefore a closure operator. If k is algebraically closed then we have shown in this section that $\mathcal{I} \circ \mathcal{V}$ is the radical-operator $\sqrt{}$.

20. The Zariski Topology

20.1. In this section we show that the Zariski closed subsets define a topology on V and use this to extend the 1:1-correspondences from Corollary 19.7 and Corollary 19.23 to include prime ideals as well.

Lemma 20.2.

a) Let $(I_j)_{j \in J}$ be a family of ideals $I_j \trianglelefteq \mathcal{P}(V)$. Then $\bigcap_{j \in J} \mathcal{V}(I_j) = \mathcal{V}(\sum_{j \in J} I_j)$.

b) Let $I_1, I_2 \trianglelefteq \mathcal{P}(V)$ be ideals. Then $\mathcal{V}(I_1) \cup \mathcal{V}(I_2) = \mathcal{V}(I_1 \cap I_2) = \mathcal{V}(I_1 I_2)$.

Proof.

a) We have that $I_i \subseteq \sum_{j \in J} I_j$ for every $i \in J$, therefore $\mathcal{V}(\sum_{j \in J} I_j) \subseteq \mathcal{V}(I_i)$ for every $i \in I$, and thus $\mathcal{V}(\sum_{j \in J} I_j) \subseteq \bigcap_{j \in J} \mathcal{V}(I_j)$.

   For $x \in \bigcap_{j \in J} \mathcal{V}(I_j)$ we have that $x \in \mathcal{V}(I_j)$ for every $j \in J$, and thus $f(x) = 0$ for every $j \in J$, $f \in I_j$. It follows that $x \in \mathcal{V}(\bigcup_{j \in J} I_j) = \mathcal{V}((\bigcup_{j \in J} I_j)) = \mathcal{V}(\sum_{j \in J} I_j)$. This shows the inclusion $\bigcap_{j \in J} \mathcal{V}(I_j) \subseteq \mathcal{V}(\sum_{j \in J} I_j)$.

b) It follows from $I_1 \cap I_2 \subseteq I_1, I_2$ that $\mathcal{V}(I_1), \mathcal{V}(I_2) \subseteq \mathcal{V}(I_1 \cap I_2)$ and therefore that $\mathcal{V}(I_1) \cup \mathcal{V}(I_2) \subseteq \mathcal{V}(I_1 \cap I_2)$.

   It follows from $I_1 I_2 \subseteq I_1 \cap I_2$ that $\mathcal{V}(I_1 \cap I_2) \subseteq \mathcal{V}(I_1 I_2)$.

For $x \notin \mathcal{V}(I_1) \cup \mathcal{V}(I_2)$ we have that $x \notin \mathcal{V}(I_1), \mathcal{V}(I_2)$, so there exist $f_1 \in I_1$, $f_2 \in I_2$ with $f_1(x), f_2(x) \neq 0$. Then $f_1 f_2 \in I_1 I_2$ with $(f_1 f_2)(x) \neq 0$, so that $x \notin \mathcal{V}(I_1 I_2)$. This shows that $\mathcal{V}(I_1 I_2) \subseteq \mathcal{V}(I_1) \cup \mathcal{V}(I_2)$. □

Corollary 20.3. There exists a topology on V whose closed subsets are precisely the Zariski closed subsets.

Proof. The subsets $\emptyset, V \subseteq V$ are Zariski closed by Example 18.4 and are closed under arbitrary intersections and finite unions by Lemma 20.2. □

Definition 20.4. The *Zariski topology* (*on* V) is the topology on V whose closed subsets are the Zariski closed subsets of V.

Proposition 20.5. Let $X \subseteq Y \subseteq V$ be subsets.

a) We have that $\overline{X} = \mathcal{V}(\mathcal{I}(X))$.

b) The subset X is dense in Y with respect to the Zariski topology if and only if X is Zariski dense in Y (in the sense of Definition 16.3).

c) The closure $\overline{X}$ is the biggest subset of V in which X is Zariski dense.

Proof.

a) We have that

$$\begin{aligned}\overline{X} &= \bigcap \{C \mid C \subseteq V \text{ is Zariski closed, } X \subseteq C\} = \bigcap \{\mathcal{V}(I) \mid I \trianglelefteq \mathcal{P}(V), X \subseteq \mathcal{V}(I)\} \\ &= \bigcap \{\mathcal{V}(I) \mid I \trianglelefteq \mathcal{P}(V), \mathcal{I}(X) \supseteq I\} = \bigcap_{\substack{I \trianglelefteq \mathcal{P}(V) \\ I \subseteq \mathcal{I}(X)}} \mathcal{V}(I) = \mathcal{V}\left(\sum_{\substack{I \trianglelefteq \mathcal{P}(V) \\ I \subseteq \mathcal{I}(X)}} I \right) = \mathcal{V}(\mathcal{I}(X)) \,.\end{aligned}$$

b) We have that

$$\begin{aligned} X \text{ is dense in } Y &\iff Y \subseteq \overline{X} \iff Y \subseteq \mathcal{V}(\mathcal{I}(X)) \\ &\iff \mathcal{I}(Y) \supseteq \mathcal{I}(X) \iff Y \text{ is Zariski dense in } X \,. \end{aligned}$$

c) The closure $\overline{X}$ is the biggest subset of V in which X is dense so the claim follows from part b). □

Remark 20.6. Propositon 20.5 shows that Zariski density in the sense of Definition 16.3 can be understood as a topological kind of density. The Zariski topology is the unique topology on V with this property:

Suppose we are given any topology on V such that Zariski density coincides with topological density. Then for every subset $X \subseteq V$ the closure $\overline{X}$ is the maximal subset of V in which X is Zariski dense, which shows that $\overline{X}$ is uniquely determined. A subset $X \subseteq V$ is closed if and only if $X = \overline{X}$ so it further follows that the closed subsets are uniquely determined. But this already determines the topology itself.

Remark 20.7. It follows from Lemma 19.3 that the composition

$$c \coloneqq \mathcal{V} \circ \mathcal{I} \colon \{\text{subsets } X \subseteq V\} \to \{\text{subsets } X \subseteq V\}$$

is idempotent and monotone with $X \subseteq c(X)$ for every subset $X \subseteq V$. The map c is therefore a closure operator. We also have that

$$c(\emptyset) = \mathcal{V}(\mathcal{I}(\emptyset)) = \mathcal{V}((1)) = \emptyset,$$

and for all subsets $X, Y \subseteq V$ we have that

$$c(X \cup Y) = \mathcal{V}(\mathcal{I}(X \cup Y)) = \mathcal{V}(\mathcal{I}(X) \cap \mathcal{I}(Y)) = \mathcal{V}(\mathcal{I}(X)) \cup \mathcal{V}(\mathcal{I}(Y)) = c(X) \cup c(Y)\,.$$

This shows that c is a Kuratowski closure operator, and thus defines a topology on V whose sets are precisely those subsets $X \subseteq V$ for which $c(X) = X$. By Proposition 20.5 this topology is precisely the Zariski topology.

Remark 20.8. Building on the ideals of Remark 19.18 one can think about the Nullstellensatz as the existence of a partition of unity, as explained in [Spe07]:

Recall that for an open covering $(U_j)_{j \in J}$ of a topological space X a partition of unity subordinate to this covering is a familiy $(\varphi_i)_{i \in I}$ of continuous maps $f_i \colon X \to \mathbb{R}$ such that for every $i \in I$ there exists some $j \in J$ with $\operatorname{supp}(\varphi_i) \subseteq U_j$, the family $(\operatorname{supp}(\varphi)_i)_{i \in I}$ is a locally finite covering of X, and $1 = \sum_{i \in I} \varphi_i$. (Here supp denotes the support $\operatorname{supp}(\varphi) = \overline{\{x \in X \mid \varphi(x) \neq 0\}}$.)

For every ideal $I \subseteq \mathcal{P}(V)$ we now set $U(I) \coloneqq V \smallsetminus \mathcal{V}(I)$. Then the sets $U(I)$ with $I \trianglelefteq \mathcal{P}(V)$ are precisely the Zariski open subsets of V, and

- we have that $U(S) = U((S))$ for every subset $S \subseteq \mathcal{P}(V)$,
- for all $S \subseteq T \subseteq \mathcal{P}(V)$ it follows from $S \subseteq T$ that $U(S) \subseteq U(T)$,
- for every family $(I_j)_{j \in J}$ of ideals $I_j \trianglelefteq \mathcal{P}(V)$ we have that $\bigcup_{j \in J} U(I_j) = U(\sum_{j \in J} I_j)$.

Suppose now that k is algebraically closed and that $(U_j)_{j \in J}$ is an open covering of V. Every set $U_j \subseteq V$ is Zariski open, and thus of the form $U_j = U(I_j)$ for some ideal $I_j \trianglelefteq \mathcal{P}(V)$. Then U_j consists of all those $a \in V$ which are not a common zero of all $f \in I_j$. The condition $V = \bigcup_{j \in J} U_j$ is therefore equivalent to the polynomial functions $f \in I \coloneqq \sum_{j \in J} I_j$ having no common roots. This can also seen by using that

$$V = \bigcup_{j \in J} U_j = \bigcup_{j \in J} U(I_j) = U\left(\sum_{j \in J} I_j \right) = U(I)\,,$$

from which it follows that $\mathcal{V}(I) = V \smallsetminus U(I) = \emptyset$.

It then follows from the Nullstellensatz (as explained in part c) of Remark 19.18) that $1 = g_1 f_1 + \dots + g_n f_n$ for some $j_1, \dots, j_n \in J$, $f_i \in I_{j_i}$ and $g_i \in \mathcal{P}(V)$. Then the polynomials functions $\varphi_i \coloneqq g_i f_i \colon V \to k$ satisfy $1 = \varphi_1 + \dots + \varphi_n$, and for every $i = 1, \dots, n$ we have that

$$U(\varphi_i) = U(g_i f_i) \subseteq U(f_i) \subseteq U(I_{j_i}) = U_{j_i}\,.$$

We can therefore regard the functions $\varphi_1, \dots, \varphi_n$ as a partition of unity subordinate to the open covering $(U_j)_{j \in J}$.

Definition 20.9. A topological space X is *irreducible* (or *hyperconnected*) if it is non-empty and cannot be written as $X = C_1 \cup C_2$ for proper closed subsets $C_1, C_2 \subsetneq X$. Otherwise X is *reducible*.

Remark 20.10. Let X be a topological space.

a) By taking complements one find that the following conditions are equivalent:

   1) The space X is irreducible.

   2) The space X is non-empty and every two non-empty open subsets of X intersect non-trivially.

   3) The space X is non-empty and every non-empty open subset of X is dense.

b) A non-empty subspace $C \subseteq X$ is irreducible (when endowed with the subspace topology) if and only if for all closed subsets $C_1, C_2 \subseteq X$ with $C \subseteq C_1 \cup C_2$ it follows that $C \subseteq C_1$ or $C \subseteq C_2$.

   We will use this observations throughout the rest of this section whenever we need to show that a subspace is irreducible.

Lemma 20.11. Let R be a commutative ring, $\mathfrak{p} \ntrianglelefteq R$ a prime ideal and let $I_1, I_2 \trianglelefteq R$ be ideals with $I_1 I_2 \subseteq \mathfrak{p}$. Then $I_1 \subseteq \mathfrak{p}$ or $I_2 \subseteq \mathfrak{p}$.

Proof. If $I_1, I_2 \subsetneq \mathfrak{p}$ then there exist $x_j \in I_j$ with $x_j \notin \mathfrak{p}$ for $j = 1, 2$. Then $x_1 x_2 \notin \mathfrak{p}$ because $\mathfrak{p}$ is prime, but $x_1 x_2 \in I_1 I_2$, which contradicts $I_1 I_2 \subseteq \mathfrak{p}$. □

Lemma 20.12. Let $X \subseteq V$ be a Zariski closed subset with corresponding vanishing ideal $\mathfrak{p} \trianglelefteq \mathcal{P}(V)$, i.e. $X = \mathcal{V}(\mathfrak{p})$ and $\mathfrak{p} = \mathcal{I}(X)$. Then X is irreducible if and only if $\mathfrak{p}$ is prime.

Proof. That X is non-empty is equivalent to $\mathcal{I}(X) = \mathfrak{p}$ being a proper ideal.

Suppose that X is irreducible and let $f_1, f_2 \in \mathcal{P}(V)$ with $f_1 f_2 \in I = \mathcal{I}(X)$. It follows from Lemma 19.2 that

$$X \subseteq \mathcal{V}(f_1 f_2) = \mathcal{V}(f_1) \cup \mathcal{V}(f_2) .$$

It follows that $X \subseteq \mathcal{V}(f_j)$ for some $j = 1, 2$ because X is irreducible, and it then follows from Lemma 19.2 that $f_j \in \mathcal{I}(X) = \mathfrak{p}$. This shows that the ideal $\mathfrak{p}$ is prime.

Suppose on the other hand that $\mathfrak{p}$ is prime and that $X = C_1 \cup C_2$ for some closed subsets $C_1, C_2 \subseteq V$. Then C_1, C_2 are also closed in V because X is a closed subset of V, so there exist ideals $I_1, I_2 \trianglelefteq \mathcal{P}(V)$ with $C_j = \mathcal{V}(I_j)$ for $j = 1, 2$. It then follows from

$$X = C_1 \cup C_2 = \mathcal{V}(I_1) \cup \mathcal{V}(I_2) = \mathcal{V}(I_1 I_2)$$

and Lemma 19.2 that $\mathfrak{p} = \mathcal{I}(X) \supseteq I_1 I_2$. It follows from Lemma 20.11 that $I_j \subseteq \mathfrak{p}$ for some $j = 1, 2$ and therefore that $C_j = \mathcal{V}(I_j) \supseteq \mathcal{V}(\mathfrak{p}) = X$. This shows that X is irreducible. □

Theorem 20.13.

a) The maps $\mathcal{I}, \mathcal{V}$ restrict to the following mutually inverse bijections:

$$\begin{tikzcd}
\begin{Bmatrix} \text{algebraic subsets} \\ X \subseteq V \end{Bmatrix} \arrow[r, shift left, "\mathcal{I}"] & \begin{Bmatrix} \text{vanishing ideals} \\ I \trianglelefteq \mathcal{P}(V) \end{Bmatrix} \arrow[l, shift left, "\mathcal{V}"] \\
\begin{Bmatrix} \text{irreducible} \\ \text{algebraic subsets} \\ X \subseteq V \end{Bmatrix} \arrow[u, phantom, sloped, "\subseteq"] \arrow[r, shift left, "\mathcal{I}"] & \begin{Bmatrix} \text{vanishing ideals} \\ \mathfrak{p} \trianglelefteq \mathcal{P}(V) \\ \text{which are prime} \end{Bmatrix} \arrow[u, phantom, sloped, "\subseteq"] \arrow[l, shift left, "\mathcal{V}"] \\
\left\{ \text{ points } a \in V \ \right\} \arrow[u, phantom, sloped, "\subseteq"] \arrow[r, shift left, "\mathcal{I}"] & \begin{Bmatrix} \text{vanishing ideals} \\ \mathfrak{m} \trianglelefteq \mathcal{P}(V) \\ \text{which are maximal} \end{Bmatrix} \arrow[u, phantom, sloped, "\subseteq"] \arrow[l, shift left, "\mathcal{V}"]
\end{tikzcd}$$

b) If k is algebraically closed then the maps $\mathcal{I}, \mathcal{V}$ restrict to the following mutually inverse bijections:

$$\begin{tikzcd}
\begin{Bmatrix} \text{algebraic subsets} \\ X \subseteq V \end{Bmatrix} \arrow[r, shift left, "\mathcal{I}"] & \begin{Bmatrix} \text{radical ideals} \\ I \trianglelefteq \mathcal{P}(V) \end{Bmatrix} \arrow[l, shift left, "\mathcal{V}"] \\
\begin{Bmatrix} \text{irreducible} \\ \text{algebraic subsets} \\ X \subseteq V \end{Bmatrix} \arrow[u, phantom, sloped, "\subseteq"] \arrow[r, shift left, "\mathcal{I}"] & \begin{Bmatrix} \text{prime ideals} \\ \mathfrak{p} \trianglelefteq \mathcal{P}(V) \end{Bmatrix} \arrow[u, phantom, sloped, "\subseteq"] \arrow[l, shift left, "\mathcal{V}"] \\
\left\{ \text{ points } a \in V \ \right\} \arrow[u, phantom, sloped, "\subseteq"] \arrow[r, shift left, "\mathcal{I}"] & \begin{Bmatrix} \text{maximal ideals} \\ \mathfrak{m} \trianglelefteq \mathcal{P}(V) \end{Bmatrix} \arrow[u, phantom, sloped, "\subseteq"] \arrow[l, shift left, "\mathcal{V}"]
\end{tikzcd}$$

Proof. These are upgraded of Corollary 19.7 and Corollary 19.23 via Lemma 20.12. For part b) we also use that every prime ideal is already radical. □

20.14. We will now show that every topological space is the union of its irreducible components:

Definition 20.15. Let X be a topological space. A subset $C \subseteq X$ is an *irreducible component* of X if C is a maximal irreducible subset of X, i.e. C is irreducible, and for every irreducible subset $C' \subseteq X$ with $C \subseteq C'$ it follows that $C = C'$.

Lemma 20.16. Let X be a topological space and let $Y \subseteq X$ be irreducible. Then the closure $\overline{Y}$ is also irreducible.

Proof. Let $C_1, C_2 \subseteq Y$ be closed subsets with $\overline{Y} \subseteq C_1 \cup C_2$. Then $Y \subseteq C_1 \cup C_2$ and it follows that $Y \subseteq C_j$ for some $j = 1, 2$ because Y is irreducible. It then follows that $\overline{Y} \subseteq C_j$ because C_j is closed. □

Corollary 20.17. The irreducible components of a topological space X are closed.

Proof. If $C \subseteq X$ is an irreducible component then $\overline{C} \subseteq X$ is an irreducible subspace with $C \subseteq \overline{C}$ It follows that $\overline{C} \subseteq C$ because C is maximal among all irreducible subspaces. We thus have that $C = \overline{C}$, which shows that C is closed. □

Proposition 20.18. Let X be a topological space.

a) Let $(C_i)_{i \in I}$ be non-empty family of irreducible subsets $C_i \subseteq X$ which is linearly ordered with respect to inclusion, i.e. for all $i, j \in I$ we have that $C_i \subseteq C_j$ or $C_j \subseteq C_i$. Then $C \coloneqq \bigcup_{i \in I} C_i$ is again irreducible.

b) Every irreducible subset $C \subseteq X$ is contained in an irreducible component of X.

c) Every $x \in X$ is contained in an irreducible component, i.e. X is the union of its irreducible components.

d) If $C, C' \subseteq X$ are two distinct irreducible components of X then $C \nsubseteq C'$.

Proof.

a) Let $C'_1, C'_2 \subseteq X$ be two distinct closed subsets with $C \subseteq C'_1 \cup C'_2$ and $C \nsubseteq C'_2$. It follows from $C \nsubseteq C'_2$ that there exists some $j \in I$ with $C_j \nsubseteq C'_2$. It also follows from $C \subseteq C'_1 \cup C'_2$ that $C_i \subseteq C'_1 \cup C'_2$ for every $i \in I$, and therefore for every $i \in I$ that $C_i \subseteq C'_1$ or $C_i \subseteq C'_2$ by the irreducibility of C_i.

   For $i = j$ we have that $C_j \subseteq C'_1$ because $C_j \nsubseteq C'_2$. For every other $i \in I$ we distinguish between two cases:

   - If $C_i \subseteq C_j$ then it follows that $C_i \subseteq C'_1$.
   - If $C_i \supseteq C_j$ then it follows that $C_i \subseteq C'_1$ because otherwise $C_j \subseteq C_i \subseteq C'_2$, which would contradicts the choice of j.

   Altogether this shows that $C_i \subseteq C'_1$ for every $i \in I$, so that $C = \bigcup_{i \in I} C_i \subseteq C'_1$.

b) We consider the set

$$\mathcal{C} = \{C' \subseteq X \mid C' \text{ is irreducible with } C' \supseteq C\}.$$

   This set is non-empty because it contains C. It follows from part a) of this proposition that the partially ordered set $(\mathcal{C}, \subseteq)$ is inductive, i.e. we can apply Zorn's Lemma. It follows that there exists a maximal element $C' \in \mathcal{C}$. Then C' is in particular a maximal irreducible subspace of X, and thus an irreducible component of X. We have that $C \subseteq C'$ because $C' \in \mathcal{C}$.

c) This follows from part c) of this proposition because $\{x\}$ is an irreducible subspace of X.

d) If $C \subseteq C'$ then it follows that already $C' = C$ because C is a maxmial irreducible subset of X. □

Example 20.19. Consider the real line $\mathbb{R}$ with the standard (i.e. euclidian) topology. If $C \subseteq \mathbb{R}$ contains at least two distinct points $x, y \in C$ then for $z = (x+y)/2$ we have that $C \subseteq (-\infty, z] \cup [z, \infty)$ but $C \nsubseteq (-\infty, z], [z, \infty)$. This shows that the only irreducible subspaces of $\mathbb{R}$ are the singletons $\{x\}$, $x \in \mathbb{R}$. These are in particular the irreducible components of $\mathbb{R}$.

20.20. It follows from Proposition 20.18 that every Zariski closed subset $V \subseteq X$ is the union of its irreducible components, each of which is closed, and which are not contained in each other. We will now show that a Zariski closed set has only finitely many irreducible components.

Definition 20.21. A topological space X is *noetherian* if every ascending sequence

$$U_1 \subseteq U_2 \subseteq U_3 \subseteq \cdots$$

of open subsets $U_i \subseteq X$ stabilizes; equivalently, every descending chain

$$C_1 \supseteq C_2 \supseteq C_3 \supseteq \cdots$$

of closed subsets $C_i \subseteq X$ stabilizes.

Lemma 20.22. A topological space X is noetherian if and only if every non-empty collection $\mathcal{U}$ of open subsets has a maximal element; equivalently, every non-empty family of closed subsets has a minimal element.

Proof. Suppose that there exists a non-empty collection $\mathcal{U}$ of open subsets of X which does not have a maximal element. Starting with any $U_1 \in \mathcal{U}$ there then exists for every $n \geq 1$ some $U_{n+1} \in \mathcal{U}$ with $U_n \subsetneq U_{n+1}$. It then follows that

$$U_1 \subsetneq U_2 \subsetneq U_3 \subsetneq \cdots$$

is an increasing sequence of open subsets of X which does not stabilize. This contradicts X being noetherian.

Suppose on the other hand that

$$U_1 \subseteq U_2 \subseteq U_3 \subseteq \cdots$$

is an increasing sequence of open subsets $U_n \subseteq X$. Then $\mathcal{U} = \{U_n \mid n \geq 1\}$ has a maximal element, i.e. there exists some $m \geq 1$ with $U_m \supseteq U_n$ for every $n \geq 1$. It then follows for all $n \geq m$ that $U_n = U_m$, which shows that the above sequence stabilizes. This shows that X is noetherian. □

Proposition 20.23. Let X be a noetherian topological space. Then there exist closed irreducible subsets $C_1, \dots, C_n \subseteq X$ with $X = C_1 \cup \cdots \cup C_n$ and $C_i \nsubseteq C_j$ for all $i \neq j$.

Proof. Suppose that X is not the union of finitely many closed irreducible subsets. Then the set

$$\mathcal{C} = \left\{ C \subseteq X \,\middle|\, \begin{array}{c} C \text{ is closed and not the union of} \\ \text{finitely many closed irreducible subsets} \end{array} \right\}$$

contains X and is therefore non-empty. It follows from Lemma 20.22 that $\mathcal{C}$ contains a minimal element $C \in \mathcal{C}$ because X is noetherian. Note that $\emptyset \notin \mathcal{C}$ because $\emptyset$ is the union of zero closed irreducible subsets. The set C is therefore non-empty.

The set C cannot be irreducible because otherwise $C \notin \mathcal{C}$. Because C is non-empty it follows that there exist proper closed subsets $C_1, C_2 \subsetneq C$ with $C = C_1 \cup C_2$. The sets C_1, C_2 cannot be the union of finitely many closed irreducible subspaces because otherwise the same would hold for $C = C_1 \cup C_2$, which would contradict $C \in \mathcal{C}$. Both C_1, C_2 are closed in X because they are closed in C which is closed in X. This shows that $C_1, C_2 \in \mathcal{C}$. But this contradicts the minimality of C.

It follows that $X = C_1 \cup \cdots \cup C_m$ for some closed irreducible subsets $C_i \subseteq X$. If $C_i \subseteq C_j$ for some $i \neq j$ then we may eliminate C_i from the collection $C_1, \ldots, C_m$ without losing the property that $X = C_1 \cup \cdots \cup C_m$. After finitely many eliminations we arrive at closed irreducible subsets $C_1, \ldots, C_n \subseteq X$ with $X = C_1 \cup \cdots \cup C_n$ and $C_i \nsubseteq C_j$ for all $i \neq j$. □

Lemma 20.24. Let X be a topological space. If $X = C_1 \cup \cdots \cup C_n$ for closed irreducible subsets $C_1, \ldots, C_n \subseteq X$ with $C_i \nsubseteq C_j$ for all $i \neq j$ then $C_1, \ldots, C_n$ are the irreducible components of X.

Proof. Let C' be an irreducible subset of X. Then $C' \subseteq X = C_1 \cup \cdots \cup C_n$ and it follows from the irreducibilty of C' that $C' \subseteq C_i$ for some i. This shows that every irreducible subset of X is contained in some C_i.

If C' is an irreducible component of X then it follows that $C' \subseteq C_i$ for some $i = 1, \ldots, n$. It then follows that $C' = C_i$ because C' is a maximal irreducible subset of X and C_i is irreducible. This shows that every irreducible component occurs as some C_i.

Fix some $i = 1, \ldots, n$. If $C' \subseteq X$ is an irreducible subset with $C_i \subseteq C'$ then C' is contained in some C_j because C' is irreducible. It follows that $C_i \subseteq C_j$ and therefore that $i = j$. Then $C_i \subseteq C' \subseteq C_i$ and thus $C_i = C$. This shows that the C_i are maximal irreducible subsets of X, i.e. irreducible components of X. □

Corollary 20.25. A noetherian topological space X has only finitely many irreducible components.

Corollary 20.26. There exist closed irreducible subsets $C_1, \ldots, C_n \subseteq X$ such that $X = C_1 \cup \cdots \cup C_n$ and $C_i \nsubseteq C_j$ for all $i \neq j$ by Proposition 20.23, and the C_i are the irreducible components of X by Lemma 20.24.

Lemma 20.27.

a) The space V (together with the Zariski topology) is noetherian.

b) If X is a noetherian topological space then every subspace $Y \subseteq X$ is noetherian.

Proof.

a) Let
$$C_1 \supseteq C_2 \supseteq C_3 \supseteq \cdots \tag{20.1}$$
be a decreasing sequence of closed subsets $C_n \subseteq X$. Then
$$\mathcal{I}(C_1) \subseteq \mathcal{I}(C_2) \subseteq \mathcal{I}(C_3) \subseteq \cdots$$
is an increasing sequence of ideals in $\mathcal{P}(V) \cong k[X_1, \dots, X_{(\dim V)}]$, which is noetherian. It follows that this chain stabilizes, so there exists some $m \geq 1$ with $\mathcal{I}(C_n) = \mathcal{I}(C_m)$ for every $n \geq m$. For every $n \geq m$ it then follows that
$$C_m = \mathcal{V}(\mathcal{I}(C_m)) = \mathcal{V}(\mathcal{I}(C_n)) = C_n \,.$$
This shows that the sequence (20.1) stabilizes.

b) Let $\mathcal{U} = \{U_i \,|\, i \in I\}$ be a collection of open subsets of Y. Then for every $i \in I$ there exists an open subset $V_i \subseteq X$ with $U_i = V_i \cap X$, and $\mathcal{V} = \{V_i \,|\, i \in I\}$ is a collection of open subsets of X. Then $\mathcal{V}$ contains a maximal element because X is noetherian, i.e. there exists some $j \in I$ with $V_j \supseteq V_i$ for every $i \in I$. It follows that $U_j \supseteq U_i$ for every $i \in I$. This shows that Y is noetherian. □

Corollary 20.28. Every $X \subseteq V$ has only finitely many irreducible components.

Proof. It follows from Lemma 20.27 that X is noetherian, so the statement follows from Corollary 20.25. □

21. Affine Algebraic Varieties as Geometric Spaces

21.1. In this section we will see that affine algebraic varities can be regarded as geometric spaces in their own right.

Conventions 21.2. In the following, U, V, W are finite-dimensional k-vector spaces.

Definition 21.3. Let $X \subseteq V$, $Y \subseteq W$ be affine algebraic varietes. A map $f \colon X \to Y$ is *polynomial* if it is the restriction of a polynomial map $V \to W$. We denote by $\operatorname{Pol}(X, Y)$ the set of polynomial maps $X \to Y$.

Remark 21.4. Let $X \subseteq V$, $Y \subseteq W$, $Z \subseteq U$ be affine algebraic varieties..

a) A function $f \colon X \to k$ is polynomial if it is the restriction of a polynomial function $V \to k$.

b) The identity $\mathrm{id}_X \colon X \to X$ is polynomial, and for all polynomials maps $f \colon X \to Y$, $g \colon Y \to Z$ their composition $g \circ f \colon X \to Z$ is again polynomial.

It follows that the class of affine algebraic varieties over k together with the polynomial maps between them form a category, which we will denote by k-**Aff**: The objects of k-**Aff** are affinee algebraic varieties over k and the Hom-sets of k-**Aff** are given by $\mathrm{Hom}_{k\text{-}\mathbf{Aff}}(X, Y) = \mathrm{Pol}(X, Y)$ for all affine algebraic varieties X, Y over k.

Note that the category k-**pol** (see Remark 7.26) is a full subcategory of k-**Aff**.

c) Given a basis $w_1, \dots, w_m$ of W, a map $f\colon X \to Y$ is polynomial if and only if it is polynomial in each coordinate, i.e. if and only if the functions $f_1, \dots, f_m\colon V \to k$ with $f(x) = f_1(x)w_1 + \cdots + f_m(x)w_m$ are polynomial.

d) The polynomial functions $f\colon X \to k$ form a k-algebra with pointwise addition and multiplication.

Definition 21.5. For an affine algebraic variety $X \subseteq V$ the *coordinate ring of* X, denoted by $\mathcal{P}(X)$, is the k-algebra of polynomial functions $X \to k$, with addition and multiplication being done pointwise.

Remark 21.6. Other popular notations for the coordinate ring $\mathcal{P}(X)$ of an affine algebraic variety X are $A(X)$, $\mathcal{O}(X)$ and $k[X]$.

Lemma 21.7. For every affine algebraic variety $X \subseteq V$ the map

$$\mathcal{P}(V)/\mathcal{I}(X) \to \mathcal{P}(X)\,, \quad [f] \mapsto f|_X$$

is an isomorphism of k-algebras.

Proof. The map $\mathcal{P}(V) \to \mathcal{P}(X)$, $f \mapsto f|_X$ is a surjective homomorphism of k-algebras by construction of $\mathcal{P}(X)$, and that $\mathcal{I}(X)$ is its kernel is a reformulation of the definition of $\mathcal{I}(X)$. □

Corollary 21.8. Let $X \subseteq V$ be an affine algebraic variety.

a) The coordinate ring $\mathcal{P}(X)$ is an integral domain if and only if X is irreducible.

b) The coordinate ring $\mathcal{P}(X)$ is a field if and only if $X = \{a\}$ is a singleton for some $a \in V$, in which case $\mathcal{P}(X) = k$.

Proof.

a) The quotient $\mathcal{P}(X) \cong \mathcal{P}(V)/\mathcal{I}(X)$ is an integral domain if and only if the ideal $\mathcal{I}(X) \trianglelefteq \mathcal{P}(V)$ is prime, which, Lemma 20.12, is the case if and only if X is irreducible by .

b) The quotient $\mathcal{P}(X) \cong \mathcal{P}(V)/\mathcal{I}(X)$ is a field if and only if the ideal $\mathcal{I}(X)$ is a maximal ideal, which, by Lemma 19.6, holds if and only if $X = \{a\}$ is a singleton for some $a \in V$. Then $\mathcal{P}(X) = \mathcal{P}(\{x\})$ consists of all maps $\{x\} \to k$, so that $\mathcal{P}(\{x\}) = k$. □

Lemma 21.9. Let X, Y, Z be affine algebraic varieties.

a) For every polynomial map $f\colon X \to Y$ the map $f^*\colon \mathcal{P}(Y) \to \mathcal{P}(X)$, $\varphi \mapsto \varphi \circ f$ is a well-defined homomorphism of k-algebras.

b) We have that $\mathrm{id}_X^* = \mathrm{id}_{\mathcal{P}(X)}$.

c) For all polynomial maps $f\colon X \to Y$, $g\colon Y \to Z$ we have that $(g \circ f)^* = f^* \circ g^*$.

Remark 21.10. Lemma 21.9 shows that the coordinate ring $\mathcal{P}$ defines a contravariant functor $\mathcal{P}\colon k\text{-}\mathbf{Aff} \to k\text{-}\mathbf{Alg}$. Note that this is an extension of the previously defined functor $\mathcal{P}$ from Remark 7.31. This functor turns out to be fully faithful, generalizing Propositon 7.32 to affine algebraic varieties:

Proposition 21.11. Let $X \subseteq V$, $Y \subseteq W$ be affine algebraic varieties. Then the map

$$\mathrm{Pol}(X,Y) \to \mathrm{Hom}_{k\text{-}\mathbf{Alg}}(\mathcal{P}(Y), \mathcal{P}(X)), \quad f \mapsto f^*$$

is a bijection.

Proof. For $Y = W$ the proof given for Propositon 7.32 still applies without any changes, simply replace V by X. The general case follows from this special one: The inclusion $i\colon Y \to W$ is a polynomial map which results in the following diagram:

$$\begin{tikzcd}
\mathrm{Pol}(X,Y) \arrow[r, "i_*"] \arrow[d, "\mathcal{P}_{X,Y}"'] & \mathrm{Pol}(X,W) \arrow[d, "\mathcal{P}_{X,W}"] \\
\mathrm{Hom}_{k\text{-}\mathbf{Alg}}(\mathcal{P}(Y), \mathcal{P}(X)) \arrow[r, "\mathcal{P}(i)^*"] & \mathrm{Hom}_{k\text{-}\mathbf{Alg}}(\mathcal{P}(W), \mathcal{P}(X))
\end{tikzcd}$$

This diagram commutes because for every $f \in \mathrm{Pol}(X,Y)$ we have that

$$\mathcal{P}(i)^*(\mathcal{P}(f)) = \mathcal{P}(f) \circ \mathcal{P}(i) = \mathcal{P}(i \circ f) = \mathcal{P}(i_*(f))\,.$$

Since we already know that $\mathcal{P}_{X,W}$ bijective it now sufficies to show that the image of i_* corresponds to the image of $\mathcal{P}(i)^*$.

The image of i_* consists precisely of those polynomial maps $f\colon X \to W$ which restrict to a polynomial map $X \to Y$, which is the case if and only if $f(X) \subseteq Y$.

When we identify the coordinate ring $\mathcal{P}(Y)$ with the quotient $\mathcal{P}(W)/\mathcal{I}(Y)$ as explained in Lemma 21.7, the homomorphism $\mathcal{P}(i)\colon \mathcal{P}(W) \to \mathcal{P}(Y)$, $f \mapsto f \circ i = f|_Y$ corresponds to the canonical projection $\mathcal{P}(W) \to \mathcal{P}(W)/\mathcal{I}(Y)$. It follows that the image of $\mathcal{P}(i)^*$ consists precisely of those k-algebra homomorphisms $F\colon \mathcal{P}(W) \to \mathcal{P}(X)$ which can be extended to an algebra homomorphisms $\mathcal{P}(W)/\mathcal{I}(Y) \to \mathcal{P}(X)$. This is the case if and only if $\mathcal{I}(Y) \subseteq \ker F$.

We thus need to show a polynomial map $f\colon X \to W$ satisfies $f(X) \subseteq Y$ if and only if $\mathcal{I}(Y) \subseteq \ker f^*$. This holds because

$$f(X) \subseteq Y \iff f(X) \subseteq \mathcal{V}(\mathcal{I}(Y)) \iff \mathcal{I}(f(X)) \supseteq \mathcal{I}(Y) \iff \ker f^* \supseteq \mathcal{I}(Y)\,,$$

where we use that

$$\begin{aligned}\mathcal{I}(f(X)) &= \{g \in \mathcal{P}(W) \mid g|_{f(X)} = 0\} = \{g \in \mathcal{P}(W) \mid (g \circ f)|_X = 0\} \\ &= \{g \in \mathcal{P}(W) \mid g \circ f = 0\} = \{g \in \mathcal{P}(W) \mid f^*(g) = 0\} = \ker f^*\,.\end{aligned}$$

This finishes the proof. □

Remark 21.12. The functor $\mathcal{P}\colon k\text{-}\mathbf{Aff} \to k\text{-}\mathbf{Alg}$ is a contravariant embedding by Proposition 21.11. It follows that k-**Aff** is dual to a strictly full subcategory of k-**Alg**. It follows from Lemma 21.7 that this strictly full subcategory has as objects precisely those k-algebras which are isomorphic to a k-algebra of the form $k[X_1, \dots, X_n]/I$ where $I \trianglelefteq k[X_1, \dots, X_n]$ is a vanishing ideal.

If k is algebraically closed then vanishing ideals are precisely radical ideals, and we get a nice description of the category dual to k-**Aff**:

Theorem 21.13. If k is algebraically closed, then the functor $\mathcal{P}\colon k\text{-}\mathbf{Aff} \to k\text{-}\mathbf{Alg}$ restrict to dualities between strictly full subcategories

$$\left\{ \begin{matrix} \text{affine algebraic} \\ \text{varieties over } k \end{matrix} \right\} \longrightarrow \left\{ \begin{matrix} \text{finitely generated} \\ k\text{-algebras which are} \\ \text{reduced} \end{matrix} \right\}$$

and

$$\left\{ \begin{matrix} \text{irreducible} \\ \text{affine algebraic} \\ \text{varieties over } k \end{matrix} \right\} \longrightarrow \left\{ \begin{matrix} \text{finitely generated} \\ k\text{-algebras which are} \\ \text{integral domains} \end{matrix} \right\} .$$

Proof. A k-algebra A is finitely generated if and only if $A \cong k[X_1, \dots, X_n]/I$ for some $n \geq 0$ and some ideal $I \trianglelefteq k[X_1, \dots, X_n]$, and the ideal I is radical (resp. prime) if and only if $k[X_1, \dots, X_n]/I \cong A$ is reduced (resp. an integral domain). □

Remark 21.14. Let k be algebraically closed. If A is a finitely generated k-algebra then $A \cong k[X_1, \dots, X_n]/I$ for some $n \geq 1$ and ideal $I \trianglelefteq k[X_1, \dots, X_n]$. If A is reduced then the ideal I is radical and it follows that $X \coloneqq \mathcal{V}(I) \subseteq k^n$ is an affine variety with $\mathcal{I}(X) = I$. It then follows that

$$\mathcal{P}(X) \cong k[X_1, \dots, X_n]/\mathcal{I}(X) = k[X_1, \dots, X_n]/I \cong A\,.$$

This construction can now be used to constructed an inverse of the duality $\mathcal{P}$.

Remark 21.15. If k is algebraically closed the one could also add another duality in the style of Theorem 20.13, namely

$$\left\{ \begin{matrix} \text{one-point} \\ \text{affine algebraic} \\ \text{varieties over } k \end{matrix} \right\} \longrightarrow \left\{ \begin{matrix} \text{finitely generated} \\ k\text{-algebras which are} \\ \text{fields} \end{matrix} \right\} .$$

The image of the left hand side under $\mathcal{P}$ is (up to isomorphism) just k itself, and we retrieve Zariski's lemma from the geometric picture of Corollary 19.23. With this, we have altogether shown the following implications:

$$\begin{tikzcd}
\text{Corollary 19.23} \arrow[rr, Rightarrow] & & \substack{\text{Zariski's Lemma}\\ \text{for alg. closed fields}} \arrow[d, Rightarrow] \\
\substack{\text{strong}\\ \text{Nullstellensatz}} \arrow[u, Rightarrow] \arrow[dr, Leftrightarrow] & & \substack{\text{weak}\\ \text{Nullstellensatz}} \\
& \text{Nullstellensatz} \arrow[ur, Leftrightarrow] &
\end{tikzcd}$$

Definition 21.16. Let X be an affine algebraic variety and let $Y \subseteq X$, $I \trianglelefteq \mathcal{P}(V)$.

a) The set
$$\mathcal{I}_X(Y) = \{f \in \mathcal{P}(X) \mid f(y) = 0 \text{ for every } y \in Y\}$$
is the *vanishing ideal* of Y in $\mathcal{P}(X)$.

b) The ideal I is a *vanishing ideal* if I is the vanishing ideal of some subset $Y \subseteq X$.

c) The set
$$\mathcal{V}_X(I) = \{x \in X \mid f(x) = 0 \text{ for every } f \in I\}$$
is the *vanishing set* of I in X.

21.17. Let $V \subseteq X$ be an affine variety. We identify $\mathcal{P}(X)$ with $\mathcal{P}(V)/\mathcal{I}(X)$ as explained in Lemma 21.7.

For every subset $Y \subseteq X$ the vanishing ideal $\mathcal{I}_X(Y)$ is then given by $\mathcal{I}(Y)/\mathcal{I}(X)$. (This shows in particular that $\mathcal{I}_X(Y)$ is indeed an ideal in $\mathcal{P}(X)$.) The subset Y is closed in X if and only if it is closed in V because X is closed in V. Whether Y is irreducible, or just a singleton $Y = \{y\}$ also does not depend on whether we view Y as a subspace of X or of V.

Every ideal $I \trianglelefteq \mathcal{P}(X)$ is of the form $I = I'/\mathcal{I}(X)$ for a unique ideal $I' \trianglelefteq \mathcal{P}(V)$ with $I' \supseteq \mathcal{I}(X)$, and we have that $\mathcal{V}_X(I) = \mathcal{V}(I')$. The ideal I is reduced (resp. prime, resp. maximal) if and only if I' is reduced (resp. prime, resp. maximal) because

$$\mathcal{P}(X)/I = (\mathcal{P}(V)/\mathcal{I}(X))/(I'/\mathcal{I}(X)) \cong \mathcal{P}(V)/I' .$$

Moreover, I is a vanishing ideal (in $\mathcal{P}(X)$) if and only if I' is a vanishing ideal (in $\mathcal{P}(V)$).

With this we find altogether that the bijections from Theorem 20.13 generalize to affine algebraic varieties:

Theorem 21.18. Let X be an affine variety.

a) The maps $\mathcal{I}_X, \mathcal{V}_X$ restrict to the following mutually inverse bijections:

$$\begin{tikzcd}
\left\{\begin{matrix}\text{algebraic subsets}\\ Y \subseteq X\end{matrix}\right\} \arrow[r, shift left, "\mathcal{I}_X"] \arrow[r, leftarrow, shift right, "\mathcal{V}_X"'] & \left\{\begin{matrix}\text{vanishing ideals}\\ I \trianglelefteq \mathcal{P}(X)\end{matrix}\right\} \\
\rotatebox{90}{$\subseteq$} & \rotatebox{90}{$\subseteq$} \\
\left\{\begin{matrix}\text{irreducible}\\ \text{algebraic subsets}\\ Y \subseteq X\end{matrix}\right\} \arrow[r, shift left, "\mathcal{I}_X"] \arrow[r, leftarrow, shift right, "\mathcal{V}_X"'] & \left\{\begin{matrix}\text{vanishing ideals}\\ \mathfrak{p} \trianglelefteq \mathcal{P}(X)\\ \text{which are prime}\end{matrix}\right\} \\
\rotatebox{90}{$\subseteq$} & \rotatebox{90}{$\subseteq$} \\
\left\{\ \text{points } x \in X\ \right\} \arrow[r, shift left, "\mathcal{I}_X"] \arrow[r, leftarrow, shift right, "\mathcal{V}_X"'] & \left\{\begin{matrix}\text{vanishing ideals}\\ \mathfrak{m} \trianglelefteq \mathcal{P}(X)\\ \text{which are maximal}\end{matrix}\right\}
\end{tikzcd}$$

b) If k is algebraically closed then the maps $\mathcal{I}_X, \mathcal{V}_X$ restrict to the following mutually inverse bijections:

$$\begin{tikzcd}
\left\{\begin{matrix}\text{algebraic subsets}\\ Y \subseteq X\end{matrix}\right\} \arrow[r, shift left, "\mathcal{I}_X"] \arrow[r, leftarrow, shift right, "\mathcal{V}_X"'] & \left\{\begin{matrix}\text{radical ideals}\\ I \trianglelefteq \mathcal{P}(X)\end{matrix}\right\} \\
\rotatebox{90}{$\subseteq$} & \rotatebox{90}{$\subseteq$} \\
\left\{\begin{matrix}\text{irreducible}\\ \text{algebraic subsets}\\ Y \subseteq X\end{matrix}\right\} \arrow[r, shift left, "\mathcal{I}_X"] \arrow[r, leftarrow, shift right, "\mathcal{V}_X"'] & \left\{\begin{matrix}\text{prime ideals}\\ \mathfrak{p} \trianglelefteq \mathcal{P}X)\end{matrix}\right\} \\
\rotatebox{90}{$\subseteq$} & \rotatebox{90}{$\subseteq$} \\
\left\{\ \text{points } x \in X\ \right\} \arrow[r, shift left, "\mathcal{I}_X"] \arrow[r, leftarrow, shift right, "\mathcal{V}_X"'] & \left\{\begin{matrix}\text{maximal ideals}\\ \mathfrak{m} \trianglelefteq \mathcal{P}(X)\end{matrix}\right\}
\end{tikzcd}$$

Part III

Semisimplicity

Semisimplicity of Modules and Rings

22. Semisimple Modules

22.1. Characterizations of Semisimple Modules

Conventions 22.1. We require all occuring rings to be unitary, but we do not require them to be commutative. My *module* we mean *left module* unless otherwise stated. We require all occuring modules to be unitary, i.e. if R is a ring and M is an R-module then

$$1 \cdot m = m$$

for every $m \in M$. We also require all k-algebras to be unitary. A module over a k-algebra is therefore in particular a k-vector spaces, and module homomorphisms are always k-linear.

Conventions 22.2. In this section, R denotes a ring.

Definition 22.3. Let M be an R-module.

a) The module M is *simple* if M is nonzero and $0, M$ are the only submodules of M.

b) A submodule $N \leq M$ is *maximal* if it is a maximal proper submodule. In other words, N is a proper submodule and for every submodule $N' \leq M$ with $N \leq N'$ we have that $N' = N$ or $N' = M$.

Example 22.4.

a) Let V be a representation of a group G over a field k. Then V is simple as a $k[G]$-module if and only if V is irreducible as representation of G.

b) If k be a field. Then a k-vector space V is simple (as a k-module) if and only if V is one-dimensional. The same holds for vector spaces over a skew field D.

c) If D is a skew field and $n \geq 1$ then D^n is simple as an $\mathrm{M}_n(D)$-module: Let $U \leq D^n$ be a nonzero submodule and let $x \in U$ with $x \neq 0$. It then follows that $x_i \neq 0$ for some $i = 1, \dots, n$. If $D \in \mathrm{M}_n(D)$ is the diagonal matrix with $D_{ii} = x_i^{-1}$ and $D_{jj} = 0$ for $j \neq i$ then it follows that

$$e_i = Dx \in U\,.$$

For every $j = 1, \dots, n$ it then follows by using a suitable permutation matrix $P \in \mathrm{M}_n(D)$ that

$$e_j = Pe_i \in U\,.$$

This shows that $e_1, \dots, e_n \in U$ and therefore that $U = D^n$.

d) If more generally D is a skew field and I is any nonempty index set then $D^{\oplus I}$ is simple as an $\mathrm{M}_I^{\mathrm{cf}}(D)$-module. Here $\mathrm{M}_I^{\mathrm{cf}}(D)$ denotes the ring of column finite $(I \times I)$-matrices with entries in D (see Definition A7.22 and Lemma A7.23). This can be seen in the same way as in the finite case $I = \{1, \dots, n\}$ above.

Remark 22.5. One can also reformulate the definitions of simple modules and maximal submodules: An R-module M is simple if and only if M contains precisely two submodules, and a submodule $N \leq M$ is maximal if and only if there exists precisely two submodules N' between N and M.

Lemma 22.6. Let M be an R-module and let $N \leq M$ be a submodule. Then N is a maximal submodule if and only if M/N is simple.

Proof. This follows from the 1:1-correspondence

$$\begin{aligned} \{\text{submodules } N' \leq M \text{ with } N \leq N' \leq M\} &\longleftrightarrow \{\text{submodules } P \leq M/N\} \\ N' &\longmapsto N'/N \end{aligned}$$

and the characterization of simplicity and maximality from Remark 22.5. □

Corollary 22.7. Let M be an R-module and let $N, P \leq M$ be submodule with $M = N \oplus P$. Then N is simple if and only if P is maximal.

Proof. This follows from Lemma 22.6 because $M/P \cong N$. □

Lemma 22.8. A nonzero R-module M is simple if and only if every nonzero $x \in M$ is a cyclic generator of M.

Proof. If M is simple then for every nonzero $x \in M$ the cyclic submodule Rx is nonzero, from which it then follows that $Rx = M$ by the simplicity of M.

Suppose on the other hand that every nonzero $x \in M$ is a cyclic generator of M. Every nonzero submodule $N \leq M$ contains some nonzero $x \in N$, for which it then follows that $M = Rx \leq N$ and therefore that $M = N$. □

Corollary 22.9. The simple R-modules are up to isomorphism precisely those R-modules of the form R/I for a maximal left ideal $I \trianglelefteq R$.

Proof. Every simple R-module is up to isomorphism of the form R/I for some left ideal $I \trianglelefteq R$ by Lemma 22.8, and R/I is simple if and only if I is maximal by Lemma 22.6. □

Example 22.10. If R is a principal ideal domain then the simple R-modules are up to isomorphism precisely R/p with $p \in R$ prime. It follows for $R = \mathbb{Z}$ that the simple R-modules are up to isomorphism precisely those of the form $\mathbb{Z}/p$ with p prime.

Lemma 22.11. Every nonzero finitely generated R-module M admits a maximal submodule.

Proof. Let $m_1, \dots, m_t$ be generators of M. A submodule $N \leq M$ is proper if and only if N does not contain all m_i, and by Zorn's lemma there exists a submodule which is maxmial with this property. □

Lemma 22.12. Let M be an R-module and let $P \leq N \leq M$ be submodules. Let C be a direct complement of P in M. Then $C \cap N$ is a direct complement of P in N.

First proof. It follows from $P \leq N \leq M$ that

$$(P + C) \cap N = P + (C \cap N)$$

by Lemma A8.6. We thus have that

$$P \cap (C \cap N) = P \cap C \cap N = 0 \cap N = 0$$

as well as

$$P + (C \cap N) = (P + C) \cap N = M \cap N = N\,,$$

which proves the claim. □

Second proof. Let $\pi\colon M \to M$ be the projection onto P along the decomposition $M = P \oplus C$. It follows from $P \leq N$ that $\pi(N) = P$. It further follows that π restrict to an endomorphism $\pi|_N \colon N \to N$ with $\operatorname{im} \pi|_N = P$ and $\ker \pi|_N = \ker \pi \cap N = C \cap N$. The restriction $\pi|_N$ is again idempotent and thus corresponds to a decomposition (see Corollary A5.11) given by

$$N = \operatorname{im} \pi|_N \oplus \ker \pi|_N = P \oplus (C \cap N)\,,$$

as desired. □

Proposition 22.13. For every R-module M the following conditions are equivalent:

a) The module M is a direct sum of simple submodules.

b) The module M is the sum of simple submodules.

c) Every submodule of M has a direct complement.

Proof.

a) $\implies$ b) Every direct sum is in particular a sum.

b) $\implies$ c) Suppose that $M = \sum_{i \in I} L_i$ where every L_i is a simple submodule of M, and let $N \leq M$ be any submodule. For every $J \subseteq I$ let

$$M_J \coloneqq \sum_{j \in J} L_j\,.$$

It follows from Zorn's lemma that there exists a maximal subset $J \subseteq I$ for which $N \cap M_J = 0$. Then $P \coloneqq M_J$ is a direct complement of N:

Otherwise there would exist some $i \in I$ with $L_i \nleq N \oplus P$. Then the intersection $L_i \cap (N \oplus P)$ is a proper submodule of the simple module L_i and it follows that $L_i \cap (N \oplus P) = 0$. It then follows that the sum $(N \oplus P) + L_i$ is direct, so that

$$(N \oplus P) + L_i = N \oplus P \oplus L_i = N \oplus P'$$

and thus $N \cap P' = 0$ for $P' \coloneqq P \oplus L_i = M_{J'}$ with $J' = J \cup \{i\}$. It follows from $L_i \nleq N \oplus M_J$ that $i \notin J$ and thus $J \subsetneq J'$. This contradicts the maximality of J.

c) $\implies$ b) It follows from Corollary 22.12 that for all submodules $N \leq C \leq M$ the module N also has a direct complement in C.

Let $S \leq M$ be the sum of all simple submodules of M and suppose that $S \neq M$. Let P be a direct complement of S so that $M = S \oplus P$. Then $P \neq 0$ does not contain any simple submodule.

For $x \in P$ with $x \neq 0$ the cyclic submodule $C := Rx \leq P$ contains a maximal submodule $N \lneq C$ by Lemma 22.11. As noted above there exists a submodule $S' \leq C$ with $C = N \oplus S'$. Then S' is simple by Lemma 22.6, which shows that P contain a simple submodule.

b) $\implies$ a) Suppose that $M = \sum_{i \in I} L_i$ where each L_i is a simple submodules of M.

By Zorn's lemma there exists a maximal subset $J \subseteq I$ for which the sum $\sum_{j \in J} L_j$ is direct: Indeed, let $(J_k)_{k \in K}$ be a chain of subsets $J_k \subseteq I$ such that for every $k \in K$ the sum $\sum_{j \in J_k} L_j$ is direct. If for $J' := \bigcup_{k \in K} J_k$ the sum $\sum_{j \in J'} L_j$ were not direct then there would exist a non-trivial linear combination $0 = \sum_{j \in J'} m_j$ with $m_j \in L_j$ for every $j \in J$. There would then exist some $k \in K$ such that every of the finitely many $j \in J'$ with $m_j \neq 0$ is already contained in J_k. The existence of the non-trivial linear combination $0 = \sum_{j \in J'} m_j = \sum_{j \in J_k} m_j$ would then contradict the directness of the sum $\bigoplus_{j \in J_k} L_j$. This shows that conditions for Zorn's lemma are satisfied. (Note that for the empty set $\emptyset$ the sum $\sum_{j \in \emptyset} L_j$ is direct.)

Let $N := \sum_{j \in J} L_j = \bigoplus_{j \in J} L_j$. If $N \neq M$ then there would exist some $i \in J$ with $L_i \nleq N$. It would then follows that $L_i \cap N$ is a proper submodule of L_i which would show that $L_i \cap N = 0$. For $K := J \cap \{i\}$ the sum $\sum_{k \in K} L_k$ would then still direct, but it would follows from $L_i \nleq N$ that $i \notin J$, which would then contradict the maximality of J. We thus have that $M = N = \bigoplus_{j \in J} L_j$. □

Definition 22.14. An R-module M is *semisimple* or *completely reducible* if it satisfies one (and thus all) of the conditions from Proposition 22.13.

Remark 22.15. If $L_i \leq M$, $i \in I$ is a collection of simple modules then the above proof of Proposition 22.13 shows that there exists a subset $J \subseteq I$ with $\sum_{i \in I} L_i = \bigoplus_{j \in J} L_j$.

Warning 22.16. Remark 22.15 does not generalize to arbitrary sums of submodules, as the example $\mathbb{Z} = 2\mathbb{Z} + 3\mathbb{Z}$ shows.

Example 22.17.

a) If k is a field then every k-module is a sum of one-dimensional, und thus simple, submodules. This shows that every k-module is semisimple. Note however that a decomposition of a k-vector space into a direct sum one-dimensional subspaces is far from unique, as it corresponds to the choice of a basis of V (up to scaling of the basis vectors).

b) Let k be a field and let

$$R := \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \,\middle|\, a, b, c \in k \right\} \subseteq \mathrm{M}_2(k) \,.$$

Then $M := k^2$ is not semisimple as an R-module because the only nonzero submodule of k^2 is

$$N := \left\{ \begin{bmatrix} x \\ 0 \end{bmatrix} \,\middle|\, x \in k \right\} .$$

Indeed, we have that

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ax + by \\ cy \end{bmatrix} ,$$

so if a submodule $N' \leq k^2$ contains an element $[x, y]^T$ with $y \neq 0$ then it contains both

$$\begin{bmatrix} 0 & y^{-1} \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

and

$$\begin{bmatrix} 0 & 0 \\ 0 & y^{-1} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

and it follows that $M = k^2$.

c) If G is a finite group and k is a field with $\operatorname{char}(k) \nmid |G|$ then every finite-dimensional representation of G over k is semisimple by Maschke's theorem, and therefore semisimple as a $k[G]$-module. This shows in particular that the regular $k[G]$-module, i.e. $k[G]$ itself, is semisimple.

Lemma 22.18. Let R be a ring.

a) If $(M_i)_{i \in I}$ is a collection of semisimple R-modules then $\bigoplus_{i \in I} M_i$ is semisimple.

b) If $(M_i)_{i \in I}$ is a collection of semisimple R-submodules $M_i \leq M$ then $\sum_{i \in I} M_i$ is again semisimple.

c) If M is a semisimple R-module and $N \leq M$ a submodule then N is semisimple.

d) If M is a semisimple R-module and $N \leq M$ a submodule then M/N is semisimple.

Proof.

a) We can write each M_i as a direct sum $M_i = \bigoplus_{j \in J_i} L^i_j$ where $L^i_j \leq M_i$ is a simple submodule for every $j \in J_i$. Then

$$\bigoplus_{i \in I} M_i = \bigoplus_{i \in I} \bigoplus_{j \in J_i} L^i_j$$

is a decomposition into simple submodules.

b) Every M_i is a sum $M_i = \sum_{j \in J_i} L^i_j$ of simple R-modulse L^i_j. It follows that $\sum_{i \in I} M_i = \sum_{i \in I} \sum_{j \in J_i} L^i_j$ is sum of simple modules.

c) This follows from Corollary 22.12.

d) There exists a direct complement $P \leq M$ of N. It follows from part d) that $M/N \cong P$ is again semisimple. □

Warning 22.19. If M is an R-module and $N \leq M$ is a submodule such that both N and M/N are semisimple then M does not need to be semisimple itself: In part b) of Example 22.17 the module M is not semisimple, but both the submodule N and the qotient M/N are one-dimensional and therefore simple.

Definition 22.20. The *socle* of an R-module M is

$$\operatorname{soc}(M) \coloneqq \sum_{\substack{L \leq M \\ \text{simple}}} L \,.$$

Remark 22.21. If M is an R-module then $\operatorname{soc}(M)$ is the biggest semisimple submodule of M, and M is semisimple if and only if $M = \operatorname{soc}(M)$. We have already encountered the socle in the proof of Proposition 22.13 where $S = \operatorname{soc}(M)$.

22.2. Schur's Lemma

Proposition 22.22 (Schur's lemma)**.** Let M, N be R-modules and let $f \colon M \to N$ be a nonzero homomorphism of R-modules.

a) If M is simple then f is injective.

b) If N is simple then f is surjective.

Let M, N be simple.

c) The homomorphism f is bijective.

d) The endomorphism ring $\operatorname{End}_R(M)$ is a skew field.

If R has the additional structure of a k-algebra then we also have the following:

e) The endomorphism ring $\operatorname{End}_R(M)$ is a division k-algebra.

f) If k is algebraically closed and M is finite-dimensional over k then $\operatorname{End}_R(M) = k$.

Proof.

a) The kernel $\ker(f)$ is a proper submodule of M, so $\ker(f) = 0$.

b) The image $\operatorname{im}(f)$ is a nonzero submodule of N, so $\operatorname{im}(f) = N$.

c) This follows from parts a), b).

d) It follows from $M \neq 0$ that $\operatorname{id}_M \neq 0$. The claim is therefore a reformulation of part d).

e) This is a combination of part e) and the k-algebra structure of $\operatorname{End}_R(M)$.

f) It follows from part f) that $\operatorname{End}_R(M)$ is a finite-dimensional skew field extension. It follows that $\operatorname{End}_R(M) = k$ because k is algebraically closed. □

Remark 22.23. Schur's lemma for representation of groups can be derived from Schur's lemma for modules by using the correspondence between k-representations of a group G and modules over the group algebra $k[G]$.

Corollary 22.24. Let M, M' be semisimple R-modules with $M = \sum_{i \in I} L_i$ and $N = \sum_{j \in J} L'_j$ for simple submodules $L_i \leq M$, $L'_j \leq M'$. If there exists a nonzero homomorphism of R-modules $f\colon M \to M'$ then $L_i \cong L'_j$ for some $i \in I$, $j \in J$.

Proof. It follows that $f|_{L_i} \neq 0$ for some $i \in I$. By Remark 22.15 we may assume that the sum $\sum_{j \in J} L'_j$ is direct by shrinking J if necessary. It then follows from $f|_{L_i} \neq 0$ that there exists some $j \in J$ for which the decomposition

$$f'\colon L_i \hookrightarrow M \xrightarrow{f} M' = \bigoplus_{k \in J} L'_k \twoheadrightarrow L'_j$$

is nonzero. It then follows from Schur's Lemma that f' is an isomorphism, which shows that $L_i \cong L'_j$. □

Corollary 22.25.

a) Suppose that $M = M_1^{\oplus n_1} \oplus \cdots \oplus M_r^{\oplus n_r}$ where $M_1, \dots, M_r$ are pairwise non-isomorphic simple R-modules and $n_1, \dots, n_r \geq 1$. Then

$$\begin{aligned} \operatorname{End}_R(M) &\cong \operatorname{End}_R(M_1^{\oplus n_1}) \times \cdots \times \operatorname{End}_R(M_r^{\oplus n_r}) \\ &\cong \mathrm{M}_{n_1}(D_1) \times \cdots \times \mathrm{M}_{n_r}(D_r) \end{aligned}$$

as rings, where $D_i \coloneqq \operatorname{End}_R(M_i)$ for every $i = 1, \dots, r$ and the first isomorphism is given by

$$f \mapsto \left(f\Big|_{M_1^{\oplus n_1}}, \dots, f\Big|_{M_t^{\oplus n_t}} \right).$$

b) Suppose more generally that $M = \bigoplus_{i \in I} M_i^{\oplus J_i}$ where M_i, $i \in I$ are pairwise non-isomorphic simple R-modules and J_i, $i \in I$ are index sets. Then

$$\operatorname{End}_R(M) \cong \prod_{i \in I} \operatorname{End}_R(M_i^{\oplus J_i}) \cong \prod_{i \in I} \mathrm{M}^{\mathrm{cf}}_{J_i}(D_i)$$

as rings, where $D_i \coloneqq \operatorname{End}_R(M_i)$ for all $i \in I$ and the first isomorphism is given by

$$f \mapsto \left(f\Big|_{M_i^{\oplus J_i}} \right)_{i \in I}.$$

Here $\mathrm{M}^{\mathrm{cf}}_{J_i}(D_i)$ denotes the ring of column finite $(J_i \times J_i)$-matrices with entries in D_i (see Definition A7.22 and Lemma A7.23).

If R is a k-algebra, then these are isomorphisms of k-algebras.

Proof.

a) This follows from Corollary A7.15 because $\operatorname{Hom}_R(M_i, M_j) = 0$ for all $i \neq j$ by Schur's lemma.

b) The first isomorphism follows from Corollary A7.19 because $\operatorname{Hom}_R(M_i, M_j) = 0$ for all $i \neq j$ by Schur's lemma. The second isomorphism then follows from Corollary A7.25 because each M_i is cyclic and thus finitely generated. □

Remark 22.26. For an algebraically closed field k we can ask ourselves how part f) of Schur's lemma generalizes to infinite-dimensional A-modules, where A is a k-algebra. We fix a cardinality κ and will examine under what conditions the following holds:

a) It holds that $\operatorname{End}_A(M) = k$ for every k-algebra A and every simple A-module M of dimension $\dim_k M \leq \operatorname{card} \kappa$.

Note that if D/k is any proper skew field extension then for $A = D$, $M = D$ we have that $\operatorname{End}_A(M) \cong D^{\mathrm{op}}$ by Lemma A4.10 with $k \subsetneq D^{\mathrm{op}}$. If on the other hand for any k-algebra A and simple A-module M the inclusion $k \subsetneq \operatorname{End}_A(M) =: D$ is proper then we can regard M as a left D-vector space via

$$\varphi \cdot m = \varphi(m)$$

for all $\varphi \in \operatorname{End}_R(M)$, $m \in M$ and it follows that

$$\dim_k M = \dim_k D \cdot \underbrace{\dim_D M}_{\geq 1} \geq \dim_k D\,.$$

Together this shows that condition a) is equivalent to the following condition:

b) There exist no proper skew field extension D/k of degree $\dim_k D \leq \kappa$.

A skew field extension D/k is proper if and only if it is trancendental, i.e. if D contains a trancendental element, because k is algebraically closed. We can therefore reformulate condition b) as follows:

c) There exist no trancendental skew field extension D/k of degree $\dim_k D \leq \kappa$, i.e. every transcendental skew field extension D/k has degree $\dim_k D > \kappa$.

If D/k is a trancendental skew field extension with $\varphi \in D$ trancendental over k then it follows that D contains a copy of the function field $k(t)$, namely $k(\varphi)$. It then follows that $\dim_k D \geq \dim_k k(t)$. We have on the other hand that $k(t)/k$ is a trancendental (skew) field extension. Together this shows that for any cardinality κ' there exists a trancendental skew field extension D/k of degree $\dim_k D = \kappa'$ if and only if $\kappa' \geq \dim_k k(t)$. This leads to the following entry to our list of equivalent conditions:

d) It holds that $\kappa < \dim_k k(t)$.

We can determine the dimension $\dim_k k(t)$ in question: The elements $1/(t-\lambda) \in k(t)$ with $\lambda \in k$ are linearly independent over k, so we find that $\dim_k k(t) \geq \operatorname{card} k$. It follows on the other hand from k being infinite that

$$\operatorname{card} k = \operatorname{card} k[t] = \operatorname{card} k(t)\,,$$

from which it follows that $\dim_k k(t) \leq \operatorname{card} k$. This shows that $\dim_k k(t) = \operatorname{card} k$. With this we arrive at the last equivalent condition for our list:

e) It holds that $\kappa < \operatorname{card} k$.

The above disucission is motivated by [Qui69], which in turn credits [Dix63].

Example 22.27.

a) If k is any algebraically closed field then k is inifinite and we retrieve part f) of Schur's lemma.

b) If A is a $\mathbb{C}$-algebra and M is a countable-dimensional simple A-module then $\operatorname{End}_A(M) = \mathbb{C}$.

c) For the $\overline{\mathbb{Q}}$-algebra $A := \overline{\mathbb{Q}}(t)$ the A-module $M := A$ is simple and countable dimensional over $\overline{\mathbb{Q}}$ but $\operatorname{End}_A(M) = \overline{\mathbb{Q}}(t) \supsetneq \overline{\mathbb{Q}}$.

22.3. Isotypical Components and Multiplicity Spaces

Conventions 22.28. In this subsection R denotes a ring, M, N denote R-modules and E, F denote simple R-modules.

Isotypical Components

22.29. While every semisimple R-module M can be decomposed into a direct sum of simple R-modules, this decomposition is generally not unique as seen in part a) of Example 22.17. We will now show that every semisimple module has a canonical decomposition into isotypical components.

Definition 22.30. The *E-isotypical component* of M is

$$M_E := \sum_{\substack{L \leq M \\ L \cong E}} L\,.$$

The module M is *E-isotypical* if $M = M_E$.

Lemma 22.31. The E-isotypical component M_E is E-isotypical.

Proof. We have that

$$(M_E)_E = \sum_{\substack{L \leq M_E \\ L \cong E}} L = \sum_{\substack{L \leq M \\ L \cong E}} L = M_E$$

because every submodule $L \leq M$ which is isomorphic to E is contained in M_E. □

Remark 22.32. The E-isotypical component M_E is semisimple because it is a sum of simple R-modules. It follows that every E-isotypical module is semisimple.

Example 22.33. If V is a representation of a group G, i.e. a $k[G]$-module, then V^G is the isotypical component associated to the trivial irreducible representation. We have thus previously encountered the idea of isotypical components in Proposition 17.15 when construction the Reynolds operator.

Lemma 22.34. *Let $N, N' \leq M$ be semisimple submodules with $N = \sum_{i \in I} L_i$ and $N' = \sum_{j \in J} L'_j$ for simple submodules $L_i, L'_j \leq M$. If $N \cap N' \neq 0$ then $L_i \cong L'_j$ for some $i \in I$, $j \in J$.*

Proof. The module $N \cap N'$ is again semisimple because it is a submodule of the semisimple modules N, N'. It follows from $N \cap N' \neq 0$ that $N \cap N'$ contains a simple module L. By applying Corollary 22.24 to the inclusions $L \hookrightarrow N$ and $L \hookrightarrow N'$ it follows that $L \cong L_i$ and $L \cong L'_j$ for some $i \in I$, $j \in J$. □

Definition 22.35. The set $\operatorname{Irr}(R)$ is the set of isomorphism classes of simple R-modules.

Remark 22.36. It follows from Corollary 22.9 that $\operatorname{Irr}(R)$ is indeed just a set, and not a proper class.

Remark 22.37. The isotypical component M_E does only depend on the isomorphism class $[E] \in \operatorname{Irr}(R)$ of E.

Theorem 22.38 (Isotypical Decomposition)**.** *If M is semisimple then*

$$M = \bigoplus_{[E] \in \operatorname{Irr}(R)} M_E \,,$$

and if $M = \sum_{i \in I} L_i$ for simple submodules $L_i \leq M$ then

$$M_E = \sum_{\substack{i \in I \\ L_i \cong E}} L_i$$

for every $[E] \in \operatorname{Irr}(R)$.

Proof. We have that

$$M = \sum_{i \in I} L_i = \sum_{[E] \in \operatorname{Irr}(R)} \underbrace{\sum_{\substack{i \in I \\ L_i \cong E}} L_i}_{\leq M_E} \leq \sum_{[E] \in \operatorname{Irr}(R)} M_E \,.$$

It thus sufficies to show that the sum $M = \sum_{[E] \in \operatorname{Irr}(R)} M_E$ is direct, i.e. that

$$M_E \cap \left(\sum_{\substack{[F] \in \operatorname{Irr}(R) \\ [F] \neq [E]}} M_F \right) \neq 0$$

for every $[E] \in \operatorname{Irr}(R)$. This follows from Lemma 22.34. □

Corollary 22.39. If M is E-isotypical and $F \ncong E$ then $M_F = 0$, i.e. if $L \leq M$ is simple then $F \cong E$.

Proof. The module M is semisimple and the isotypical decomposition of M is given by $M = M_E$. It follows that $M_F = 0$ for every $[F] \in \operatorname{Irr}(R)$ with $[F] \neq [E]$. □

Lemma 22.40. If $N \leq M$ is a submodule then $N_E = N \cap M_E$.

Proof. It follows from $N \leq M$ that $N_E \leq M_E$ and therefore that $N_E \leq N \cap M_E$. The module $N \cap M_E$ is a submodule of M_E and therefore semisimple. For every simple submodule $L \leq N \cap M_E \leq M_E$ we have that $L \cong E$ by Corollary 22.39 and therefore $L \leq N_E$. It follows that $N \cap M_E \leq N_E$. □

Corollary 22.41. If M is E-isotypical then every submodule $N \leq M$ is E-isotypical.

Proof. We have that $N_E = N \cap M_E = N \cap M = N$. □

Lemma 22.42. If M is semisimple and $M = \bigoplus_{i \in I} L_i$ is a decomposition into simple submodules $L_i \leq M$ then for every simple submodule $E \leq M$ there then exists some $i \in I$ with $E \cong L_i$.

First proof. This follows from $0 \neq E \leq M_E \leq \bigoplus_{i \in I, L_i \cong E} L_i$. □

Second proof. Apply Corollary 22.24 to the inclusion $E \hookrightarrow M = \sum_{i \in I} L_i$. □

Lemma 22.43. Every homomorphism of R-modules $f\colon M \to N$ restrict to a homomorphism $f_E\colon M_E \to N_E$.

Proof. For every simple submodule $L \leq M$ the restriction $f|_L$ is either zero or injective, and it follows that either $f(L) = 0$ or $f(L) \cong L$. It follows that

$$f(M_E) \leq f\left(\sum_{\substack{L \leq M \\ L \cong E}} L\right) = \sum_{\substack{L \leq M \\ L \cong E}} f(L) \leq \sum_{\substack{L' \leq N \\ L' \cong E}} L' = N_E\,,$$

which proves the claim. □

Corollary 22.44. If M is semisimple, then the map

$$\operatorname{End}_R(M) \to \prod_{[E] \in \operatorname{Irr}(R)} \operatorname{End}_R(M_E), \quad f \mapsto (f_E)_{[E] \in \operatorname{Irr}(R)}$$

is a well-defined isomorphis of rings. If R is a k-algebra, then it is an isomorphism of k-algebras.

Proof. It follows from Lemma 22.43 that every endomorphism $f\colon M \to M$ restrict for every $E \in \operatorname{Irr}(R)$ to an endomorphism $f_E\colon M_E \to M_E$. The statement therefore follows from Corollary A7.18. □

Multiplicities of Simple Summands

22.45. We know from linear algebra that for a k-vector space V with $V \cong k^{\oplus I}$ the cardinality $|I|$ (i.e. the dimension of V) is unique. We will now show how this generalizes to semisimple modules.

Lemma 22.46. Let M be semisimple and let

$$M = L_1 \oplus \cdots \oplus L_n = L'_1 \oplus \cdots \oplus L'_{n'}$$

be two decompositions into finitely many simple submodules $L_i, L'_j \leq M$. Then this decomposition is unique up to permutation and isomorphism, i.e. it follows that $n = n'$ and there exists a bijection $\pi\colon \{1, \dots, n\} \to \{1, \dots, n'\}$ with $L'_{\pi(i)} \cong L_i$ for every $i = 1, \dots, n$.

First proof. We use the language of composition series (see Appendix A8): Both decompositions give rise to composition series

$$0 \lneq L_1 \lneq L_1 \oplus L_2 \lneq \cdots \lneq L_1 \oplus \cdots \oplus L_n = M$$

and

$$0 \lneq L'_1 \lneq L'_1 \oplus L'_2 \lneq \cdots \lneq L'_1 \oplus \cdots \oplus L'_{n'} = M$$

with composition factors L_i, L'_j. The claim therefore follows from the Jordan–Hölder Theorem. □

Second proof. Suppose that

$$M \cong E_1^{\oplus n_1} \oplus \cdots \oplus E_r^{\oplus n_r} \cong E_1^{\oplus n'_r} \oplus \cdots \oplus E_r^{\oplus m_r}$$

for simple, pairwise non-isomorphic R-modules $E_1, \dots, E_r$ and $n_i, m_i \geq 0$ for every $i = 1, \dots, r$. We need to show that $n_i = m_i$ for every $i = 1, \dots, r$.

For every $i = 1, \dots, r$ we have that $M_{E_i} \cong E_i^{\oplus n_i}$ and $M_{E_i} \cong E_i^{\oplus m_i}$ by Theorem 22.38. It therefore sufficies to show that for every simple R-module E and all $n, m \geq 0$ it follows from $E^{\oplus n} \cong E^{\oplus m}$ that $n = m$.

Let $f\colon E^{\oplus n} \to E^{\oplus m}$ be an isomorphism of R-modules. Then for $D \coloneqq \operatorname{End}_R(M)$ we may represent f as a matrix $A \in \mathrm{M}(m \times n, D)$ and $f^{-1}\colon E^{\oplus m} \to E^{\oplus n}$ as a matrix $B \in \mathrm{M}(n \times m, D)$ (see Appendix A7 for a more detailed explanation on this). It then follows from $f \circ f^{-1} = \mathrm{id}_{E^{\oplus m}}$ and $f^{-1} \circ f = \mathrm{id}_{E^{\oplus n}}$ that $AB = I_n$ and $BA = I_m$.

The matrix is A is therefore invertible with $A^{-1} = B$. It follows that A defines an isomorphism of right D-vector spaces $D^n \to D^m$ by left multiplication, from which it then further follows that $n = m$ □

Theorem 22.47. Let M be semisimple and let $M = \bigoplus_{i \in I} L_i = \bigoplus_{j \in J} L'_j$ be two decompositions into simple submodules $L_i, L'_j \leq M$. Then for every simple R-module E the sets

$$\{i \in I \mid L_i \cong E\} \quad \text{and} \quad \{j \in J \mid L'_j \cong E\}$$

have the same cardinality.

Proof. We know from Theorem 22.38 that

$$M_E = \bigoplus_{\substack{i \in I \\ L_i \cong E}} L_i = \bigoplus_{\substack{j \in J \\ L_j \cong E}} L_j \,.$$

We may therefore replace M by M_E and thus assume that M is E-isotypical. We then have that $L_i, L'_j \cong E$ for all i, j, and we need to show that $\operatorname{card} I = \operatorname{card} J$. We make the following observation:

Claim. For every $j \in J$ there exists a finite subset $I' \subseteq I$ with $L'_j \leq \bigoplus_{i \in I'} L_i$.

Proof. Let $y \in L'_j$ be nonzero. Then $y = \sum_{i \in I} x_i$ with $x_i \in L_i$ for every $i \in I$ and $x_i = 0$ for all but finitely many $i \in I$. It follows that there exists a finite subset $I' \subseteq I$ with $x \in \bigoplus_{i \in I'} L_i$. It follows from the simplicity of L'_j that x is a cylic generator of L'_j, and therefore that $L'_j \leq \bigoplus_{i \in I'} L_i$. □

We now distinguish between four cases:

- If I and J are both finite then the theorem follows from Lemma 22.46.
- If J is finite then by the above claim that there exists a finite subset $I' \subseteq I$ with $L'_j \leq \bigoplus_{i \in I} L_i$ for every $j \in J$. It then follows that $M = \bigoplus_{i \in I'} L_i$ and therefore that $I = I'$. Then both I, J are finite and the theorem follows from the first case.
- If I is finite then we find in the same way as above that J is finite and that the theorem follows from the first case.
- Suppose now that both I and J are infine. It follows from the above claim that there exists for every $j \in J$ some finite subset $I_j \subseteq I$ with $L'_j \leq \bigoplus_{i \in I_j} L_i$. For $I' := \bigcup_{j \in J} I_j$ we then have that $L'_j \leq \bigoplus_{i \in I'} L_i$ for every $j \in J$. It follows that $M = \bigoplus_{i \in I'} L_i$ and therefore that $I = I'$. Note that $I = I' = \bigcup_{j \in J} I_j$ has at most the cardinality of J because J is infinite and every I_j is finite.

  This shows that $\operatorname{card} I \leq \operatorname{card} J$. It follows in the same way that $\operatorname{card} J \leq \operatorname{card} I$. Together this shows that $\operatorname{card} I = \operatorname{card} J$ by the theorem of Cantor–Schröder–Bernstein. □

Remark 22.48. Theorem 22.47 can be reformulated as stating that there exists a bijection $\pi \colon I \to J$ with $L'_{\pi(i)} \cong L_i$ for every $i \in I$.

Definition 22.49. If $M = \bigoplus_{i \in I} L_i$ is any decomposition into simple submodules $L_i \leq M$ then the cardinality of the set $\{i \in I \mid L_i \cong E\}$ is the *multiplicity of* E *in* M.

Multiplicity Spaces

22.50. Another approach to both isotypical components and multiplicities is given by multiplicity spaces. For this we will require tensor products of modules, a nice introduction to which can be found in [DF04, Chapter 10.4].

22.51. Every nonzero homomorphism $E \to M$ is injective by by Schur's Lemma, so we may think about $\operatorname{Hom}_R(E, M)$ as the space of all embeddings $E \to M$ (together with the zero homomorphism). The images $f(E)$ of the various embeddings $f \in \operatorname{Hom}_R(E, M)$ are precisely those submodules of M which are isomorphic to E, the sum of which is the E-isotypical component M_E. Hence, if we consider the evaluation map

$$\operatorname{Hom}_R(M, E) \times E \to M, \quad (f, e) \mapsto f(e)\,, \tag{22.1}$$

then the image of the induced map

$$\operatorname{Hom}_R(E, M) \otimes_{\mathbb{Z}} E \to M, \quad f \otimes e \mapsto f(e)\,,$$

is precisely the E-isotypical component M_E. But this map will in general not be injective, which we can fix by tensoring over $\operatorname{End}_R(E)$ instead of $\mathbb{Z}$:

We also know from Schur's Lemma that the endomorphism ring $D \coloneqq \operatorname{End}_R(E)$ is a skew field. The R-module E is also a left D-vector space via

$$\varphi \cdot e = \varphi(e)$$

for all $\varphi \in D$, $e \in E$. This also induces a right D-vector space structure on the $\operatorname{Hom}_R(E, M)$ via precomposition, i.e. via

$$f \cdot \varphi = f \circ \varphi$$

for all $f \in \operatorname{Hom}_R(E, M)$, $\varphi \in D$. The evaluation map (22.1) is D-balenced and thus induces a well-defined additive map

$$\operatorname{Hom}_R(E, M) \otimes_D E \to M, \quad f \otimes e \mapsto f(e)\,,$$

whose image is again the E-isotypical component M_E.

The abelian group $\operatorname{Hom}_R(E, M) \otimes_D E$ inherits the structure of a left R-module from E via

$$r \cdot (f \otimes e) = f \otimes (re)$$

for all $r \in R$ and simple tensors $f \otimes e \in \operatorname{Hom}_R(E, M) \otimes_D E$. Indeed, the actions of R and D on E commute in the sense that

$$\varphi \cdot (r \cdot e) = r \cdot (\varphi \cdot e)$$

for all $r \in R$, $\varphi \in D$, $e \in E$ by definition of D. Hence E carries the structure of an D-R^{op}-bimodule via

$$\varphi \cdot e \cdot r^{\mathrm{op}} = \varphi \cdot (r \cdot e) = r \cdot (\varphi \cdot e)$$

for all $r \in R$, $\varphi \in D$, $e \in E$. This then endows $\operatorname{Hom}_R(E, M) \otimes_D E$ with the structure of a right R^{op}-module via

$$(f \otimes e) \cdot r^{\mathrm{op}} = f \otimes (e \cdot r^{\mathrm{op}}) = f \otimes (re)$$

for all $r \in R$. The corresponding left R-module structure is then as claimed.

Definition 22.52. The right $\operatorname{End}_R(E)$-vector space $\operatorname{Hom}_R(E, M)$ is the *multiplicity space*[1] of M with respect to E.

Proposition 22.53. Let $D \coloneqq \operatorname{End}_R(E)$.

a) If $F \cong E$ then the multiplicity space $\operatorname{Hom}_R(E, F)$ is one-dimensional as a right D-vector space.

b) Let $M_E = \bigoplus_{i \in I} L_i$ be a decomposition into simple R-module, each of which (necessarily) isomorphic to E. For every $i \in I$ let $\tilde{f}_i \colon E \to L_i$ be an isomorphism of R-modules and let $f_i \colon E \to M$ be the extension of $\tilde{f}_i$ to a homomorphism $E \to M$. Then the family $(f_i)_{i \in I}$ is a right D-basis for $\operatorname{Hom}_R(E, M)$.

c) The evaluation map

$$\Phi \colon \operatorname{Hom}_R(E, M) \otimes_D E \to M_E, \quad f \otimes e \mapsto f(e)$$

is an isomorphism of R-modules.

Proof.

a) Any isomorphism of R-modulen $f \colon F \to E$ induces an isomorphism of right D-vector spaces

$$\operatorname{Hom}_R(E, F) \xrightarrow{f_*} \operatorname{Hom}_R(E, E) = D\,.$$

b) The inclusion $\iota \colon M_E \to M$ induces an isomorphism of right D-vector spaces

$$\operatorname{Hom}_R(E, M_E) \xrightarrow{\iota_*} \operatorname{Hom}_R(E, M)\,.$$

For every $i \in I$ let $\pi_i \colon M_E \to L_i$ be the projection along this decomposition and for every $f \in \operatorname{Hom}_R(E, M_E)$ let $f_i \coloneqq \pi_i \circ f$ be the i-th component of f. It follows from E being cyclic (and thus finitely generated) that the map

$$\operatorname{Hom}_R(E, M_E) = \operatorname{Hom}_R\left(E, \bigoplus_{i \in I} L_i\right) \xrightarrow{f \mapsto (f_i)_{i \in I}} \bigoplus_{i \in I} \operatorname{Hom}_R(E, L_i)$$

is an isomorphism of abelian groups (by Lemma A7.21). This is also an isomorphism of right D-vector spaces, so it follows altogether that

$$\operatorname{Hom}_R(E, M) \cong \operatorname{Hom}_R(E, M_E) = \operatorname{Hom}_R\left(E, \bigoplus_{i \in I} L_i\right) \cong \bigoplus_{i \in I} \operatorname{Hom}_R(E, L_i)$$

as right D-vector spaces. For every $i \in I$ the element $\tilde{f}_i \in \operatorname{Hom}_R(E, L_i)$ is a right D-basis by part a), and under the above isomorphism the resulting right D-basis $(\tilde{f}_i)_{i \in I}$ of $\bigoplus_{i \in I} \operatorname{Hom}_R(E, L_i)$ corresponds to the family $(f_i)_{i \in I}$ in $\operatorname{Hom}_R(E, M)$, which is therefore also a right D-basis.

[1] The author has taken this term from [Yua12] and does not know how common its usage is.

c) It follows that from part b) that

$$\operatorname{Hom}_R(E, M) \otimes_D E = \left(\bigoplus_{i \in I} f_i D \right) \otimes_D E = \bigoplus_{i \in I} (f_i D) \otimes_D E = \bigoplus_{i \in I} (f_i \otimes E) \,.$$

Observe that Φ maps the summand $f_i \otimes E$ onto the summand $f_i(E) = L_i$ and because f_i is an isomorphism it does so bijectively. (Here we use that D a skew field: The map $E \to \operatorname{Hom}_R(E, M) \otimes_D E$, $e \mapsto f_i \otimes e$ is injective because $\operatorname{Hom}_R(E, M)$ is free as a right D-module.) It follows that $\Phi\colon \bigoplus_{i \in I} (f_i \otimes_D E) \to \bigoplus_{i \in I} L_i$ is also bijective.

For all $r \in R$ and simple tensors $f \otimes e \in \operatorname{Hom}_R(E, M) \otimes_D E$ we have that

$$\Phi(r \cdot (f \otimes e)) = \Phi(f \otimes (re)) = f(re) = r f(e) = r \, \Phi(f \otimes e) \,,$$

which shows that Φ is an isomorphism of R-modules. □

Corollary 22.54. The $\operatorname{End}_R(E)$-dimension of $\operatorname{Hom}_R(E, M)$ is given by the multiplicity of E in M.

Corollary 22.55. If M is semisimple then the map

$$\bigoplus_{[E] \in \operatorname{Irr}(R)} \operatorname{Hom}_R(E, M) \otimes_{\operatorname{End}_R(E)} E \to M \,, \quad f \otimes e \mapsto f(e)$$

is an isomorphism of R-modules, where R acts on $\operatorname{Hom}_R(E, M) \otimes_{\operatorname{End}_R(E)} E$ via

$$r \cdot (f \otimes e) = f \otimes (re)$$

for all $r \in R$ and simple tensors $f \otimes e \in \operatorname{Hom}_R(E, M) \otimes_{\operatorname{End}_R(E)} E$.

23. Semisimple and Simple Rings

23.1. In this section we introduce and classify semisimple rings.

Conventions 23.2. In this section R denotes a ring.

Lemma 23.3. For every $n \geq 0$ the map

$$\mathrm{Z}(R) \to \mathrm{Z}(\mathrm{M}_n(R)) \,, \quad z \mapsto z I_n$$

is an isomorphism of rings.

Proof. The given map is a well-defined injective ring homomorphism and we need to show that it is surjective, i.e. that every $A \in \mathrm{Z}(\mathrm{M}_n(R))$ is of the form $A = z I_n$ for some $z \in \mathrm{Z}(R)$.

We have for all $i = 1, \dots, n$ that

$$i\text{-th column of } A = A e_i = A E_{ii} e_i = E_{ii} A e_i = \begin{bmatrix} 0 & \cdots & 0 & a_{ii} & 0 & \cdots & 0 \end{bmatrix}^T \,,$$

which shows that A is a diagonal matrix. We have for all $i, j = 1, \dots, n$ that

$$A_{ii} E_{ij} = A E_{ij} = E_{ij} A = A_{jj} E_{ij}$$

and therefore $A_{ii} = A_{jj}$. This shows that A is a scalar matrix, i.e. that $A = z I_n$ for some $z \in R$. We have for every $r \in R$ that

$$(rz) I_n = (r I_n)(z I_n) = (r I_n) A = A (r I_n) = (z I_n)(r I_n) = (z I_n) I_n \,,$$

which shows that $rz = zr$ for every $r \in R$ and therefore that $z \in \mathrm{Z}(R)$. □

23.1. Semisimple Rings & Artin–Wedderburn

Definition 23.4. The ring R is *semisimple* if it is semisimple as an R-module.

Example 23.5.

a) Fields and skew fields are semisimple.

b) Let be G be a finite group and let k a field.

   - If $\operatorname{char}(k) \nmid |G|$ then the group algebra $k[G]$ is semisimple by Maschke's theorem as seen in Example 22.17.
   - If $\operatorname{char}(k) \mid |G|$ then the group algebra $k[G]$ is not semisimple: The element

     $$x \coloneqq \sum_{g \in G} g \in k[G]$$

     is nonzero and G-invariant in the sense that $gx = x$ for every $g \in G$. It follows that kx is the submodule of $k[G]$ generated by x and that $ax' = x'$ for all $a \in k[G]$ and $x' \in kx$. If $k[G]$ were semisimple then kx would be a direct summand of $k[G]$ and there would exist a $k[G]$-linear projection $\pi \colon k[G] \to k[G]$ onto kx, for which we then have that $\pi(x) = x$. But follows for every $g \in G$ that

     $$\pi(g) = \pi(g \cdot 1) = g \cdot \underbrace{\pi(1)}_{\in x} = \pi(1)$$

     and therefore that

     $$x = \pi(x) = \sum_{g \in G} \pi(g) = |G| \pi(1) = 0$$

     which contradicts x being nonzero.

   Together this shows that the group algebra $k[G]$ is semisimple if and only if $\operatorname{char}(k) \nmid |G|$.

c) If R is a principal ideal domain which is not a field then R is not semisimple as it does not contain any simple submodule by Example 22.10.

d) For a skew field D the matrix ring $\mathrm{M}_n(D)$ is semisimple for all $n > 0$: We have seen in Example 22.4 that D^n is simple as an $\mathrm{M}_n(D)$-module. We now have that

$$\mathrm{M}_n(D) = C_1 \oplus \cdots \oplus C_n$$

for the submodules $C_i \leq \mathrm{M}_n(D)$ given by

$$C_i \coloneqq \{A \in \mathrm{M}_n(D) \mid A \text{ has nonzero entries only in the } i\text{-th column}\},$$

and we have that $C_i \cong D^n$ as $\mathrm{M}_n(D)$-modules for every $i = 1, \dots, n$.

Note that with respect to Corollary A5.9 this decomposition corresponds to the complete set of parwise orthogonal idempotents $E_{11}, \dots, E_{nn} \in \mathrm{M}_n(D)$. Indeed, we have for every $i = 1, \dots, n$ that $C_i = \mathrm{M}_n(D)E_{ii}$.

General Properties of Semisimple Rings

Proposition 23.6. The ring R is semisimple if and only if every R-module is semisimple.

Proof. If every R-module M is semisimple then this holds in particular for $M = R$. Every R-module is isomorphic to a quotient of a free R-moudule, so if R is semisimple then every R-module is semisimple by Lemma 22.18. □

Corollary 23.7. If R is semisimple and $I \trianglelefteq R$ is a two-sided ideal then the quotient ring R/I is again semisimple.

Proof. The (R/I)-submodules of R are precisely the R-submodules of R/I. It follows from the semisimplicity of R that R/I is a sum of simple R-submodules and thus a sum of simple (R/I)-submodules. □

Lemma 23.8. Let R be semisimple with $R = \bigoplus_{i \in I} L_i$ for simple submodules $L_i \leq R$. Then every simple R-module is isomorphic to some L_i.

Warning 23.9. If R is not semisimple then to every simple R-module must occur in R: For $R = \mathbb{Z}$ we have seen in Example 23.5 that up to isomorphism the only simple $\mathbb{Z}$-modules are $\mathbb{Z}/p$ for p prime, none of which is isomorphic to a submodule of $\mathbb{Z}$.

Proof. Let E be a simple R-module and let $x \in E$ with $x \neq 0$. Then the map $R \to E$, $r \mapsto rx$ is a nonzero homomorphism of R-modules and the claim follows from Corollary 22.24. □

Example 23.10. It follows from Lemma 23.8 and the decompositon of $\mathrm{M}_n(D)$ into simple submodules from Example 23.5 that D^n is the only simple $\mathrm{M}_n(D)$-module up to isomorphism

Lemma 23.11. Let R be semisimple with $R = \sum_{i \in I} L_i$ for submodules $L_i \leq R$. Then $R = \sum_{j \in J} L_j$ for some finite subset $J \subseteq I$.

Proof. We can decompose $1 \in R$ as $1 = \sum_{i \in I} e_i$ with $e_i \in L_i$ for every $i \in I$ and $e_i = 0$ for all but finitely many $i \in I$. For

$$J \coloneqq \{ i \in I \,|\, e_i \neq 0 \} \,.$$

the sum $\sum_{j \in J} L_j$ is a submodule of R, i.e. an ideal in R, which therefore contains 1. It follows that $\sum_{j \in J} L_j = R$. □

Corollary 23.12. If R is semisimple then R is a finite direct sum of simple submodules.

Proof. The claim follows by applying Lemma 23.11 to a decomposition into simple submodules. □

Corollary 23.13. If R is a semisimple then there exist only finitely many simple R modules up to isomorphism.

Proof. This follows from Corollary 23.12 and Lemma 23.8. □

Corollary 23.14. Every semisimple ring is both noetherian and artinian.

Proof. By using Corollary 23.13 we may write

$$R = L_1 \oplus \dots \oplus L_n$$

for some simple submodules $L_i \leq R$. It then follows that

$$0 \lneq L_1 \lneq L_1 \oplus L_2 \lneq \dots \lneq L_1 \oplus \dots \oplus L_n = R$$

is a composition series of R of length n. It follows from the Jordan-Hölder theorem that every strictly increasing (resp. strictly decreasing) sequence of submodules of R stabilizes after at most n steps (see Corollary A8.15). □

Example 23.15.

a) Let R be a nonzero ring. If I is an infinite ring then the ring $\mathrm{M}_I^{\mathrm{cf}}(R)$ of column finite $(I \times I)$-matrices is not semisimple: There exist a stricty increasing sequence of subsets

$$I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \dots \subsetneq I \,,$$

and for every $n \geq 0$ the set

$$J_n \coloneqq \{ A \in \mathrm{M}_I^{\mathrm{cf}}(R) \,|\, \text{the } i\text{-th column of } A \text{ is zero for all } i \in I_n \}$$

is a left ideal of $\mathrm{M}_I^{\mathrm{cf}}(R)$. The existence of the stricty decreasing sequence of left ideals

$$J_0 \supsetneq J_1 \supsetneq J_2 \supsetneq \cdots$$

shows that $\mathrm{M}_I^{\mathrm{cf}}(R)$ is not artinian.

b) If $(R_i)_{i \in I}$ is a family of rings with $R_i \neq 0$ for infinitely many $i \in I$ then the product $\prod_{i \in I} R_i$ is neither noetherian nor artinian and therefore not semisimple, even if every factor R_i is semisimple.

Products of Matrix Rings over Skew Fields

23.16. We start by taking a closer look at matrix rings over skew fields and how products of those kind of rings behave. For this we will need some understanding of how modules over a product $R_1 \times \cdots \times R_n$ of rings $R_1, \dots, R_n$ look like. An explanation of this can be found in appendix A6. We will also use some of the notation introduced there.

Proposition 23.17. Let R_1, R_2 be rings and let M_i be an R_i-module for $i = 1, 2$.

a) The $(R_1 \times R_2)$-module $M_1 \boxplus M_2$ is simple if and only if either (M_1 is a simple R_1-module and $M_2 = 0$) or ($M_1 = 0$ and M_2 is a simple R_2-module).

b) The map

$$\begin{aligned} \operatorname{Irr}(R_1) \amalg \operatorname{Irr}(R_2) &\longrightarrow \operatorname{Irr}(R_1 \times R_2)\,, \\ [E] &\mapsto \begin{cases} E \boxplus 0 & \text{if } [E] \in \operatorname{Irr}(R_1)\,, \\ 0 \boxplus E & \text{if } [E] \in \operatorname{Irr}(R_2) \end{cases} \end{aligned}$$

is a well-defined bijection.

c) The $(R_1 \times R_2)$-module $M_1 \boxplus M_2$ is semisimple if and only if M_i is semisimple as an R_i-module for both $i = 1, 2$.

d) The ring $R_1 \times R_2$ is semisimple if and only if both R_1 and R_2 are semisimple.

Proof.

a) Let $\mathcal{S}_i$ be the set of R_i-submodules of M_i for $i = 1, 2$ and let $\mathcal{S}$ be the set of $(R_1 \times R_2)$-submodules of $M_1 \boxplus M_2$. The map

$$\mathcal{S}_1 \times \mathcal{S}_2 \to \mathcal{S}, \quad (N_1, N_2) \mapsto N_1 \boxplus N_2$$

is a bijection by Proposition A6.25, from which it follows that

$$|\mathcal{S}| = |\mathcal{S}_1| \cdot |\mathcal{S}_2|\,.$$

The $(R_1 \times R_2)$-module $M_1 \boxplus M_2$ is simple if and only if $|\mathcal{S}| = 2$. This is the case if and only if either ($|\mathcal{S}_1| = 2$ and $|\mathcal{S}_2| = 1$) or ($|\mathcal{S}_1| = 1$ and $|\mathcal{S}_2| = 2$), which is equivalent to (M_1 simple and $M_2 = 0$), resp. ($M_1 = 0$ and M_2 simple).

b) This follows by restricting the bijection from Corollary A6.24 according to part a).

c) This can be seen in (at least) two ways:

- Every submodule $N \leq M_1 \boxplus M_2$ is of the form $N = N_1 \boxplus N_2$ for unique R_i-submodules $N_i \leq M_i$ by Proposition A6.25. It thus follows from Corollary A6.29 that every submodule of $M_1 \boxplus M_2$ is a direct summand if and only if for both $i = 1, 2$ every submodules of M_i is a direct summand.

- Suppose that M_1, M_2 are semisimple. Then $M_i = \bigoplus_{j \in J_i} L_1^j$ for simple submodules $L_i^j \leq M_i$. It then follows that

  $$M_1 \boxplus M_2 = \left(\bigoplus_{j \in J_1} L_1^j \right) \boxplus \left(\bigoplus_{j \in J_2} L_2^j \right) = \bigoplus_{j \in J_1} (L_1^j \boxplus 0) \oplus \bigoplus_{j \in J_2} (0 \boxplus L_2^j)$$

  is a decomposition into submodules which are simple by part a).

  Suppose now that $M_1 \boxplus M_2$ is semisimple. Then there exists a decomposition $M_1 \boxplus M_2 = \bigoplus_{j \in J} L^j$ into simple submodules $L^j \leq M_1 \boxplus M_2$. Every L^j is of the form $L^j = L_1^j \boxplus L_2^j$ for unique R_i-submodules $L_i^j \leq M_i$ by Proposition A6.25. It follows from part a) that J is the disjoint union of

  $$J_1 = \{ j \in J \mid L_2^j = 0 \} \quad \text{and} \quad J_2 = \{ j \in J \mid L_1^j = 0 \}$$

  and that L_i^j is simple for every $j \in L_i$. It thus follows that

  $$\begin{aligned} M_1 \boxplus M_2 &= \bigoplus_{j \in J} L^j = \bigoplus_{j \in J} (L_1^j \boxplus L_2^j) \\ &= \left(\bigoplus_{j \in J_1} (L_1^j \boxplus 0) \right) \oplus \left(\bigoplus_{j \in J_2} (0 \boxplus L_2^j) \right) \\ &= \left(\left(\bigoplus_{j \in J_1} L_1^j \right) \boxplus 0 \right) \oplus \left(0 \boxplus \left(\bigoplus_{j \in J_2} (0 \boxplus L_2^j) \right) \right) \\ &= \left(\bigoplus_{j \in J_1} L_1^j \right) \boxplus \left(\bigoplus_{j \in J_2} L_2^j \right) \end{aligned}$$

  and therefore that $M_i = \bigoplus_{j \in J_i} L_i^j$ is a direct sum of simple modules for both $i = 1, 2$.

d) We have that $R_1 \times R_2 = R_1 \boxplus R_2$ as $(R_1 \times R_2)$-modules. The claim therefore follows from part c). □

Remark 23.18. Lemma 23.17 does not hold for infinite products: Let $(R_i)_{i \in I}$ be a family of rings with $R_i \neq 0$ for infinitely many $i \in I$. Then $\bigoplus_{i \in I} R_i$ is a proper ideal in R and is thus (by Zorn's lemma) contained in a maximal left ideal I. The quotient $E \coloneqq R/I$ is then simple as an R-module but annihilated by every factor R_i.

Corollary 23.19. Let $D_1, \dots, D_r$ be skew fields and let $n_1, \dots, n_r \geq 1$.

a) The ring $R \coloneqq \mathrm{M}_{n_1}(D_1) \times \cdots \times \mathrm{M}_{n_r}(D_r)$ is semisimple.

b) The R-modules $S_1, \dots, S_r$ with

$$S_i \coloneqq 0 \boxplus \cdots \boxplus 0 \boxplus D_i^{n_i} \boxplus 0 \boxplus \cdots \boxplus 0$$

where $D_i^{n_i}$ is in the i-th position form a set of representatives of the isomorphism classes of simple R-modules.

c) We have that $R \cong \bigoplus_{i=1}^r S_i^{\oplus n_i}$ as R-modules.

23.20. We will also need the endomorphisms rings of the simple modules $S_1, \dots, S_r$ from Corollary 23.19. From now on we will need some knowledge about the opposite ring R^{op}, a brief introduction to which can be found in Appendix A4.

Lemma 23.21. Let D be a skew-field and let $n \geq 1$. Then the map

$$\Phi\colon D^{\mathrm{op}} \to \mathrm{End}_{\mathrm{M}_n(D)}(D^n)\,, \quad d^{\mathrm{op}} \mapsto (x \mapsto xd)$$

is an isomorphism of rings.

Proof. The column space D^n carries the structure of a right D-module via scalar multiplication from the right. This right D-module structure corresponds to a left D^{op}-modules structure (see Proposition A4.11), which in turn corresponds to a ring homomorphism $\Phi'\colon D^{\mathrm{op}} \to \mathrm{End}_{\mathbb{Z}}(D^n)$ as described above. For every matrix $A \in \mathrm{M}_n(D)$, vector $x \in D^n$ and scalar $d \in D$ we have that

$$A(xd) = Axd = (Ax)d\,,$$

which shows that Φ' restrict to a ring homomorphism $\Phi\colon D^{\mathrm{op}} \to \mathrm{End}_{\mathrm{M}_n(D)}(D^n)$ as desired.

It remains to show that Φ is bijective. For $d_1, d_2 \in D$ with $d_1 \neq d_2$ we have that

$$\Phi(d_1^{\mathrm{op}})(e_1) = e_1 d_1 \neq e_1 d_2 = \Phi(d_2^{\mathrm{op}})(e_1)\,,$$

which shows that Φ is injective. To see that Φ is surjective let $f \in \mathrm{End}_{\mathrm{M}_n(D)}(D^n)$. Let $A \in \mathrm{M}_n(D)$ be the matrix whose first column is e_1 and whose other columns are 0, so that

$$A = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}.$$

Then $Ae_1 = e_1$ and therefore

$$Af(e_1) = f(Ae_1) = f(e_1)\,,$$

which shows that $f(e_1)$ is of the form

$$f(e_1) = \begin{bmatrix} d \\ 0 \\ \vdots \\ 0 \end{bmatrix} = e_1 d$$

for some $d \in D$. For every $x \in D^n$ there exists some $A \in \mathrm{M}_n(D)$ with $Ae_1 = x$ (take x as the first column of A) and it follows that

$$f(x) = f(Ae_1) = Af(e_1) = Ae_1 d = xd\,.$$

This shows that $f(x) = xd$ for every $x \in D^n$, which shows that Φ is surjective. □

Remark 23.22. It follows more generally for every nonempty index set I in the same way as above that

$$\mathrm{End}_{\mathrm{M}_I^{\mathrm{cf}}(D)}(D^{\oplus I}) \cong D^{\mathrm{op}}$$

where we identify $D^{\oplus I}$ with the space of (column finite) column vectors $\mathrm{M}^{\mathrm{cf}}(I \times 1, D)$ and the action of $\mathrm{M}_I^{\mathrm{cf}}(D)$ on $D^{\oplus I} = \mathrm{M}^{\mathrm{cf}}(I \times 1, D)$ is given by matrix-vector multiplication.

One can also identify $D^{\oplus I}$ with the space of (row finite) row vectors $\mathrm{M}^{\mathrm{rf}}(1 \times I, D)$, which we denote by $(D^{\oplus I})^T$. Then $(D^{\oplus I})^T$ is a right $\mathrm{M}_I^{\mathrm{rf}}(D)$-module via vector-matrix multiplication. It can be shown in the same way as above that the endomorphism ring of this right module structure is given by D, with D acting on $(D^{\oplus I})^T$ by left multiplication. Since we are working mostly with left module structures we can replace this right $\mathrm{M}_I^{\mathrm{rf}}(D)$-module structure by the corresponding left $\mathrm{M}_I^{\mathrm{rf}}(D)^{\mathrm{op}}$-module structure and find that

$$\mathrm{End}_{\mathrm{M}_I^{\mathrm{rf}}(D)^{\mathrm{op}}}\left((D^{\oplus I})^T\right) \cong D\,.$$

Corollary 23.23. In the situation and notation of Corollary 23.19 we have that $\mathrm{End}_R(S_i) \cong D_i^{\mathrm{op}}$ for every $i = 1, \dots, r$.

Proof. We have that

$$\begin{aligned}
&\mathrm{End}_{\mathrm{M}_{n_1}(D_1)\times\cdots\times\mathrm{M}_{n_r}(D_r)}(S_i) \\
\cong\ &\mathrm{End}_{\mathrm{M}_{n_1}(D_1)}(0) \times \cdots \times \mathrm{End}_{\mathrm{M}_{n_i}(D_i)}(D^{n_i}) \times \cdots \times \mathrm{End}_{\mathrm{M}_{n_r}(D_r)}(0) \\
=\ &0 \times \cdots \times 0 \times \mathrm{End}_{\mathrm{M}_{n_i}(D_i)}(D^{n_i}) \times 0 \times \cdots \times 0 \\
\cong\ &\mathrm{End}_{\mathrm{M}_{n_i}(D_i)}(D^{n_i}) \\
\cong\ &D_i^{\mathrm{op}}
\end{aligned}$$

by Corollary A6.22. □

Notation 23.24. By abuse of notation we will often denote the simple modules $S_1, \dots, S_r$ from Corollary 23.19 by $D_1^{n_1}, \dots, D_r^{n_r}$. We then have that

$$\mathrm{End}_{\mathrm{M}_{n_1}(D_1)\times\cdots\times\mathrm{M}_{n_r}(D_r)}(D_i^{n_i}) \cong D_i^{\mathrm{op}}$$

by Corollary 23.23, with $d^{\mathrm{op}} \in D_i^{\mathrm{op}}$ acting on $D_i^{n_i}$ by right multiplication with d.

The Theorem of Artin–Wedderburn

Theorem 23.25 (Artin–Wedderburn)**.** Let R be semisimple.

a) If $R \cong E_1^{\oplus n_1} \oplus \cdots \oplus E_r^{\oplus n_r}$ for some $r \geq 0$, pairwise non-isomorphic simple R-modules $E_1, \dots, E_r$ and $n_1, \dots, n_r \geq 1$, then

$$R \cong \operatorname{End}_R(E_1^{\oplus n_1})^{\mathrm{op}} \times \cdots \times \operatorname{End}_R(E_r^{\oplus n_r})^{\mathrm{op}} \cong \mathrm{M}_{n_1}(D_1) \times \cdots \times \mathrm{M}_{n_r}(D_r)$$

as rings with $D_i = \operatorname{End}(E_i)^{\mathrm{op}}$ for every $i = 1, \dots, r$. If R is a k-algebra then this is an isomorphism of k-algebras.

b) This decomposition is unique in the following sense: If

$$R \cong \mathrm{M}_{m_1}(D'_1) \times \cdots \times \mathrm{M}_{m_s}(D'_s)$$

for any $s \geq 0$, $m_1, \dots, m_s \geq 1$ and skew fields $D'_1, \dots, D'_s$ then $r = s$ and the pairs $(D_1, n_1), \dots, (D_r, n_r)$ coincide with the pairs $(D'_1, m_1), \dots, (D'_s, m_s)$ up to permutation and isomorphism, i.e. there exists a bijection $\pi \colon \{1, \dots, r\} \to \{1, \dots, s\}$ such that $m_{\pi(i)} = n_i$ and $D'_{\pi(i)} \cong D_i$ for every $i = 1, \dots, r$.

Proof.

a) It follows from Lemma A4.10 and Corollary 22.25 that

$$\begin{aligned} R^{\mathrm{op}} \cong \operatorname{End}_R(R) &\cong \operatorname{End}_R(E_1^{\oplus n_1} \oplus \cdots \oplus E_r^{\oplus n_r}) \\ &\cong \operatorname{End}_R(E_1^{\oplus n_1}) \times \cdots \times \operatorname{End}_R(E_r^{\oplus n_r}) \\ &\cong \mathrm{M}_{n_1}(D_1) \times \cdots \times \mathrm{M}_{n_r}(D_r) \,. \end{aligned}$$

It further follows from Remark A4.4 and Lemma A4.8 that

$$\begin{aligned} R = (R^{\mathrm{op}})^{\mathrm{op}} &\cong (\mathrm{M}_{n_1}(D_1) \times \cdots \times \mathrm{M}_{n_r}(D_r))^{\mathrm{op}} \\ &= \mathrm{M}_{n_1}(D_1)^{\mathrm{op}} \times \cdots \times \mathrm{M}_{n_r}(D_r)^{\mathrm{op}} \\ &\cong \mathrm{M}_{n_1}(D_1^{\mathrm{op}}) \times \cdots \times \mathrm{M}_{n_r}(D_r^{\mathrm{op}}) \,. \end{aligned}$$

b) Let $\varphi \colon R \to \mathrm{M}_{m_1}(D'_1) \times \cdots \times \mathrm{M}_{m_s}(D'_s) \coloneqq R'$ be an isomorphism of rings. By using Corollary 23.19 (and the Notation of 23.24) we have that

$$R' \cong {D'_1}^{\oplus m_1} \oplus \cdots \oplus {D'_s}^{\oplus m_s}$$

as R'-modules. For every $i = 1, \dots, r$ we can pull back the R'-module structure of ${D'_i}^{\oplus m_i}$ to an R-module structure. The ${D'_i}^{\oplus m_i}$ thus become simple pairwise non-isomorpic R-modules with

$$R \cong {D'_i}^{\oplus m_i} \oplus \cdots \oplus {D'_i}^{\oplus m_i}$$

as R-modules.

By using the uniqueness of multiplicities of simple summands (see Theorem 22.47 and Remark 22.48) it follows that the two decompositions

$$R = E_1^{\oplus n_1} \oplus \cdots \oplus E_r^{\oplus n_r} \cong D_1'^{\oplus m_1} \oplus \cdots \oplus D_1'^{\oplus m_1}$$

into simple submodules coincide up to permutation and isomorphism: We have that $r = s$ and there exists a bijection $\pi\colon \{1, \dots, r\} \to \{1, \dots, s\}$ such that $m_{\pi(i)} = n_i$ for every $i = 1, \dots, r$ and $D'_{\pi(i)} \cong E_i$ as R-modules for every $i = 1, \dots, r$. We also find that

$$D_i = \operatorname{End}_R(E_i)^{\mathrm{op}} \cong \operatorname{End}_R(D_i'^{\oplus m_i})^{\mathrm{op}} = \operatorname{End}_{R'}(D_i'^{\oplus m_i})^{\mathrm{op}} \cong ((D_i')^{\mathrm{op}})^{\mathrm{op}} = D_i'$$

as rings. This finishes the proof. □

Remark 23.26. Corollary 23.19 and the theorem of Artin–Wedderburn together give a classification of semisimple rings up to isomorphism: Semisimple rings are precisely the products of matrix rings over skew fields.

Corollary 23.27. If R is semisimple then R^{op} is also semisimple.

Proof. By the theorem of Artin–Wedderburn we have that

$$R \cong \mathrm{M}_{n_1}(D_1) \times \cdots \times \mathrm{M}_{n_r}(D_r)$$

as rings for some $r \geq 0$, $n_1, \dots, n_r \geq 1$ and skew fields $D_1, \dots, D_r$. It follows that

$$\begin{aligned} R^{\mathrm{op}} &\cong (\mathrm{M}_{n_1}(D_1) \times \cdots \times \mathrm{M}_{n_r}(D_r))^{\mathrm{op}} \\ &= \mathrm{M}_{n_1}(D_1)^{\mathrm{op}} \times \cdots \times \mathrm{M}_{n_r}(D_r)^{\mathrm{op}} \\ &= \mathrm{M}_{n_1}(D_1^{\mathrm{op}}) \times \cdots \times \mathrm{M}_{n_r}(D_r^{\mathrm{op}}) \,. \end{aligned}$$

The rings D_i^{op} are skew fields because the D_i are skew fields, so it follows from Corollary 23.19 that R^{op} is semisimple. □

Definition 23.28. An R-module M is *faithful* if for all $r_1, r_2 \in R$ with $r_1 \neq r_2$ there exists some $m \in M$ with $r_1 m \neq r_2 m$.

Example 23.29. The R-module R is faithful because we can choose $m = 1$.

Recall 23.30. For an R-module M the following conditions are equivalent:

a) The module M is faithful.

b) For every $r \in R$ with $r \neq 0$ there exists some $m \in M$ with $rm \neq 0$.

c) The corresponding ring homomorphism $R \to \operatorname{End}_{\mathbb{Z}}(M)$ is injective.

d) The annihilator $\operatorname{Ann}_R(M) = \{r \in R \mid rm = 0\}$ is 0.

Corollary 23.31. If R is semisimple and M is a faithful R-module then the isotypical components of M are all nonzero, i.e. M contains every simple R-module up to isomorphism.

Proof. By the theorem of Artin–Wedderburn we may assume w.l.o.g. that

$$R = M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$$

for some $r \geq 0$, $n_1, \dots, n_r \geq 1$ and skew field $D_1, \dots, D_r$. Then $D_1^{n_1}, \dots, D_r^{n_r}$ form a set of representatives for the isomorphism classes of simple R-modules. For every $i = 1, \dots, r$ let M_i be the $D_i^{n_i}$-isotypical component of M.

The module M is semisimple because R is semisimple, so there exists a decomposition into isotypical components $M = \bigoplus_{i=1}^r M_i$. If $M_i = 0$ for some i then every element $A \in \mathrm{M}_{n_i}(D_i) \subseteq R$ would act by multiplication with zero on M, which would contradicts the faithfulness of M. The isotypical components M_i are therefore all nonzero. □

Warning 23.32. If R is semisimple then a faithful module does not have to contain a copy of every simple R-module: We have seen in Warning 23.9 that for $R = \mathbb{Z}$ the faithful $\mathbb{Z}$-module $M = \mathbb{Z}$ contains no simple submodules.

Remark 23.33. Let G be a finite group and let k be a field. We have seen in Example 23.5 that the groups algebra $k[G]$ is not semisimple if $\operatorname{char}(k) \mid |G|$. This also follows from the theorem of Artin–Wedderburn:

If $k[G]$ were semisimple then

$$k[G] \cong \mathrm{M}_{n_1}(D_1) \times \cdots \times \mathrm{M}_{n_r}(D_r)$$

for some $r \geq 1$, $n_1, \dots, n_r \geq 1$ and skew fields $D_1, \dots, D_r$. The element $x := \sum_{g \in G} g$ is central in $k[G]$ in because $gx = x = xg$ for all $g \in G$ and it is nilpotent because $x^2 = |G| x = 0$. The center of $k[G]$ is given by

$$\begin{aligned} \mathrm{Z}(k[G]) &\cong \mathrm{Z}\left(\mathrm{M}_{n_1}(D_1) \times \cdots \times \mathrm{M}_{n_r}(D_r)\right) \\ &= \mathrm{Z}(\mathrm{M}_{n_1}(D_1)) \times \cdots \times \mathrm{Z}(\mathrm{M}_{n_r}(D_r)) \\ &\cong \mathrm{Z}(D_1) \times \cdots \times \mathrm{Z}(D_r) \end{aligned}$$

where the second isomorphism follows from Lemma 23.3. The rings $\mathrm{Z}(D_i)$ are fields because the D_i are skew fields. This shows that $\mathrm{Z}(k[G])$ is isomorphic to a product of fields. But x is a nonzero nilpotent element of $\mathrm{Z}(k[G])$, which is absurd.

23.2. Simple Rings & Weddeburn

Definition 23.34. The ring R is simple if it is nonzero and $0, R$ are the only two-sided ideals of R, i.e. if R contains precisely two two-sided ideals.

Example 23.35. If D is a division ring and $n \geq 1$ then $M_n(D)$ is simple. This follows from the following lemma:

Lemma 23.36. For every $n \geq 1$ the map

$$\begin{aligned} \{\text{two-sided ideals } I \trianglelefteq R\} &\longrightarrow \{\text{two-sided ideals } J \trianglelefteq \mathrm{M}_n(R)\}, \\ I &\longmapsto \mathrm{M}_n(I) \end{aligned}$$

is a well-defined bijection.

Proof. If $I \trianglelefteq R$ is a two-sided ideal then the canonical projection $\pi\colon R \to R/I$ is a ring homomorphism. The induced ring homomorphism $\mathrm{M}_n(R) \to \mathrm{M}_n(R/I)$ has $\mathrm{M}_n(I)$ as its kernel, which is therefore a two-sided ideal in $\mathrm{M}_n(R)$.

Let on the other hand $J \trianglelefteq \mathrm{M}_n(R)$ be a two-sided ideal. For all $i, j = 1, \dots, n$ let

$$I_{ij} = \{r \in R \,|\, \text{there exists a matrix } A \in J \text{ whose } ij\text{-th coefficient is } r\}\,.$$

Then I_{ij} is a two-sided ideal in R: The projection $\pi_{ij}\colon \mathrm{M}_n(R) \to R$ onto the ij-th coefficient is a homomorphism of both left and right R-modules and the two-sided ideal J is both a left and right R-submodule of $\mathrm{M}_n(R)$. It follows that $\pi_{ij}(J)$ is both a left and right R-submodule of R, i.e. a two-sided ideal.

By multiplying a matrix $A \in J$ with permutation matrices from the left and from the right we can move every coefficient of A to every other position without leaving J. It follows that the ideal $I \coloneqq I_{ij}$ does not depend on the position i, j, and we have have that $J = \mathrm{M}_n(I)$ by construction of I. □

Warning 23.37. A simple ring R is not necessarily simple as an R-module: The ring $\mathrm{M}_n(D)$ for a skew field D and $n \geq 2$ is a counterexample.

Warning 23.38. Not every simple ring is semisimple, despite its name:

Example 23.39. Let $\operatorname{char}(k) = 0$. The (first) Weyl algebra $\mathcal{A} = \mathcal{A}_1$ from subsection 6.3 is simple but not semisimple:

To show that $\mathcal{A}$ is not semisimple it sufficies by Corollary 23.14 to observe that $\mathcal{A}$ is not artinian: We have seen that $\mathcal{A}$ has a basis given by $X^n \partial^m$ with $n, m \geq 0$. It then follows for every $i \geq 0$ that

$$\mathcal{A}\,\partial^i = \left\langle X^n \partial^{m+i} \,\middle|\, n, m \geq 0 \right\rangle_k = \langle X^n \partial^m \,|\, n \geq 0, m \geq i \rangle_k \;,$$

which shows that

$$\mathcal{A} = \mathcal{A}\,\partial^0 \gneq \mathcal{A}\,\partial^1 \gneq \mathcal{A}\,\partial^2 \gneq \cdots$$

is a strictly decreasing sequence of left ideals of $\mathcal{A}$.

To show that $\mathcal{A}$ is simple let $I \trianglelefteq \mathcal{A}$ be a two-sided ideal and let $f \in I$ be non-zero. We can then write f uniquely as

$$f = \sum_{m \geq 0} p_m \partial^m$$

with $p_m \in k[X] \subseteq \mathcal{A}$ for all $m \geq 0$. It follows from $\partial X = X\partial + 1$ by induction that

$$\partial^n X = X \partial^n + n \partial^{n-1}$$

for all $n \geq 0$. It follows that

$$\begin{aligned} fX - Xf &= \sum_{m \geq 0} (p_m \partial^m X - X p_m \partial^m) \\ &= \sum_{m \geq 0} \left(p_m X \partial^m + m p_m \partial^{m-1} - p_m X \partial^m\right) = \sum_{m \geq 0} m p_m \partial^{m-1}\,. \end{aligned}$$

For the maximal index $m \geq 0$ with $p_m \neq 0$ it follows that $m! p_m \in I$ and therefore that

$$p_m \in I\,.$$

This shows that I already contains a non-zero polynomial from $k[X] \subseteq \mathcal{A}$. We have seen in subsection 6.3 (namely Equation (6.3)) that the formula $\partial X = X\partial + 1$ generalizes to

$$\partial p = p\partial + p'$$

for all $p \in k[X] \subseteq \mathcal{A}$, where p' denotes the (formal) derivative of p. We thus have that

$$\partial p - p\partial = p'$$

for all $p \in k[X]$. It follows for $d := \deg_X(p_m)$ that $p^{(d)} \in I$ is a non-zero constant polynomial (because $\operatorname{char}(k) \neq 0$). This shows that I contains a unit, which shows that $I = \mathcal{A}$.

Remark 23.40. We have given in Remark 6.30 a short overview how the Weyl algebra $\mathcal{A}$ can be understood as a skew polyonmial ring over the ground ring $k[X]$ with respect to the k-derivation $\partial\colon k[X] \to k[X]$.

It can be shown more generally that for a field of characteristic $\operatorname{char}(k) = 0$ and a k-algebra A a skew polynomial ring $A[y;\delta]$ (with respect to a k-derivation $\delta\colon A \to A$) is simple if and only if A is *δ-simple* and δ is not an *inner derivation*; proofs of this can be found in [Lam91, Theorem 3.15] and [GW04, Proposition 2.1] (where definitions of the above terms can also be found). If $\operatorname{char}(k) = 0$ then it also holds for every simple k-algebra A and every non-inner derivation $\delta\colon A \to A$ that the skew polynomial ring $A[y;\delta]$ is a nonartinian simple ring; a proof of this can be found in [Lam91, Corollary 3.16].

This gives a recipe for constructing simple rings which are not semisimple.

Example 23.41. The following example is taken from [Lam91, 3.14]: Let V be a countable infinite-dimensional k-vector space for some (skew) field k. Then

$$I := \{f \in \operatorname{End}(V) \mid f \text{ has finite rank}\}$$

is a two-sided ideal because we have for all $g \in \operatorname{End}(V)$ and $f, f_1, f_2 \in I$ that

$$\operatorname{rank}(f \circ g), \operatorname{rank}(g \circ f) \leq \operatorname{rank}(f)$$

and

$$\operatorname{rank}(f_1 + f_2) \leq \operatorname{rank}(f_1) + \operatorname{rank}(f_2)\,.$$

The two-sided ideal I is already maxmimal:

Suppose that $f \in \operatorname{End}(V)$ has infinite rank. Let C_1 be a direct complement of $\operatorname{im}(f)$ and let C_2 be a direct complement of $\ker(f)$. Then $\operatorname{im}(f)$ is countable infinite-dimensional, so there exists an endomorphism $g_1\colon V \to V$ such that the restriction $g_1|_{\operatorname{im}(f)} \to V$ is an isomorphism. The endomorphism f restricts to an isomorphism $C_2 \to \operatorname{im}(f)$, so C_2 is also countable infinite-dimensional. It follows that there exists an endomorphism $g_2\colon V \to V$ which restricts to an isomorphism $V \to C_2$. The composition $g_1 \circ f \circ g_2\colon V \to V$ is then an isomorphism. This shows that the two-sided ideal generated by f is already $\mathrm{End}(V)$ itself.

It follows from the maximality of I that $\mathrm{End}(V)/I$ is simple. We now show that $\mathrm{End}(V)/I$ is not noetherian, from which it follows by Corollary 23.14 that $\mathrm{End}(V)/I$ is not semisimple.

We choose a basis $(b_{i,j})_{i,j \geq 0}$ of V, and for every $n \geq 0$ we consider the left ideal of $\mathrm{End}(V)$ given by

$$J_n \coloneqq \{f \in \mathrm{End}(V) \mid f(b_{ij}) = 0 \text{ for all } i \geq n,\, j \geq 0\}\,.$$

We then have that $J_n \subsetneq J_{n+1}$ for all $n \geq 0$.

Claim. For all $n \geq 0$ we have that $I + J_n \subsetneq I + J_{n+1}$.

Proof. It sufficies to show that $J_{n+1} \not\subseteq I + J_n$: Consider an element $f \in J_{n+1}$ with

$$f(b_{n+1,j}) = b_{n+1,j}$$

for all $j \geq 0$. If $f \in I + J_n$ then there would exist $g \in I$, $f' \in J_n$ with $f = g + f'$. It then follows that

$$b_{n+1,j} = f(b_{n+1,j}) = g(b_{n+1,j}) + f'(b_{n+1,j}) = g(b_{n+1,j})$$

for all $j \geq 0$, and therefore that

$$g(b_{n+1,j}) = -b_{n+1,j}$$

for all $j \geq 0$. But this contradicts g having finite rank. □

It follows that

$$I = I + J_0 \subsetneq I + J_1 \subsetneq I + J_2 \subsetneq \cdots$$

is a strictly increasing sequence of ideals in $\mathrm{End}(V)$ and it follows that

$$0 = (I + J_0)/I \subsetneq (I + J_1)/I \subsetneq (I + J_2)/I \subsetneq \cdots$$

is a strictly increasing sequence of ideals in $\mathrm{End}(V)/I$. This shows that $\mathrm{End}(V)/I$ is not noetherian.

Lemma 23.42. If E is a simple R-module then the isotypical component R_E is a two-sided ideal of R.

Proof. The isotypical component R_E is a submodule of R and therefore a left ideal. For every $r \in R$ the map $R \to R$, $x \mapsto xr$ is a homomorphism of R-modules and therefore maps R_E into R_E by Lemma 22.43. This shows that R_E is also a right ideal. □

Theorem 23.43 (Wedderburn)**.** The following conditions are equivalent:

a) The ring R is simple and (left) artinian.

b) The ring R is simple and contains a minimal nonzero left ideal $I \trianglelefteq R$.

c) The ring R is both simple and semisimple.

d) The ring R is semisimple and has only one simple module up to isomorphism.

e) We have that $R \cong \mathrm{M}_n(D)$ for some $n \geq 1$ and skew field D.

The skew field D is then up to isomorphism uniquely determined as $D \cong \mathrm{End}_R(I)^{\mathrm{op}}$, with I as above being the unique simple R-module up to isomorphism. The number n is uniquely determined as the multiplicity of I in R.

Proof.

a) $\implies$ b) The set of nonzero left ideals of R is non-empty because $R \neq 0$ and thus contains a minimal element because R is artinian.

b) $\implies$ c) The ideal I is a simple R-module and the I-isotypical component R_I is a nonzero two-sided ideal by Lemma 23.42. It follows from R being simple that $R_I = R$, and therefore that R is semisimple.

c) $\implies$ d) Because $R \neq 0$ is a sum of simple R-modules it follows that there exists a simple R-module E. The E-isotypical component R_E is a two-sided ideal by Lemma 23.42 which is nonzero by Lemma 23.8. It follows that $R_E = R$, and therefore from Lemma 23.8 that E is the unique simple R-module up to isomorphism.

d) $\implies$ e) This follows from the theorem of Artin–Wedderburn.

e) $\implies$ c) That $\mathrm{M}_n(D)$ is simple follows from Example 23.35, and that R is semisimple follows from Example 23.5.

c) $\implies$ a) This follows from Corollary 23.14.

The minimal ideal I is a simple submodule of R, and thus the unique simple R-module up to isomorphism . Because D^n is a simple $\mathrm{M}_n(D)$-module, so it follows that

$$D^{\mathrm{op}} \cong \mathrm{End}_{\mathrm{M}_n(D)}(D^n) \cong \mathrm{End}_R(I)\,,$$

and therefore that $D \cong \mathrm{End}_R(I)^{\mathrm{op}}$. The multiplicity of I in R is the same as the multiplicity of D^n in $\mathrm{M}_n(D)$, which is n. □

23.3. Alternative Approach

23.44. We will now show another approach to the theorems of Artin–Wedderburn and Wedderburn which illuminates the role that simple ring play in the theory.

We have seen in Lemma 23.42 that the isotypical components of a ring R are two-sided ideals. We will begin by strengthening this result:

Lemma 23.45 ([FD93, Lemma 1.14])**.** Let M be an R-module.

a) For every simple R-module E the E-isotypical component M_E is $\operatorname{End}_R(M)$-invariant, i.e. we have that $f(M_E) \subseteq M_E$ for every $f \in \operatorname{End}_R(M)$.

b) If M is semisimple and $N \leq M$ is an R-submodule which is $\operatorname{End}_R(M)$-invariant then N is a sum of isotypical components of M, i.e. there exists some subset $\mathcal{S} \subseteq \operatorname{Irr}(R)$ with $N = \bigoplus_{[E] \in \mathcal{S}} M_E$.

Proof.

a) This follows from Lemma 22.43.

b) We have that $M = \bigoplus_{[E] \in \operatorname{Irr}(R)} M_E$ and $N = \bigoplus_{[E] \in \operatorname{Irr}(R)} N_E$, so we need to show that for every $E \in \operatorname{Irr}(R)$ with $N_E \neq 0$ we already have that $N_E = M_E$.

Note that $N_E = N \cap M_E$ is $\operatorname{End}_R(M)$-invariant and therefore also $\operatorname{End}_R(M_E)$-invariant because every R-module endomorphism of M_E extends to an endomorphism of M by Corollary 22.44. It therefore sufficies to consider the case that $M = M_E$ for some $E \in \operatorname{Irr}(R)$, i.e. that M is E-isotypical.

Then N is also E-isotypical and it follows from $N \neq 0$ that there exists a submodule $L \leq N$ with $L \cong E$. If $L' \leq M$ is any submodule with $L' \cong E$ then $L \cong L'$ and every isomorphism $f \colon L \to L'$ extends to an R-module endomorphism $g \colon M \to M$: We may choose direct complements C, C' of L, L' because M is semisimple and define g by

$$g \colon M = L \oplus C \xrightarrow{\begin{bmatrix} f & 0 \\ 0 & 0 \end{bmatrix}} L' \oplus C' = M \,,$$

i.e. g is given by the composition

$$g \colon M = L \oplus C \twoheadrightarrow L \xrightarrow{f} L' \hookrightarrow L' \oplus C' = M \,.$$

It follows that

$$L' = f(L) = g(L) \leq N$$

because N is $\operatorname{End}_R(M)$-invariant. This shows that

$$M = M_E = \sum_{\substack{L' \leq M \\ L' \cong E}} L' \leq N \,,$$

which shows that $M = N$. □

Corollary 23.46.

a) For every simple R-module E the E-isotypical component R_E is a two-sided ideal of R.

b) If R is semisimple and $E_1, \dots, E_n$ is a set of representatives for the isomorphism classes of simple R-modules (this set is finite by Corollary 23.13) then the E_i-isotypical components R_{E_i} are minimal two-sided ideals of R, and every two-sided ideal of R is a sum of isotypical components.

Proof. The two-sided ideal of R are precisely those left ideals which are also invariant under right multiplication with elements of R. By using the isomorphism $R^{\mathrm{op}} \cong \mathrm{End}_R(R)$, $r^{\mathrm{op}} \mapsto (x \mapsto xr)$ from Lemma A4.10 we find that for any left ideal, invariance under right multiplication is the same as $\mathrm{End}_R(R)$-invariance. The two-sided ideals of R are therefore precisely those left ideals which are $\mathrm{End}_R(R)$-invariant.

With this observation the claims follow from Lemma 23.45. □

Corollary 23.47. If R is semisimple then R contains only finitely many two-sided ideals, namely 2^n many where $n = |\mathrm{Irr}(R)|$.

Remark 23.48. Corollary 23.47 also follows from the theorem of Artin–Wedderburn: We may assume that the semisimple ring R is given by $R = \mathrm{M}_{n_1}(D_1) \times \cdots \times \mathrm{M}_{n_r}(D_r)$ with $r \geq 0$, $n_1, \dots, n_r \geq 1$ and skew fields $D_1, \dots, D_r$. Then every two-sided ideal $I \trianglelefteq R$ is of the form $I = I_1 \times \cdots \times I_r$ for unique two-sided ideals $I_j \trianglelefteq \mathrm{M}_{n_j}(D_j)$ by Remark A6.27. It follows for every $j = 1, \dots, r$ that either $I_j = 0$ or $I_j = \mathrm{M}_{n_j}(D_j)$ because the matrix rings $\mathrm{M}_{n_j}(D_j)$ are simple. It thus follows that R contains precisely 2^r two-sided ideals, with $r = |\mathrm{Irr}(R)|$.

23.49. If R is semisimple then by Corollary 23.13 there exist only finitely many simple R-modules $E_1, \dots, E_r$ up to isomorphism. The isotypical decomposition then reads

$$R = R_{E_1} \oplus \cdots \oplus R_{E_r}$$

and each R_{E_i} is a non-trivial two-sided ideal by Lemma 23.8 and Corollary 23.46.

Each R_{E_i} is then itself a ring with respect to the addition and multiplication inherited from R and the map

$$R_{E_1} \times \cdots \times R_{E_r} \to R, \quad (r_1, \dots, r_n) \mapsto r_1 + \cdots + r_n$$

is an isomorphism of rings, as explained in Proposition A5.16. Each R_{E_i} is itself semisimple by Proposition 23.17 with E_i being its only simple module up to isomorphism. The rings R_{E_i} are simple, as can be seen in two ways:

- Every R_{E_i} is a minimal two-sided ideal of R, so it cannot contain any nonzero proper ideals.
- Because R_{E_i} is semisimple and has precisely one isomorphism class of simple modules it follows from Corollary 23.46 that R_{E_i} is the unique nonzero two-sided ideal of R_{E_i}.

We have thus shown that every semisimple ring has a canonical decomposition into a direct product of rings, each of which is simple and semisimple with only one isomorphism class of simple modules. We would now like to rewoke Wedderburn's theorem to conclude that each factor R_{E_i} is already of the form $R_{E_i} \cong \mathrm{M}_{n_i}(D_i)$ for some $n_i \geq 1$ and skew field D_i.

But in the above proof of Wedderburn's theorem we actually used the theorem of Artin–Wedderburn, which are trying to avoid. However, by taking a careful look at the given proof of Wedderburn's theorem we see that we only used the theorem of

Artin–Wedderburn for one of the implications. We will therefore now give another proof of Wedderburn's theorem which does not rely on the theorem of Artin–Wedderburn. The main tool is the following observation due to [Rie65].

Lemma 23.50 (Rieffel's Theorem)**.** Let $I \trianglelefteq R$ be a left ideal. Then I is a left D-module for $D \coloneqq \operatorname{End}_R(I)$ via

$$\varphi \cdot x = \varphi(x)$$

for all $\varphi \in D$, $x \in I$ and the map

$$\Phi \colon R \to \operatorname{End}_D(I)\,, \quad r \mapsto (x \mapsto rx)$$

is a well-defined ring homomorphism. If R is simple and I is nonzero then Φ is an isomorphism.

Proof. That I is a left D-module follows by direct calculation. The R-module structure of I corresponds to a ring homomorphism $\Phi' \colon R \to \operatorname{End}_{\mathbb{Z}}(I)$, $r \mapsto (x \mapsto rx)$, which restrict to the desired ring homomorphism Φ because the actions of R and D on I commute (by definition of D).

It follows from $I \neq 0$ that $D \neq 0$ and therefore that $\Phi \neq 0$. The kernel $\ker(\Phi)$ is therefore a proper two-sided ideal of R, and must be trivial by the simplicity of R. This shows that Φ is injective.

The key observation behind the surjectivity of Φ is that $\Phi(I)$ is a left-ideal in $\operatorname{End}_D(I)$: Let $f \in \operatorname{End}_D(I)$ and $x \in I$. For every $y \in I$ the map $\rho_y \colon I \to I$, $x' \mapsto x'y$ is a homomorphism of R-modules, i.e. an element of D, and thus commutes with f. It follows for every $y \in I$ that

$$(f\Phi(x))(y) = f(\Phi(x)(y)) = f(xy) = f(\rho_y(x)) = \rho_y(f(x)) = f(x)y = \Phi(f(x))(y)\,,$$

showing that $f\Phi(x) = \Phi(f(x)) \in \Phi(I)$.

It follows that $\Phi(R)$ is a left ideal in $\operatorname{End}_D(I)$: It follows from IR being a nonzero two-sided ideal of R that $R = IR$ by the simplicity of R. It follows that $\Phi(R) = \Phi(I)\Phi(R)$, and because $\Phi(I)$ is a left ideal in $\operatorname{End}_D(R)$ it further follows that

$$\operatorname{End}_D(I)\Phi(R) = \operatorname{End}_D(I)\Phi(I)\Phi(R) \subseteq \Phi(I)\Phi(R) = \Phi(R)\,.$$

Because the left ideal $\Phi(R)$ contains $1 = \Phi(1)$ it follows that $\Phi(R) = \operatorname{End}_D(I)$, showing the surjecitvity of R. □

Alternative proof of Wedderburn's theorem.

a) $\implies$ b) As in the first proof.

b) $\implies$ e) It follows from Lemma 23.50 that $R \cong \operatorname{End}_D(I)$ for $D \coloneqq \operatorname{End}_R(I)$. It follows from I being simple as an R-module that D is a skew field. If I were not finite-dimensional as a D-vector space then it would follow as in Example 23.41 that

$$\{f \in \operatorname{End}_D(I) \mid f \text{ has finite rank}\}$$

is a nonzero proper two-ideal in $\operatorname{End}_D(I)$, which would contradict R being simple. We thus find that I is finite-dimensional as a D-vector space. Let $n := \dim_D(I)$. By linear algebra we find that $I \cong D^n$ as D-vector spaces; contrary to our usual convention we will regard D^n as the space of *row* vectors of width n. It then follows from linear algebra that every D-endomorphism $f \colon D^n \to D^n$ is given by right multiplication with a matrix $A \in \mathrm{M}_n(D)$, resulting in an isomorphism of rings $\operatorname{End}_D(D^n) \cong \mathrm{M}_n(D)^{\mathrm{op}}$. It follows that

$$R \cong \operatorname{End}_D(I) \cong \operatorname{End}_D(D^n) \cong \mathrm{M}_n(D)^{\mathrm{op}} \cong \mathrm{M}_n(D^{\mathrm{op}})$$

with D^{op} being a skew field.

e) $\implies$ c) We know that $\mathrm{M}_n(D)$ is both simple and semisimple.

c) $\implies$ d) As in the first proof.

d) $\implies$ a) Every semisimple ring is artinian by Corollary 23.14, and if R has only a single isomorphism class of simple modules then it follows from Corollary 23.46 that R is simple.

The uniqueness of D up to isomorphism and the uniqueness of n can be shown as in the first proof. □

23.51. We now have an alternative proof for the existence of an Artin–Wedderburn decomposition of a semisimple ring R: We first decompose R as

$$R = R_{E_1} \times \cdots \times R_{E_n}$$

where $E_1, \dots, E_n$ is a set of representatives for the isomorphism classes of simple R-modules. This is a decomposition into two-sided ideals, and therefore a decomposition of R into a direct products of rings $R_{E_1}, \dots, R_{E_n}$. Each factor R_{E_i} is then a ring which is both simple and semisimple. By Wedderburn's theorem each factor R_{E_i} isomorphic to a matrix ring $R_{E_i} \cong \mathrm{M}_{n_i}(D_i)$ where n_i is the multiplicity of E_i in R_{E_i}, which is the same as the multiplicity of E_i in R, and $D_i = \operatorname{End}_{R_{E_i}}(E_i)^{\mathrm{op}} = \operatorname{End}_R(E_i)^{\mathrm{op}}$ is a skew field.

We can also give an alternative proof of the uniqueness of the Artin–Wedderburn decomposition (up to isomorphism):

Lemma 23.52. Let $R = I_1 \oplus \cdots \oplus I_n = J_1 \oplus \cdots \oplus J_m$ be two decompositions into minimal two-sided ideals. Then both decompositions coincide up to permutation of the summands.

First proof ([Lam91, Lemma 3.8]). Each I_i inherits the structure of a ring from R by Proposition A5.16, and R is the internal direct product of the rings $I_1, \dots, I_n$ in the sense of Definition A5.17. It follows from Remark A6.27 that every two-sided ideal $K \trianglelefteq R$ is of the form

$$K = K_1 \oplus \cdots \oplus K_n$$

for unique two-sided ideals $K_i \trianglelefteq I_i$, and the component K_i can be described as $K_i = K \cap I_i$. We thus find for all $j = 1, \dots, m$ that

$$J_j = (J_j \cap I_1) \oplus \cdots \oplus (J_j \cap I_n) \,.$$

The intersections $J_j \cap I_i$ are again two-sided ideals. It therefore follows from the minimality of J_j that there exists a unique index $1 \leq \tau(j) \leq n$ with $J_j = J_j \cap I_{\tau(j)}$, which can be rephrased as $J_j \subseteq I_{\tau(j)}$. (For $k = 1, \dots, n$ with $k \neq j$ we have that $J_j \cap I_k = 0$.)

We find in the same way that there exists for every $i = 1, \dots, n$ some $1 \leq \sigma(i) \leq m$ with $I_i \subseteq J_{\sigma(i)}$. It follows for every $i = 1, \dots, n$ that

$$I_i \subseteq J_{\sigma(i)} \subseteq I_{\tau(\sigma(i))} \,,$$

from which it follows that $\tau(\sigma(i)) = i$. It then also follows that $I_i = J_{\sigma(i)}$ for every $i = 1, \dots, n$. That $\sigma(\tau(j)) = j$ and $J_j = I_{\tau(j)}$ for all $j = 1, \dots, m$ follows in the same way.

This shows that the mappings σ, τ are mutually inverse bijections, which shows that $n = m$. We have also shown that both $I_1, \dots, I_n$ and $J_1, \dots, J_m = J_n$ agree up to permutation (namely σ, resp. τ). □

Second proof ([FD93, Theorem 1.13]). We have for all $j = 1, \dots, m$ that

$$J_j = RJ_j = \bigoplus_{i=1}^{n} I_i J_j$$

with the summands $I_i J_j$ being two-sided ideals which are contained in J_j. It follows from the minimality of J_j that there exists a unique index $1 \leq \tau(j) \leq n$ with $J_j = I_{\tau(i)} J_j$ and thus $J_j \subseteq I_{\tau(i)}$. We can now proceed as in the first proof. □

23.53. We can now prove the uniqueness part of the theorem of Artin–Wedderburn: Suppose that R is semisimple with $R \cong \mathrm{M}_{n_1}(D_1) \times \cdots \times \mathrm{M}_{n_r}(D_r)$ for some $r \geq 0$, $n_1, \dots, n_r \geq 1$ and skew fields D_i. Then the factors $\mathrm{M}_{n_i}(D_i)$ corresponding precisely to the isotypical components of R, as can be seen in two ways:

- The factors $\mathrm{M}_{n_i}(D_i)$ are the isotypical components of $\mathrm{M}_{n_1}(D_1) \times \cdots \times \mathrm{M}_{n_r}(D_r)$ and are thus mapped by every isomorphism $\mathrm{M}_{n_1}(D_1) \times \cdots \times \mathrm{M}_{n_r}(D_r) \to R$ bijectively onto the isotypical components of R.
- The product structure of $\mathrm{M}_{n_1}(D_1) \times \cdots \times \mathrm{M}_{n_r}(D_r)$ correspondings to a decomposition $R = I_1 \oplus \cdots \oplus I_r$ into two-sided ideals. The ideals I_i are minimal nonzero two-sided ideals because the rings $\mathrm{M}_{n_i}(D_i)$ are simple. It follows from Lemma 23.52 that the ideals $I_1, \dots, I_r$ coincide the with isotypical components of R up to permutation.

By reordering the factors $\mathrm{M}_{n_i}(D_i)$ we may therefore assume that $R_{E_i} \cong \mathrm{M}_{n_i}(D_i)$ for all $i = 1, \dots, r$, where $E_1, \dots, E_r$ is a set of representatives for the isomorphism classes of simple R-modules. It now follows from Wedderburn's theorem that the number n_i is uniquely determined as the multiplicity of E_i in R, and the skew field D_i is uniquely determined up to isomorphism as $D_i \cong \mathrm{End}_R(E_i)^{\mathrm{op}}$.

23.54. Altogether we have shown that every semisimple ring R has a unique decomposition into a product of simple rings, and that each factor is isomorphic to matrix ring $\mathrm{M}_{n_i}(D_i)$ over a skew field D_i by Wedderburn's theorem, with n_i being uniquely determined and D_i being unique up to isomorphism.

24. Centralizers and Jacobson Density Theorems

24.1. Centralizers

Conventions 24.1. In this section, R denotes a ring.

Definition 24.2. The *centralizer* or *commutant* of a subset $S \subseteq R$ is

$$\mathrm{Z}_R(S) = \{r \in R \mid rs = sr \text{ for every } s \in S\}\,.$$

The set S'' is the *double centralizer* or *double commutant* or *bicommutant* of S.

Definition 24.3. The *center* of R is

$$\mathrm{Z}(R) \coloneqq \mathrm{Z}_R(R) = \{r \in R \mid rs = sr \text{ for every } s \in R\}\,.$$

Lemma 24.4. For every subset $S \subseteq R$ the centralizer $\mathrm{Z}_R(S)$ is a subring of R. The center $\mathrm{Z}(R)$ in particular is a subring of R.

Proof. We have that $1 \in \mathrm{Z}_R(S)$. For all $r_1, r_2 \in \mathrm{Z}_R(S)$ we have for every $s \in S$ that

$$(r_1 + r_2)s = r_1 s + r_2 s = s r_1 + s r_2 = s(r_1 + r_2)$$

and therefore $r_1 + r_2 \in \mathrm{Z}_R(S)$, as well as

$$r_1 r_2 s = r_1 s r_2 = s r_1 r_2$$

and therefore $r_1 r_2 \in \mathrm{Z}_R(S)$. For every $r \in \mathrm{Z}_R(S)$ we have for every $s \in S$ that

$$(-r)s = -(rs) = -(sr) = s(-r)$$

and therefore $-r \in \mathrm{Z}_R(S)$. □

Notation 24.5. We will often denote the centralizer of $S \subseteq R$ by S' instead of $\mathrm{Z}_R(S)$.

Lemma 24.6. Let $S, T \subseteq R$ be subsets.

a) If $S \subseteq T$ then $S' \supseteq T'$.

b) We have that $S \subseteq T'$ if and only if $S' \supseteq T$.

Proof. b) Both conditions express that every $s \in S$ commutes with every $t \in T$. □

Corollary 24.7. For every subset $S \subseteq R$ both S and $\langle S \rangle$, the subring generated by S, have the same centralizer $S' = \langle S \rangle'$.

Proof. For every subset $X \subseteq R$ we have that

$$S' \supseteq X \iff S \subseteq X' \iff \langle S \rangle \subseteq X' \iff \langle S \rangle' \supseteq X$$

because X' is a subring of R. This shows that S' and $\langle S \rangle'$ have the same subsets and are therefore equal. □

24.8. In the language of Remark 19.8 we have shown that the centralizer $(-)'$ defines an antitone Galois connection

$$\begin{tikzcd}\{\text{subrings } S \subseteq R\} \arrow[r, shift left, "(-)'"] & \{\text{subrings } S \subseteq R\} \arrow[l, shift left, "(-)'"]\end{tikzcd}$$

As always with antitone Galois connections we get the following consequences:

Corollary 24.9. Let $S \subseteq R$ be a subsets. Then $S \subseteq S''$ and $S''' = S'$.

Proof. That $S \subseteq S''$ follows from $S' \supseteq S'$ by Lemma 24.6. It follows from $S \subseteq S''$ that $S' \supseteq S'''$ because $(-)'$ is order-reversing and it follows from $S'' \supseteq S''$ that $S' \subseteq S'''$ by Lemma 24.6. □

24.10. Let us give some motivation for some of the upcomming sections and results:

Let M be an abelian group. Then M is a left $\mathrm{End}_{\mathbb{Z}}(M)$-module via

$$f \cdot m = f(m)$$

for all $f \in \mathrm{End}_{\mathbb{Z}}(M)$, $m \in M$.

Suppose that $R \subseteq \mathrm{End}_{\mathbb{Z}}(M)$ is a subring. Then the abelian groups M inherts an R-module structure by restriction. The centralizer R' then consists of all additive maps $f \colon M \to M$ such that

$$f \circ r = r \circ f$$

for all $r \in R$, which is equivalent to the condition

$$f(r \cdot m) = r \cdot f(m)$$

holding for all $r \in R$, $m \in M$. We therefore have that $R' = \mathrm{End}_R(M)$. By applying this result to the subring $\mathrm{End}_R(M) \subseteq \mathrm{End}_{\mathbb{Z}}(M)$ we also find that

$$R'' = \mathrm{End}_{R'}(M) = \mathrm{End}_{\mathrm{End}_R(M)}(M)\,.$$

The inclusion $R \subseteq R''$ tells us that every $r \in R$ acts on M by $\mathrm{End}_R(M)$-endomorphisms.

Suppose more generally that M is an R-module for a ring R. Then the R-module structure of M corresponds to a ring homomorphism

$$\Phi \colon R \to \mathrm{End}_{\mathbb{Z}}(M)\,, \quad r \mapsto (m \mapsto rm)\,.$$

By the above discussion we have that

$$\mathrm{im}(\Phi)' = \mathrm{End}_{\mathrm{im}(\Phi)}(M) = \mathrm{End}_R(M)$$

and we have that $\operatorname{im}(\Phi) \subseteq \operatorname{End}_{\operatorname{End}_R(M)}(M)$. By abuse of notation we will therefore also write

$$R' \coloneqq R'(M) \coloneqq \operatorname{End}_R(M)$$

even if R itself is not a subring of $\operatorname{End}_{\mathbb{Z}}(M)$. We can also replace the inclusion $R \subseteq R''(M)$, by the observation that Φ restrict to a homomorphism $R \to R''(M)$, which we will refer to as the *canonical homomorphism*.

We will be concerned with the following problems regarding centralizers:

- Suppose that $R \subseteq \operatorname{End}_{\mathbb{Z}}(M)$ is a subring. Then under what conditions do we have that $R = R''$? That is, under what conditions does R have the *double centralizer property*?

- Suppose more generally that M is an R-module for a ring R. Then under what conditions do R and M have the *double centralizer property* in the sense that the canonical homomorphism $R \xrightarrow{\Phi} R''(M)$ is surjective?

- Suppose that $R, S \subseteq \operatorname{End}_{\mathbb{Z}}(M)$ are subrings. Then under what conditions do we have that $R = S'$ and $S' = R$? That is, under what conditions do R and S *centralize each other*?

- Suppose more generally that M is both an R-module and and S-module for rings R, S and let $\Phi\colon R \to \operatorname{End}_{\mathbb{Z}}(M)$ and $\Psi\colon S \to \operatorname{End}_{\mathbb{Z}}(M)$ be the corresponding ring homomorphisms. Suppose further that the actions of R, S on M commute, i.e. that

  $$r \cdot (s \cdot m) = s \cdot (r \cdot m)$$

  for all $r \in R$, $s \in S$, $m \in M$. Then $\operatorname{im}(\Phi) \subseteq S'$ and $\operatorname{im}(\Psi) \subseteq R'$. That under what conditions do R and S *centralize each other* in the sense that $\operatorname{im}(\Phi) = S'$ and $\operatorname{im}(\Psi) = R'$?

Example 24.11. If R is simple then R has the double centralizer property with respect to every submodule $M \trianglelefteq R$ by Rieffel's theorem because the canonical homomorphism $R \to R''(M)$ is an isomorphism for $M \neq 0$, and still surjective for $M = 0$. Indeed, the original formulation of Rieffel's theorem in [Rie65] is that "R coincides with the bicommutant of M".

Proposition 24.12. If R is semisimple then every R-module M has the double centralizer property, i.e. for every R-module M the canonical homomorphism $R \to R''(M)$ is surjective.

Proof. We may assume w.l.o.g. that $R = \mathrm{M}_{n_1}(D_1) \times \cdots \times \mathrm{M}_{n_r}(D_r)$ for some $r \geq 0$, $n_1, \dots, n_r \geq 1$ and skew fields $D_1, \dots, D_r$ by the theorem of Artin–Wedderburn. If $M = M_1 \oplus \cdots \oplus M_r$ is the isotypical decomposition of M with M_i being the $D_i^{n_i}$-isotypical component then it follows that

$$R' = \operatorname{End}_R(M) \cong \operatorname{End}_R(M_1) \times \cdots \times \operatorname{End}_R(M_r)$$

with the factor $\operatorname{End}_R(M_i)$ acting on M_i but annihilating M_j for $j \neq i$. We thus have that $M = M_1 \boxplus \cdots \boxplus M_r$ as an $(\operatorname{End}_R(M_1) \times \cdots \times \operatorname{End}_R(M_r))$-module. It follows that

$$\begin{aligned} R'' &= \operatorname{End}_{R'}(M) \\ &= \operatorname{End}_{\operatorname{End}_R(M_1)\times\cdots\times\operatorname{End}_R(M_r)}(M_1 \boxplus \cdots \boxplus M_r) \\ &\cong \operatorname{End}_{\operatorname{End}_R(M_1)}(M_1) \times \cdots \times \operatorname{End}_{\operatorname{End}_R(M_r)}(M_r) \end{aligned}$$

by Lemma A6.22. The canonical homomorphism $R \to R''$ maps the factor $\mathrm{M}_{n_i}(D_i)$ of R into the factor $\operatorname{End}_{\operatorname{End}_R(M_i)}(M_i)$ of R'', so it sufficies to consider the case $r = 1$.

Thus we may assume that $R = \mathrm{M}_n(D)$ for some $n \geq 1$ and skew field D. We may then assume that $M = (D^n)^{\oplus I}$ for some index set I. Then

$$R' = \operatorname{End}_R(M) = \operatorname{End}_R((D^n)^{\oplus I}) \cong \mathrm{M}_I^{\mathrm{cf}}(\operatorname{End}_R(D^n)) \cong \mathrm{M}_I^{\mathrm{cf}}(D^{\mathrm{op}}) \cong \mathrm{M}_I^{\mathrm{rf}}(D)^{\mathrm{op}} .$$

where the first two isomorphisms follow from Corollary 22.25 and the third isomorphism follows from Remark A4.9.

To understand how the R'-module structure on M behaves under these isomorphisms we may think of $M = (D^n)^{\oplus I}$ as the space of row-finite matrices $\mathrm{M}^{\mathrm{rf}}(n \times I, D)$. The left R-module structure of M is then simply given by matrix-matrix multiplication, and the left R'-module structure on M corresponds to the right $\mathrm{M}_I^{\mathrm{rf}}(D)$-module structure on M given by matrix-matrix multiplication:

$$\begin{tikzcd} R \arrow[d, equal] & \curvearrowright & M \arrow[d, equal] & \curvearrowleft & (R')^{\mathrm{op}} \arrow[d, equal, "\wr"] \\ \mathrm{M}_n(D) & \curvearrowright & \mathrm{M}^{\mathrm{rf}}(n \times I, D) & \curvearrowleft & \mathrm{M}_I^{\mathrm{rf}}(D) \end{tikzcd}$$

We denote by $(D^{\oplus I})^T \coloneqq \mathrm{M}^{\mathrm{rf}}(1 \times I, D)$ the space of (row finite) row vectors of size I. Then

$$M \cong \underbrace{(D^{\oplus I})^T \oplus \cdots \oplus (D^{\oplus I})^T}_{n \text{ times}}$$

as left $\mathrm{M}_I^{\mathrm{rf}}(D)^{\mathrm{op}}$-modules, resp. right $\mathrm{M}_I^{\mathrm{rf}}(D)$-modules by decomposing M into rows. It follows from Remark 23.22 that

$$\operatorname{End}_{\mathrm{M}_I^{\mathrm{rf}}(D)^{\mathrm{op}}}\left((D^{\oplus I})^T\right) \cong D$$

with D acting on $(D^{\oplus I})^T$ by multiplication from the left. It follows that

$$\begin{aligned} R'' &= \operatorname{End}_{R'}(M) \\ &= \operatorname{End}_{\mathrm{M}_I^{\mathrm{rf}}(D)^{\mathrm{op}}}(M) \\ &\cong \operatorname{End}_{\mathrm{M}_I^{\mathrm{rf}}(D)^{\mathrm{op}}}\left((D^{\oplus I})^T \oplus \cdots \oplus (D^{\oplus I})^T\right) \\ &\cong \mathrm{M}_n\left(\operatorname{End}_{\mathrm{M}_I^{\mathrm{rf}}(D)^{\mathrm{op}}}\left((D^{\oplus I})^T\right)\right) \\ &\cong \mathrm{M}_n(D) \\ &= R \end{aligned}$$

with the action of R'' on M corresponding to the action of R on M. This shows that every $\varphi \in R''$ is of the form $\varphi(m) = rm$ for some $r \in R$, i.e. that the canonical homomorphism $R \to R''$ is surjective. □

24.2. Jacobson Density Theorems

24.13. We will finish this section by giving two classical results due to Jacobson which holds for (semi)simple modules over arbitrary rings.

Theorem 24.14 (First Jacobson density theorem)**.** If M is a semisimple R-module then the image of the canonical homomorphism $\Phi\colon R \to R''(M)$ is "dense" in $R''(M)$ in the sense that for every $f \in R''(M)$ and all finitely many elements $m_1, \dots, m_n \in M$ there exists some $r \in R$ with

$$f(m_i) = r \cdot m_i$$

for all $i = 1, \dots, n$.

Proof. We consider first the case $n = 1$:

Let $m = m_1 \in M$, let $f \in R''$ and let C be a direct complement of the cylic submodule $Rm \leq M$. Let $\pi\colon M \to M$ be the projection onto Rm along the decomposition $M = Rm \oplus C$. Then π is R-linear, i.e. an element of R', and it follows that f and π commute. It follows that

$$f(m) = f(\pi(m)) = \pi(f(m)) \in Rm$$

which shows that $f(m) = rm$ for some $r \in R$.

Suppose now that $n \geq 2$ and let $f \in R''$. We extend f to an additive map

$$\hat{f} \coloneqq f^{\oplus n}\colon M^{\oplus n} \to M^{\oplus n},$$

which is in matrix form (see Appendix A7) given by the diagonal matrix

$$\hat{f} = \begin{bmatrix} f & & \\ & \ddots & \\ & & f \end{bmatrix}.$$

It then follows from $f \in R'' = \operatorname{End}_{\operatorname{End}_R(M)}(M)$ that $\hat{f} \in \operatorname{End}_{\operatorname{End}_R(M^{\oplus n})}(M^{\oplus n})$: We can represent every $g \in \operatorname{End}_R(M^{\oplus n})$ as a matrix

$$g = \begin{bmatrix} g_{11} & \cdots & g_{1n} \\ \vdots & \ddots & \vdots \\ g_{n1} & \cdots & g_{nn} \end{bmatrix}$$

with entries $g_{ij} \in \operatorname{End}_R(M) = R'$. Then f commutes with every g_{ij} and it follow $\hat{f}$ and g commute.

The R-module $M^{\oplus n}$ is again semisimple to it follows from the previously considered case $n = 1$ that for all $m_1, \dots, m_n \in M$ there exists some $r \in R$ with

$$(f(m_1), \dots, f(m_n)) = \hat{f}(m_1, \dots, m_n) = r \cdot (m_1, \dots, m_n) = (r \cdot m_1, \dots, r \cdot m_n) \,.$$

We find that $f(m_i) = r \cdot m_i$ for every $i = 1, \dots, n$. □

Corollary 24.15. Let M be a semisimple R-module such that M is finitely-generated as an $R'(M)$-module. Then the canonical homomorphism $R \to R''(M)$ is surjective.

Proof. Let $m_1, \dots, m_n \in R$ be a finite R'-generating set of M. By the first Jacobson density theorem there exists some $r \in R$ with $r \cdot m_i = f(m_i)$ for all $i = 1, \dots, n$. Then the two R'-module homomorphisms $r \cdot (-)$ and f coincide on the R'-generating set $m_1, \dots, m_n$ of M, which shows that $f = r \cdot (-)$. □

Remark 24.16. The “density” in the first Jacobson density theorem can also be explained topologically: We can endow M with the discrete topology and $R''(M) \subseteq M^M$ with the induced product topology. Then the first Jacobson density theorem states that R (or more precisely $\operatorname{im}(\Phi)$ for the canonical homomorphism $\Phi \colon R \to R''(M)$) is topologically dense in $R''(M)$.

Theorem 24.17 (Second Jacobson density theorem)**.** Let M be a simple R-module and let $D \coloneqq R'(M)$. Suppose that $u_1, \dots, u_n \in M$ are D-linearly independent. Then the image of the canonical homomorphism $R \to R''(M)$ is dense in $R''(M)$ in the sense that for all $v_1, \dots, v_n \in M$ there exists some $r \in R$ with

$$r \cdot u_i = v_i$$

for all $i = 1, \dots, n$.

First proof. It follows from Schur’s lemma that D is a skew field. It follows from linear algebra that we can extend $u_1, \dots, u_n$ to a basis of M, from which it then follows that there exists some $f \in \operatorname{End}_D(M)$ with $f(u_i) = v_i$ for all $i = 1, \dots, n$. It then follows from the first Jacobson density theorem that there exists some $r \in R$ with

$$r \cdot u_i = f(u_i) = v_i$$

for all $i = 1, \dots, n$. □

Second proof. We need to show that $N \coloneqq M^{\oplus n}$ is as an R-module cyclicly generated by $x \coloneqq (u_1, \dots, u_n)$. The R-module N is semisimple, so there exists a direct complement C of Rx. Let $\pi \colon N \to N$ be the projection onto C along the decomposition $N = Rx \oplus C$. Then $\pi \in \operatorname{End}_R(N) = \operatorname{End}_R(M^{\oplus n})$ is given by a matrix

$$\pi = \begin{bmatrix} d_{11} & \cdots & d_{1n} \\ \vdots & \ddots & \vdots \\ d_{n1} & \cdots & d_{nn} \end{bmatrix}$$

with entries $d_{ij} \in \operatorname{End}_R(M) = D$ (see Appendix A7). It follows from $\pi(x) = 0$ that

$$d_{i1}u_1 + \dots + d_{in}u_n = d_{i1}(u_1) + \dots + d_{in}(u_n) = 0$$

for all $i = 1, \dots, n$. By using the D-linear independence of $u_1, \dots, u_n$ it follows that $d_{ij} = 0$ for all $i, j = 1, \dots, n$. This shows that $\pi = 0$, which shows that $C = 0$ and therefore that $N = Rx$. □

Remark 24.18. It can be shown that over an artinian ring R every simple R-module E is finite-dimensional as an $R'(M)$-module and therefore has the double centralizer property by the the second Jacobson density theorem. A proof of this finite-dimensionality can be found in [Isa09, Lemma 13.17].

25. The Double Centralizer Theorem

25.1. In this section we formulate and proof a double centralizer theorem for semisimple rings. Our exposition is inspired by [Yua12].

Conventions 25.2. In the following, R denotes a ring and M denotes an R-module.

25.1. Revisiting Isotypical Components and Multiplicity Spaces

25.3. We will begin by investigating how M behaves as an $R'(M)$-module. While we do not follow any particular source, most of the following results can be found in [DaS17, Chapter 3.2].

For this we first observe that the actions of R and R' on M commute in the sense that

$$\varphi \cdot (r \cdot m) = r \cdot (\varphi \cdot m)$$

for all $r \in R$, $\varphi \in R'$, $m \in M$. It follows that the R- and R'-module structures on M extend to an $(R' \otimes_{\mathbb{Z}} R)$-module structure given by

$$(\varphi \otimes r) \cdot m = \varphi \cdot (r \cdot m) = r \cdot (\varphi \cdot m)$$

for all simple tensors $\varphi \otimes r \in R' \otimes_{\mathbb{Z}} R$ and all $m \in M$.

The $(R' \otimes_{\mathbb{Z}} R)$-submodules of M are then precisely those R-submodules which are also R'-submodules. We have seen in Lemma 23.45 that if M is semisimple then these are precisely those R-submodules, which are a (direct) sum of isotypical components of M. We can therefore reformulate Lemma 23.45 as follows:

Lemma 25.4. Let M be semisimple as an R-module.

a) The isotypical decomposition $M = \bigoplus_{[E] \in \operatorname{Irr}(R)} M_E$ is a decomposition into simple $(R' \otimes R)$-submodules, and it is the unique such decomposition.

b) The summand M_E, $[E] \in \operatorname{Irr}(R)$ are pairwise non-isomorphic as $(R' \otimes R)$-modules.

The R-module M is in particular also semisimple as an $R' \otimes_{\mathbb{Z}} R$-module.

Proof. That $M = \bigoplus_{[E]\in\operatorname{Irr}(R)} M_E$ is the unique decomposition into simple $(R' \otimes R)$-submodules is a reformulation of Lemma 23.45. If $M_E \cong M_F$ as $(R' \otimes R)$-modules for some simple R-modules E, F then in particular $M_E \cong M_F$ as R-modules and therefore $E \cong F$. □

25.5. We have seen in subsection 22.3 that for every simple R-module E the E-isotypical component M_E can be described via the multiplicity space $\operatorname{Hom}_R(E, M)$: For the skew field $D \coloneqq \operatorname{End}_R(E)$ the evaluation map

$$\Phi\colon \operatorname{Hom}_R(E, M) \otimes_D E \to M_E, \quad f \otimes e \mapsto f(e)$$

is an isomorphism of R-modules. Here the left D-vector space structure on E is given by $\psi \cdot e = \psi(e)$ for all $\psi \in D$, $e \in E$, the right D-vector space structure on $\operatorname{Hom}_R(E, M)$ is induced by this left D-vector space structure on E, and the left R-module structure on $\operatorname{Hom}_R(E, M) \otimes_D E$ is inherited from E via

$$r \cdot (f \otimes e) = f \otimes (re)$$

for all $r \in R$ and simple tensors $f \otimes e \in \operatorname{Hom}_R(E, M) \otimes_D E$. We can now strengthen these results:

The multiplicity space $\operatorname{Hom}_R(E, M)$ carries the structure of a left R'-module via

$$\varphi \cdot f = \varphi \circ f$$

for all $\varphi \in R'$, $f \in \operatorname{Hom}_R(E, M)$. Together with the right D-vector space structure this makes $\operatorname{Hom}_R(E, M)$ into an R'-D-bimodule via

$$(\varphi \cdot f) \cdot \psi = \varphi \circ f \circ \psi = \varphi \cdot (f \cdot \psi)$$

for all $\varphi \in R'$, $f \in \operatorname{Hom}_R(E, M)$, $\psi \in D$. It follows that $\operatorname{Hom}_R(E, M) \otimes_D E$ carries the structure of a left R'-module via

$$\varphi \cdot (f \otimes e) = (\varphi \cdot f) \otimes e$$

for all $\varphi \in R'$ and simple tensors $f \otimes e \in \operatorname{Hom}_R(E, M) \otimes_D E$.

The actions of R' and R on $\operatorname{Hom}_R(E, M) \otimes E$ commute because

$$\varphi \cdot (r \cdot (f \otimes e)) = (\varphi \cdot f) \otimes (r \cdot e) = r \cdot (\varphi \cdot (f \otimes e))$$

for all $\varphi \in R'$, $r \in R$ and simple tensors $f \otimes e \in \operatorname{Hom}_R(E, M) \otimes_D E$. It follows that the R'- and R-module structures on $\operatorname{Hom}_R(E, M) \otimes_D E$ extend to an $(R' \otimes_{\mathbb{Z}} R)$-module structure given by

$$(\varphi \otimes r) \cdot (f \otimes e) = (\varphi \cdot f) \otimes (r \cdot e)$$

for all simple tensors $\varphi \otimes r \in R' \otimes_{\mathbb{Z}} R$ and $f \otimes e \in \operatorname{Hom}_R(E, M) \otimes_D E$.

Lemma 25.6. For $D \coloneqq \operatorname{End}_R(E)$ the evaluation map $\Phi\colon \operatorname{Hom}_R(E, M) \otimes_D E \to M_E$, $f \otimes e \mapsto f(e)$ is an isomorphism of $(R' \otimes R)$-modules.

Proof. We know from Lemma 22.53 that Φ is bijective, so it remains to show that Φ is $(R' \otimes R)$-linear. This holds because

$$\begin{aligned}\Phi((\varphi \otimes r) \cdot (f \otimes e)) &= \Phi((\varphi \cdot f) \otimes (r \cdot e)) = (\varphi \cdot f)(r \cdot e) = (\varphi \circ f)(re) \\ &= \varphi(f(re)) = \varphi(rf(e)) = (\varphi \otimes r) \cdot f(e) = (\varphi \otimes r) \cdot \Phi(f \otimes e)\end{aligned}$$

for all simple tensors $\varphi \otimes r \in R' \otimes_{\mathbb{Z}} R$ and $f \otimes e \in \mathrm{Hom}_R(E, M) \otimes_D E$. □

25.7. This shows us that under the above isomorphism $M_E \cong \mathrm{Hom}_R(E, M) \otimes_D E$ the action of $R' \otimes_{\mathbb{Z}} R$ on M_E can be understood componentwise. If M is semisimple and contains (an isomorphic copy of) E then $\mathrm{Hom}_R(E, M) \otimes_D E$ is nonzero and simple as an $(R' \otimes_{\mathbb{Z}} R)$-module, and the tensor factor E is simple as an R-module by construction. This begs the questions if $\mathrm{Hom}_R(E, M)$ is simple as an R'-module.

Lemma 25.8. Let M be semisimple and suppose that $M_E \neq 0$. Let $D \coloneqq \mathrm{End}_R(E)$.

a) The R'-module $\mathrm{Hom}_R(E, M)$ is simple.

b) If $E \ncong F$ as R-modules then $\mathrm{Hom}_R(E, M) \ncong \mathrm{Hom}_R(E, F)$ as R'-modules.

c) We have that $\mathrm{End}_{R'}(\mathrm{Hom}_R(E, M)) \cong D^{\mathrm{op}}$ with the left $\mathrm{End}_{R'}(\mathrm{Hom}_R(E, M))$-module structure of $\mathrm{Hom}_R(E, M)$ corresponding to the left D^{op}-module structure of $\mathrm{Hom}_R(E, M)$ associated to the right D-module structure discussed in 22.51.

Proof.

a) The inclusion $\iota\colon M_E \to M$ induces an isomorphism of abelian groups

$$\mathrm{Hom}_R(E, M_E) \xrightarrow{\iota_*} \mathrm{Hom}_R(E, M)\,,$$

so we may identify $\mathrm{Hom}_R(E, M)$ with $\mathrm{Hom}_R(E, M_E)$. We have that

$$R' = \mathrm{End}_R(M) \cong \prod_{[E'] \in \mathrm{Irr}(R)} \mathrm{End}_R(M_{E'})$$

with all factors but $\mathrm{End}_R(M_E)$ annihilating M_E, and therefore also $\mathrm{Hom}_R(E, M)$. We therefore need to show that $\mathrm{Hom}_R(E, M_E)$ is simple as an $\mathrm{End}_R(M_E)$-module, i.e. it sufficies to consider the case $M = M_E$, i.e. the case that M is E-isotypical.

Let $M = \bigoplus_{i \in I} L_i$ be a decomposition into simple R-modules, each of which (necessarily) isomorphic to E, and let $D \coloneqq \mathrm{End}_R(E)$. We have that $I \neq \emptyset$ because $M_E \neq 0$. For every $i \in I$ let $\tilde{f}_i\colon E \to L_i$ be an isomorphism and let $f_i\colon E \to M$ be the extension of $\tilde{f}_i$ to a homomorphism $E \to M$. Then $(f_i)_{i \in I}$ is a right D-basis of $\mathrm{Hom}_R(E, M)$ by Proposition 22.53, so that

$$\mathrm{Hom}_R(E, M) = \bigoplus_{i \in I} f_i D \cong D^{\oplus I}\,.$$

We have on the other hand that

$$R' = \mathrm{End}_R(M) = \mathrm{End}_R\left(\bigoplus_{i\in I} L_i\right) \cong \mathrm{End}_R(E^{\oplus I}) \cong \mathrm{M}_I^{\mathrm{cf}}(\mathrm{End}_R(E)) = \mathrm{M}_I^{\mathrm{cf}}(D)$$

by Corollary 22.25. The left R'-module structure of $\mathrm{Hom}_R(E,M)$ corresponds under these isomorphisms to the $\mathrm{M}_I^{\mathrm{cf}}(D)$-module structure of $D^{\oplus I}$ which is given by matrix-vector multiplication, and which is simple by Example 22.4, part d).

b) Under the above isomorphism $R' \cong \prod_{[E']\in\mathrm{Irr}(R)} \mathrm{End}_R(M_{E'})$ the factor $\mathrm{End}_R(M_E)$ acts non-trivially on $\mathrm{Hom}_R(M,E)$ (because it is simple as an $\mathrm{End}_R(M_E)$-module as seen above) but annihilates M_F and therefore also $\mathrm{Hom}_R(F,M)$.

c) We have by the above identifications that

$$\begin{aligned}\mathrm{End}_{R'}(\mathrm{Hom}_R(E,M)) &\cong \mathrm{End}_{\mathrm{End}_R(M_E)}(\mathrm{Hom}_R(E,M_E))\\ &\cong \mathrm{End}_{\mathrm{M}_I^{\mathrm{cf}}(D)}(D^{\oplus I}) \cong D^{\mathrm{op}}\end{aligned}$$

as seen in Remark 23.22. □

Warning 25.9. If M is not semisimple then $\mathrm{Hom}_R(E,M)$ is non necessarily simple as an R'-module, as the following counterexample from [MS18b] shows: Consider the ring $R = k[X,Y]$, the ideal $I \coloneqq (X,Y)$ and the R-modules $M \coloneqq R/I^2$. Then $E \coloneqq R/I$ is simple (because it is one-dimensional) with

$$\mathrm{Hom}_R(E,M) = \mathrm{Hom}_R(R/I, R/I^2) \cong I/I^2\,.$$

We have that $\mathrm{End}_R(E) = \mathrm{End}_R(R/I) \cong R/I \cong k$ but I/I^2 is two-dimensional and therefore not simple as an $\mathrm{End}_R(E)$-module.

25.10. Suppose that $M_E \neq 0$, i.e. that (up to isomorphism) E occurs in M. For $E' \coloneqq \mathrm{Hom}_R(E,M)$ we have now seen that $M_E \cong E' \otimes_D E$ as $(R' \otimes R)$-modules with E simple as an R-module and R' simple as an R'-module. From this we get the following observations:

- We have that

$$M_E \cong E' \otimes_D E \cong D^{\oplus \dim_D(E')} \otimes_D E \cong E^{\oplus \dim_D(E')}$$

as R-modules, so the multiplicity of E in M_E, which is the same as the multiplicity of E in M, is the right D-dimension of E'. (We have already seen this in Corollary 22.54.)

- We similarly have that

$$M_E \cong E' \otimes_D E \cong E' \otimes_D D^{\oplus \dim_D(E)} \cong (E')^{\oplus \dim_D(E)}\,. \tag{25.1}$$

It follows that the R-isotypical decomposition $M = \bigoplus_{[E]\in\mathrm{Irr}(R)} M_E$ coincides with the R'-isotypical decomposition in such way that $M_{E'} = M_E$ for all $[E] \in \mathrm{Irr}(R)$ because $E' \ncong F'$ for $E \ncong F$. It therefore also follows from (25.1) that the multiplicity of E' in M is the left D-dimension of D.

We can summarize our findings as follows:

Theorem 25.11. Let M be semisimple.

a) There exists a unique decomposition $M = \bigoplus_{i \in I} M_i$ into simple $(R' \otimes_{\mathbb{Z}} R)$-modules. The simple $(R' \otimes_{\mathbb{Z}} R)$-modules M_i are pairwise non-isomorphic and this decomposition coincides with both the R-isotypical and the R'-isotypical compositions of M. The R-module M is in particular also semisimple as an R'-module.

b) Every simple $(R' \otimes_{\mathbb{Z}} R)$-submodule M_i is of the form $E'_i \otimes_{D_i} E_i$ for a simple R'-module E'_i, a simple R-module E_i and a skew field D_i with $D_i \cong \operatorname{End}_R(E_i)$ and $D_i^{\mathrm{op}} \cong \operatorname{End}_{R'}(E'_i)$. The modules E_i, E'_i and the skew field D_i are unique up to isomorphism.

c) The simple $(R' \otimes_{\mathbb{Z}} R)$-module M_i coincides with both the E_i-isotypical and the E'_i-isotypical components of M.

d) The simple R-modules which occur in M are up to isomorphism precisely E_i, $i \in I$ and these modules are pairwise non-isomorphic. Similarly, the simple R'-modules which occur in M are up to isomorphism precisely E'_i, $i \in I$ and these modules are pairwise non-isomorphic.

   Thus the correspondence $E_i \leftrightarrow E'_i$ is a 1:1-correspondence between the isomorphism class of simple R-modules occuring in E and the isomorphism classes of simple R'-modules occuring in M.

e) The multiplicity of E_i in M is the right D_i-dimension of E'_i and the multiplicity of E'_i in M is the left D_i-dimension of E_i.

Proof. It only remains to show for part b) that when $E' \otimes_{D_1} E \cong F' \otimes_{D_2} F$ as $(R' \otimes_{\mathbb{Z}} R)$-modules then $E' \cong F'$ as R'-modules and $F \cong E$ as R-modules. We have that

$$E' \otimes_{D_1} E \cong E^{\oplus \dim_{D_1}(E')} \quad \text{and} \quad F' \otimes_{D_2} F \cong F^{\oplus \dim_{D_1}(F')}$$

as R-modules, so if $E' \otimes_{D_1} E \cong F' \otimes_{D_2} F$ as $(R' \otimes_{\mathbb{Z}} R)$-modules then also

$$E^{\oplus \dim_{D_1}(E')} \cong F^{\oplus \dim_{D_2}(F')}$$

as R-modules and therefore $E \cong F$ as R-modules. That $E' \cong F'$ as R'-modules follows in the same way. □

Warning 25.12. Not every simple R'-module needs to occur in M even if M is semisimple: Consider the semisimple $\mathbb{Z}$-module $M := \bigoplus_{p \text{ prime}} \mathbb{Z}/p$. We have that

$$R' = \operatorname{End}_R(M) \cong \prod_{p \text{ prime}} \operatorname{End}_{\mathbb{Z}}(\mathbb{Z}/p) \cong \prod_{p \text{ prime}} \mathbb{Z}/p$$

and the simple R'-module occuring in M are precisely the summands $\mathbb{Z}/p$. But we have seen in Remark 23.18 that R' admits other simple modules then the $\mathbb{Z}/p$.

Remark 25.13. It can also be shown in a more direct way that M is semisimple as an R'-module if it is semisimple as an R-module, as explained in [Beh72, Chapter IV, Section 2,Theorems 6,7,8]. We will sketch of this approach here:

- By using the uniqueness of multiplicities it can be shown that every isomorphism $L \to L'$ between simple submodules $L, L' \leq M$ can not only be extended to an endomorphism $M \to M$ but already to an automorphism $M \to M$.
- It then follows that for every simple R-module $L \leq M$ and $m \in M$ the cyclic R'-module $R'm$ is simple (as in R'-module).
- This shows that every element $m \in M$ which is contained in a simple R-submodule is also contained in a simple R'-submodule. Since M is the sum of its simple R-submodules it then follows that M is also the sum of its simple R'-submodules.

Digression: M as an R''-module

25.14. We have so far examined how a semisimple R-module M looks like as an R'-module: It is again semisimple with the same isotypical components and the occuring simple R'-modules can be described as multiplicity spaces of the occuring simple R-modules.

We can also investigate how E looks like as an R''-module. The main observations are taken from [DaS17, Chapter 2.6].

Lemma 25.15. Two subsets $N, P \subseteq M$ are R-submodules with $M = N \oplus P$ if and only if they are R''-submodules with $M = N \oplus P$.

Proof. That N, P are R-submodules with $M = N \oplus P$ is equivalent to the existence of an idempotent element $e \in \operatorname{End}_R(M) = R'$ with $N = \ker(e)$ and $P = \operatorname{im}(e)$. Similary, N, P are R''-sumodules if and only if there exists an idempotent element $e \in \operatorname{End}_{R''}(M) = R'''$ with $N = \ker(e)$ and $P = \operatorname{im}(e)$. Both conditions are equivalent because $R' = R'''$. □

Proposition 25.16. Let M be semisimple as an R-module.

a) The R-submodules of M are precisely the R''-submodules of M.

b) A submodule $E \leq M$ is simple over R if and only if it is simple over R''. The R-module M is in particular also semisimple as an R''-module.

c) For every two submodules $N, P \leq M$ we have that $\operatorname{Hom}_R(N, P) = \operatorname{Hom}_{R''}(N, P)$. The submodules $N, P \leq M$ are in particular isomorphic as R-modules if and only if they are isomorphic as R''-modules.

d) The isotypical components of M as an R-module coincide with the isotypical components of M as an R''-module.

Proof.

a) Every R''-submodule is also an R-submodule, and every R-submodule is a direct summand and therefore also an R''-submodule by Lemma 25.15.

b) The simple submodules are precisely the minimal nonzero submodules, which are by part a) the same for both R and R''. It follows from the R-semisimplicity of M that M is a sum of simple R-modules, and therefore also a sum of simple R''-modules.

c) Every R-module homomorphism $N \to P$ extends to an R-module endomorphism $M \to M$ because M is semisimple as an R-module. In other words, every R-module homomorphism $N \to P$ is the restriction of an R-module endomorphism $M \to M$. The same holds for M as an R''-module. The claim thus follows from the equality $\mathrm{End}_R(M) = R' = R''' = \mathrm{End}_{R''}(M)$.

d) This follows from part a) with help of part c) because two simple submodules of M are isomorphic as R-modules if and only they are isomorphic as R'-modules. □

25.2. The Double Centralizer Theorem

Proposition 25.17. If M is semisimple then R' is semisimple if and only if M is the sum of only finitely many simple submodules.

Proof. Let $(E_i)_{i \in I}$ be a set of representatives for the isomorphism classes of simple R-modules. We may assume w.l.o.g. that $M = \bigoplus_{i \in I} E_i^{\oplus J_i}$ for some index sets J_i, $i \in I$. It then follows from Corollary 22.25 that

$$R' = \mathrm{End}_R(M) \cong \prod_{i \in I} \mathrm{M}^{\mathrm{cf}}_{J_i}(D_i)$$

for the skew fields $D_i \coloneqq \mathrm{End}_R(E_i)$. If J_i were nonempty for infinitey many $i \in I$ then R' would not be semisimple, as can be seen in (at least) two ways:

- The ring $\prod_{i \in I} \mathrm{M}^{\mathrm{cf}}_{J_i}(D_i)$ would be neither noetherian nor artinian, and would therefore not semisimple by Corollary 23.14,
- The ring $\prod_{i \in I} \mathrm{M}^{\mathrm{cf}}_{J_i}(D_i)$ would contain infinitely many two-sided ideals (namely the factors $\mathrm{M}^{\mathrm{cf}}_{J_i}(D_i)$) and would therefore not be semisimple by Corollary 23.47.

Thus for R' to be semisimple, J_i must be empty for all but finitely many $i \in I$, i.e. up to isomorphism only finitely many simple R-modules are allowed to occur in M.

Hence we need only consider the case $M = E_1^{\oplus J_1} \oplus \cdots \oplus E_n^{\oplus J_n}$ and

$$R' \cong \mathrm{M}^{\mathrm{cf}}_{J_1}(D_1) \times \cdots \times \mathrm{M}^{\mathrm{cf}}_{J_n}(D_n) \,.$$

It then follows from Proposition 23.17 that R' is semisimple if and only if each factor $\mathrm{M}^{\mathrm{cf}}_{J_i}(D_i)$ is semisimple, which by Example 23.5 and Example 23.15 holds if and only if each J_i is finite. □

Theorem 25.18 (Double Centralizer Theorem)**.** Let R be semisimple and let M be faithful. Suppose that M decomposes into finitely many simple R-modules.

a) The centralizer R' is again semisimple.

b) The canonical homomorphism $R \to R''$ is an isomorphism.

c) There exists a unique decomposition

$$M = M_1 \oplus \cdots \oplus M_n$$

into simple $(R' \otimes_{\mathbb{Z}} R)$-modules and this decomposition coincides with both the R-isotypical decomposition and the R'-isotypical decomposition of M.

d) Each $(R' \otimes_{\mathbb{Z}} R)$-submodule M_i is of the form $M_i \cong E'_i \otimes_{D_i} E_i$ for a simple R'-module E'_i, a simple R-module E_i and a skew field D_i with $D_i \cong \mathrm{End}_R(E_i)$ and $D_i^{\mathrm{op}} \cong \mathrm{End}_R(E'_i)$. The modules E_i, E'_i and the skew field D_i are unique up to isomorphism.

e) The summand M_i is both the E_i-isotypical and the E'_i-isotypical component of M.

f) The R-modules $E_1, \dots, E_n$ form a set of representatives of the isomorphism classes of simple R-modules and the R'-modules $E'_1, \dots, E'_n$ form a set of representatives of the isomorphism classes of simple R'-modules.

   Thus the correspondence $E_i \leftrightarrow E'_i$ is a 1:1-correspondence $\mathrm{Irr}(R) \leftrightarrow \mathrm{Irr}(R')$.

Proof.

a) This follows from Proposition 25.17.

b) This follows from Proposition 24.12.

c) This follows from Theorem 25.11.

d) This follows from Theorem 25.11.

e) This follows from Theorem 25.11.

f) It follows from Corollary 23.31 that up to isomorphism every simple R-module and every simple R'-module occurs in M, so the claim follows from Theorem 25.11. □

Remark 25.19. The above version of the double centralizer theorem is a combination of the version given in the lecture (which can be found in Corollary 26.25) and the version given in [Yua12].

Semisimple k-Algebras

26. Consequences for k-Algebras

26.1. From now on we will restrict our attention to k-algebras, often finite-dimensional and semisimple. In this section we collect some results for semisimple k-algebras which follows from the general theory of semisimple modules and rings from the previous chapter.

Conventions 26.2. In this section k denotes a field and A denotes a k-algebra. We abreviate $\dim_k =: \dim$ and $\otimes_k =: \otimes$.

Lemma 26.3. If A is a finite-dimensional k-algebra then every simple A-module is also finite-dimensional.

Proof. Every simple A-module M is of the form A/I for a maximal left ideal $I \trianglelefteq A$. □

Notation 26.4. The set of isomorphism classes of finite-dimensional simple A-modules is denoted by $\operatorname{irr}(A)$.

26.5. Note that if A is finite-dimensional then $\operatorname{irr}(A) = \operatorname{Irr}(A)$ by Lemma 26.3.

Multiplicities

26.6. We can strengthen Lemma 22.46 for finite-dimensional semisimple modules by calculations the multiplicities of the simple summands.

Lemma 26.7. Let M, N be two finite-dimensional semisimple A-modules. Then

$$\dim \operatorname{Hom}_A(M, N) = \dim \operatorname{Hom}_A(N, M) .$$

Proof. Let $M = M_1 \oplus \cdots \oplus M_m$ and $N = N_1 \oplus \cdots \oplus N_n$ be decompositions into simple submodules. We then have that

$$\operatorname{Hom}_A(M, N) \cong \prod_{i=1}^{m} \prod_{j=1}^{n} \operatorname{Hom}_A(M_i, N_j)$$

and

$$\operatorname{Hom}_A(N, M) \cong \prod_{j=1}^{n} \prod_{i=1}^{m} \operatorname{Hom}_A(N_i, M_j)$$

as k-vector spaces (see Theorem A7.6). It therefore sufficies to consider the case that both M, N are simple. For $M \cong N$ we have that $\operatorname{Hom}_A(M, N) \cong \operatorname{Hom}_A(N, M)$ as k-vector spaces, so it sufficies to consider the case $M \ncong N$. It then follows from Schur's lemma that $\operatorname{Hom}_A(M, N) = 0 = \operatorname{Hom}_A(N, M)$. □

Lemma 26.8. Let M be a semisimple A-module with $M \cong M_1^{\oplus n_1} \oplus \cdots \oplus M_r^{\oplus n_r}$ for pairwise non-isomorphic finite-dimensional simple A-modules $M_1, \dots, M_r$.

a) The numbers $n_1, \dots, n_r$ are uniquely determined as

$$n_i = \frac{\dim \operatorname{Hom}_A(M_i, M)}{\dim \operatorname{End}_A(M_i)} = \frac{\dim \operatorname{Hom}_A(M, M_i)}{\dim \operatorname{End}_A(M_i)}$$

for all $i = 1, \dots, r$.

b) If k is algebraically closed then $n_i = \dim \operatorname{Hom}_A(M_i, M) = \dim \operatorname{Hom}_A(M, M_i)$ for all $i = 1, \dots, r$.

Proof.

a) We have that

$$\begin{aligned} \operatorname{Hom}_A(M_i, M) &= \operatorname{Hom}_A(M_i, M_1^{\oplus n_1} \oplus \cdots \oplus M_r^{\oplus n_r}) \\ &\cong \operatorname{Hom}_A(M_i, M_1)^{n_1} \times \cdots \times \operatorname{Hom}_A(M_i, M_r)^{n_r} \end{aligned}$$

as k-vector spaces (see Corollary A7.8). It follows from Schur's lemma and the simplicity of the M_i that $\operatorname{Hom}(M_i, M_j) = 0$ for all $i \neq j$, and therefore that

$$\operatorname{Hom}_A(M_i, M) \cong \operatorname{Hom}_A(M_i, M_i)^{n_i} = \operatorname{End}_A(M_i)^{n_i}$$

as k-vector spaces. It follows that

$$\dim \operatorname{Hom}_A(M_i, M) = \dim \operatorname{End}_A(M_i)^{n_i} = n_i \dim \operatorname{End}_A(M_i)\,,$$

and it follows from the finite-dimensionality of M_i that $\operatorname{End}_A(M_i)$ is finite-dimensional. This shows the first equality of the first formula. The second equality follows from Lemma 26.7.

b) If k is algebraically closed then it follows for every $i = 1, \dots, r$ from Schur's lemma that $\operatorname{End}_A(M_i) = k$ and therefore that $\dim \operatorname{End}_A(M_i) = 1$. □

Proposition 26.9. Let A be finite-dimensional and semisimple. Let $M_1, \dots, M_r$ be a set of representatives for the isomorphism classes of simple A-modules, let $d_i = \dim M_i$ and let n_i be the multiplicity of M_i in A.

a) We have that

$$n_i = \frac{d_i}{\dim \operatorname{End}_A(M_i)}$$

for every $i = 1, \dots, r$, and

$$\dim A = \sum_{i=1}^{r} \frac{d_i^2}{\dim \operatorname{End}_A(M_i)}\,.$$

b) If k is algebraically closed then $n_i = m_i$ for every $i = 1, \dots, r$ and $\dim A = \sum_{i=1}^{r} d_i^2$.

Proof.

a) We have that $\operatorname{Hom}_A(A, M_i) \cong M_i$ as k-vector spaces, and therefore that

$$d_i = \dim M_i = \dim \operatorname{Hom}_A(A, M_i) = n_i \dim \operatorname{End}_A(M_i)$$

by Lemma 26.8. It further follows from $A \cong M_1^{\oplus n_1} \oplus \cdots \oplus M_r^{n_r}$ that

$$\dim A = \sum_{i=1}^{r} n_i d_i = \sum_{i=1}^{r} \frac{d_i^2}{\dim \operatorname{End}_A(M_i)} \,.$$

b) If k is algebraically closed then $\dim \operatorname{End}_A(M_i) = 1$ by Schur's Lemma. □

The Theorems of Artin–Wedderburn and Wedderburn

Corollary 26.10 (Artin–Wedderburn)**.** Let k be algebraically closed and let A be finite-dimensional and semisimple.

a) We have that $A \cong \mathrm{M}_{n_1}(k) \times \cdots \times \mathrm{M}_{n_r}(k)$ as k-algebras for some $r \geq 0$ and $n_1, \dots, n_r \geq 1$. The number r is uniquely determined as the number of isomorphism classes of simple A-modules and if $V_1, \dots, V_r$ is a set of representatives for those isomorphism classes then the numbers $n_1, \dots, n_r$ agree with the numbers $\dim V_1, \dots, \dim V_r$ up to permutation.

b) The following conditions are equivalent:

1) The k-algebra A is commutative.
2) We have that $A \cong k \times \cdots \times k$.
3) All simple A-modules are one-dimensional.
4) There exist precisely $\dim A$ many isomorphism classes of simple modules.

Proof.

a) This is a consequence of the theorem of Artin–Wedderburn because it follows from Lemma 26.3 and Schur's Lemma that $\operatorname{End}_A(M) = k$ for every simple A-module M.

b) This follows from part a). □

Corollary 26.11. If k is algebraically closed and A is finite-dimensional and semisimple then $\dim \mathrm{Z}(A)$ coincides with the number of isomorphism classes of simple A-modules.

Proof. We have that $A \cong \mathrm{M}_{n_1}(k) \times \cdots \times \mathrm{M}_{n_r}(k)$ where $r \geq 0$ is the number of isomorphism classes of simple A-modules and $n_1, \dots, n_r \geq 1$. It follows that

$$\begin{aligned} F\,\mathrm{Z}(A) &\cong \mathrm{Z}(\mathrm{M}_{n_1}(k) \times \cdots \times \mathrm{M}_{n_r}(k)) \\ &= \mathrm{Z}(\mathrm{M}_{n_1}(k)) \times \cdots \times \mathrm{Z}(\mathrm{M}_{n_r}(k)) \cong k \times \cdots \times k = k^{\times r} \end{aligned}$$

is r-dimensional where the second isomorphism follows from Lemma 23.3. □

26.12. We can use the theorem of Artin–Wedderburn to given an alternative proof for Propositon 26.9.

Alternative proof to Proposition 26.9, part a). By the theorem of Artin–Wedderburn there exist division k-algebras $D_1, \dots, D_r$ such that

$$A \cong \mathrm{M}_{n_1}(D_1) \times \cdots \times \mathrm{M}_{n_r}(D_r)$$

as k-algebras. Then $D_1^{n_1}, \dots, D_r^{n_r}$ is another set of representatives for the isomorphism classes of simple A-modules, and $\mathrm{End}_A(D_i^{n_i}) \cong D_i^{\mathrm{op}}$ for every $i = 1, \dots, r$. We may assume w.l.o.g. that $M_i = D_i^{n_i}$ for every $i = 1, \dots, r$. We then have that $D_i^{\mathrm{op}} \cong \mathrm{End}_A(M_i)$ for every $i = 1, \dots, r$ and it follows that

$$d_i = \dim M_i = \dim D_i^{n_i} = n_i \dim D_i = n_i \dim \mathrm{End}_A(M_i)^{\mathrm{op}} = n_i \dim \mathrm{End}_A(M_i) \,,$$

which proves the first equality. The second equality follows as in the first proof, but can also be calculated as

$$\dim A = \sum_{i=1}^{r} n_i^2 \dim D_i = \sum_{i=1}^{r} n_i^2 \dim \mathrm{End}_A(M_i) = \sum_{i=1}^{r} \frac{d_i}{\dim \mathrm{End}_A(M_i)}$$

where we used the first equality for the last step. □

Corollary 26.13 (Wedderburn)**.** Let A be finite-dimensional and simple.

a) We have that $A \cong \mathrm{M}_n(D)$ as k-algebras for some $n \geq 1$ and divison k-algebra D.

b) If k is algebraically closed then $A \cong \mathrm{M}_n(k)$ for some $n \geq 1$.

Proof.

a) The k-algebra A contains a nonzero left ideal of minimal dimension, which is then a minimal nonzero left ideal. The claim thus follows from Wedderburn's theorem.

b) We have that $\dim D \leq \dim A < \infty$ so it follows that $D = k$. □

The number n is uniquely determined and the division k-algebra D is uniquely determined up to isomorphism.

Centralizers and Jacobson Density Theorems

Centralizers

26.14. In our previous discussion about centralizers (subsection 24.1) we have used the endomorphism ring $\mathrm{End}_{\mathbb{Z}}(M)$ of an abelian group M. When working with k-algebras instead of general rings it is however more natural to replace $\mathbb{Z}$ by k, requiring M to be a k-vector space and working with $\mathrm{End}_k(M)$ instead of $\mathrm{End}_{\mathbb{Z}}(M)$. It turns out that it makes no difference if we use $\mathrm{End}_{\mathbb{Z}}(M)$ or $\mathrm{End}_k(M)$ if we want to compute centralizers of k-subalgebras:

Let M be a k-vector space and let $A \subseteq \operatorname{End}_k(M)$ be a k-subalgebra. Let A'_k be the centralizer of A in $\operatorname{End}_k(M)$ and let A' be the usual centralizer of A in $\operatorname{End}_{\mathbb{Z}}(M)$. Then $A'_k = A'$: It follows from $\operatorname{End}_k(M) \subseteq \operatorname{End}_{\mathbb{Z}}(M)$ that $A'_k \subseteq A'$. To show the other inclusion let

$$K := \{(m \mapsto \lambda m) \mid \lambda \in M\} \subseteq \operatorname{End}_{\mathbb{Z}}(M)\,.$$

Then $\operatorname{End}_k(M) = \mathrm{Z}_{\operatorname{End}_{\mathbb{Z}}(M)}(K) = K'$ and $K \subseteq A$. It follows that $A' \subseteq K' = \operatorname{End}_{\mathbb{Z}}(M)$ and therefore that $A' \subseteq A' \cap \operatorname{End}_k(M) = A'_k$.

This shows that we do not have to distinguish between the centralizer of A in $\operatorname{End}_{\mathbb{Z}}(M)$ and the centralizer of A in $\operatorname{End}_k(M)$. Note also that A' is again a k-subalgebra of A because $A \subseteq \operatorname{End}_k(A) = K'$ and thus $A' \supseteq K$.

If A is any k-algebra and M is a A-module then by the above disucussion the commutator A' can be computed in $\operatorname{End}_k(A)$ and is again a k-subalgebra of $\operatorname{End}_k(A)$.

Density Theorem

26.15. While we have given the Jacobson density theorems in their general form in subsection 24.2 we will mostly apply them to finite-dimensional (semi)simple modules over k-algebras for an algebraically closed field k. This hat two main reasons:

- If M is finite-dimensional then M is finitely generated over all occuring k-algebras (over which M is a module). This allows us to replace the "density" from the Jacobson density theorems by actual equality, resp. surjectivity of the canonical homomorphism $A \to A''(M)$.
- If k is algebraically closed and M is finite-dimensional simple A-module then it follows from Schur's Lemma that $\operatorname{End}_A(M) = k$ and the double centralizer A'' becomes
$$A'' = \operatorname{End}_{\operatorname{End}_A(M)}(M) = \operatorname{End}_k(M)\,.$$
(The consequences of this should not be underestimated.)

Roughly speaking this make sure that we can apply the Jacobson density theorems to all occuring (semi)simple modules and that the results become particularly nice.

Lemma 26.16. Every finite-dimensional semisimple A-module M has the double centralizer property, i.e. the canonical homomorphism $A \to A''(M)$ is surjective.

Proof. It follows from the finite-dimensionality of M that M is finitely generated as an A'-module, so the claim follows from Corollary 24.15. □

Corollary 26.17 (Existence of projection operators, [Lan05, XVII, Theorem 3.7])**.** Let $M_1, \dots, M_n$ be pairwise non-isomorphic finite-dimensional simple A-modules. Then there exists for every $i = 1, \dots, n$ some element $a \in A$ with $am_i = m_i$ for every $m_i \in M_i$ and $aM_j = 0$ for every $j \neq i$.

Proof. The A-module $M := M_1 \oplus \cdots \oplus M_n$ is finite-dimensional and semisimple, which is why the canonical homomorphism $A \to A'' = \operatorname{End}_{\operatorname{End}_A(M)}(M)$ is surjective. It therefore sufficies to show that for every $i = 1, \dots, n$ the projection $\pi_i \colon M \to M$ onto

M_i along the decomposition $M = M_1 \oplus \cdots \oplus M_n$ is contained in A''. For this we need to show that for every $f \in A'$, i.e. every A-linear map $f\colon M \to M$, we have that

$$\pi_i \circ f = f \circ \pi_i \,.$$

This is equivalent to the inclusion $f(M_i) \subseteq M_i$ which holds because M_i is the M_i-isotypical component of M. □

Corollary 26.18. If A is finite dimensional then there exist at most $\dim A$ many simple A-modules up to isomorphism.

Proof. If $M_1, \dots, M_r$ are pairwise non-isomorphic simple A-modules then they are finite-dimensional by Lemma 26.3. It then follows that there exist elements $a_1, \dots, a_r$ such that a_i acts on $M_1 \oplus \cdots \oplus M_r$ by the projection π_i onto the i-th summand M_i. The projections $\pi_1, \dots, \pi_n$ are linearly independent elements of $\operatorname{End}_k(M_1 \oplus \cdots \oplus M_r)$ so it follows that $a_1, \dots, a_r$ are also linearly independent elements of A. □

Remark 26.19. If A is infinite-dimensional then the cardinality $\operatorname{card} \operatorname{irr}(R)$ cannot be bound in terms of $\dim A$:

For the countable infinite-dimensional k-algebra $A \coloneqq k[X]$ every element $\lambda \in k$ results in a simple A-module $M_\lambda \coloneqq k[X]/(X - \lambda)$, which is one-dimensional and on which $X \in A$ acts by multiplication with λ. Then M_λ, $\lambda \in k$ are pairwise non-isomorphic simple A-modules and it follows that $\operatorname{card} \operatorname{irr}(A) \geq \operatorname{card} k$, independent of the countable dimension of A.

(Since A contains only $\operatorname{card} k$ many elements, thus at most $\operatorname{card} k$ many principal ideals, and therefore at most $\operatorname{card} k$ many maximal left ideals, it also follows that $\operatorname{card} \operatorname{Irr}(A) \leq \operatorname{card} k$ which then shows that $\operatorname{card} \operatorname{irr}(A) = \operatorname{card} \operatorname{Irr}(A) = \operatorname{card} k$.)

Theorem 26.20 (Density theorem, [Eti+11, Theorem 2.5])**.** Let k be algebraically closed.

a) If M is a finite-dimensional A-module then M is simple if and only if the canonical homomorphism $\Phi\colon A \to \operatorname{End}_k(M)$, $a \mapsto (m \mapsto am)$ is surjective.

b) Let $M_1, \dots, M_n$ be finite-dimensional pairwise non-isomorphic simple A-modules, and for every $i = 1, \dots, n$ let $\Phi_i\colon A \to \operatorname{End}_k(A)$ be the canonical homomorphism. Then the homomorphism of k-algebras

$$\Phi \coloneqq (\Phi_1, \dots, \Phi_n)\colon A \to \operatorname{End}_k(M_1) \times \cdots \times \operatorname{End}_k(M_n)$$

is surjective.

Proof.

a) For every two nonzero elements $m_1, m_2 \in M$ there exists some $f \in \operatorname{End}_k(M)$ with $f(m_1) = m_2$. This shows that M is simple as an $\operatorname{End}_k(M)$ module. If Φ is surjective then it follows that M is simple as an A-module.

If M is simple then $A' = \operatorname{End}_k(M) = k$ by Schur's Lemma, and it follows from Lemma 26.16 that $\operatorname{im}(\Phi) = A'' = \operatorname{End}_{A'}(M) = \operatorname{End}_k(M)$.

b) Let $f = (f_1, \dots, f_n) \in \prod_{i=1}^n \mathrm{End}_k(M_i)$. It follows from Corollary 26.17 that there exists for every $i = 1, \dots, n$ some element $e_i \in A$ with $\Phi_i(e_i) = \mathrm{id}_{M_i}$ for every $i = 1, \dots, n$ and $\Phi_j(e_i) = 0$ for every $j \neq i$. It follows from part a) that there exists for every $f_i \in \mathrm{End}_k(M_i)$ some $a_i \in A$ with $\Phi_i(a_i) = f_i$. We now have that $\Phi(a_1 e_1 + \dots + a_n e_n) = (f_1, \dots, f_n)$. □

Remark 26.21. Part a) of Theorem 26.20 is known as *Burnside's theorem* (*on matrix algebras*): It states that for an algebraically closed field k the only k-subalgebra $A \subseteq \mathrm{M}_n(k)$ for which k^n simple as an A-module (with respect to the action given by matrix-vector multiplication) is $\mathrm{M}_n(k)$ itself. More information on Burnside's theorem can be found in [Sha14].

The above proof of Burnside's thorem relies on the first Jacobson density theorem in the guise of the existence of projection operators, but Burnside's theorem can also be shown using the second Jacobson density theorem:

Alternative Proof of Burnside's theorem: We have $\mathrm{End}_A(k^n) = k$ by Schur's Lemma. The standard basis $e_1, \dots, e_n$ of k^n is therefore linearly independent over $\mathrm{End}_A(k^n)$. Let $M \in \mathrm{M}_n(k)$ and let $m_i \in k^n$ be the i-th column vector of M for every $i = 1, \dots, n$ It follows from the second Jacobson density theorem that there exists some $M' \in A$ with $M' e_i = m_i$ for every $i = 1, \dots, n$, and thus $M = M' \in A$. □

Remark 26.22. Burnside's theorem does not hold for non-algebraically closed fields: If k is not algebraically closed then there exists a finite field extension L/k of degree $\dim L > 1$. The L-vector space structure of L itself corresponds to an injective k-algebra homomorphism $\Phi\colon L \to \mathrm{End}_k(L)$, $l \mapsto (x \mapsto lx)$. It follows for the k-subalgebra $A \coloneqq \mathrm{im}(\Phi) \subsetneq \mathrm{End}_k(L)$ that L is a simple A-module because L is simple as an L-module. But the strict inequality

$$\dim A = \dim L < (\dim L)^2 = \dim \mathrm{End}_k(L)$$

shows that $\mathrm{im}(\Phi)$ is a proper subalgebra of $\mathrm{End}_k(L)$.

Corollary 26.23. If k is algebraically closed and $M_1, \dots, M_n$ are pairwise non-isomorphic finite-dimensional simple A-module then

$$\sum_{i=1}^n (\dim M_i)^2 \leq \dim A\,.$$

Proof. This follows from the density theorem because

$$\sum_{i=1}^n (\dim M_i)^2 \leq \dim \prod_{i=1}^n \mathrm{End}_k(M_i) \leq \dim A$$

by the surjectivity of $A \to \prod_{i=1}^n \mathrm{End}_k(M_i)$. □

Remark 26.24. Corollary 26.23 does not hold for non-algebraically closed fields: If k is not algebraically closed then there exists a finite field extension L/k of degree $\dim L > 1$. It then follows that $M = L$ is a simple L-module with

$$(\dim M)^2 = (\dim L)^2 > \dim L\,.$$

The Double Centralizer Theorem

Corollary 26.25 (Double Centralizer Theorem)**.** Let W be a finite-dimensional k-vector space and let $A \subseteq \operatorname{End}_k(W)$ be a semisimple k-subalgebra.

a) The centralizer A' is again a semisimple k-subalgebra of $\operatorname{End}_k(W)$.

b) We have that $A = A''$.

c) There exists a unique decomposition

$$W = W_1 \oplus \cdots \oplus W_r$$

into simple $(A' \otimes_k A)$-submodules, and this decomposition coincides with both the A-isotypical and the A'-isotypical decomposition of W.

d) Each $(A' \otimes_k A)$-submodule W_i is of the form $W_i \cong V_i' \otimes_{D_i} V_i$ for a simple A-module V_i, a simple A'-module V_i' and a division k-algebra D_i with $D_i \cong \operatorname{End}_A(V_i)$ and $D_i^{\mathrm{op}} \cong \operatorname{End}_{A'}(V_i')$. The modules V_i, V_i' and the division k-algebra D_i are unique up to isomorphism.

e) The summand W_i is both the E_i-isotypical and the E_i'-isotypical component of M.

f) The simple A-modules $V_1, \dots, V_n$ form a set of representatives for the isomorphism classes of simple A-modules, and the A'-modules $V_1', \dots, V_i'$ form a set of representatives for the isomorphism classes of simple A-modules.

   Thus the correspondence $V_i \leftrightarrow V_i'$ is a 1:1-correspondece $\operatorname{Irr}(A) \leftrightarrow \operatorname{Irr}(A')$.

Proof. This follows from the double centralizer theorem because W is the sum of only finitely many simple A-modules because W is finite-dimensional. □

27. Central Simple Algebras

Conventions 27.1. In this section k denotes a field and we abbreviate $\otimes \coloneqq \otimes_k$.

27.2. In this section we give a short introduction to central simple k-algebras.

Definition 27.3. A k-algebra A is *central* if $\mathrm{Z}(A) = k$.

Definition 27.4. A *central simple k-algebra* is a k-algebra A which is simple (as a ring) and central. The class of finite-dimensional central simple k-algebras is denoted by CSA_k.

Remark 27.5. Many (most?) authors reserve the notion of a “central simple k-algebra” for finite-dimensional central simple k-algebras. We will write $A \in \mathrm{CSA}_k$ if we want A to be finite-dimensional.

27.1. Tensor Products of CSA

Lemma 27.6. Let A, B be k-algebras and let $A' \subseteq A$, $B' \subseteq B$ be subalgebras. Then

$$\mathrm{Z}_{A \otimes B}(A' \otimes B') = \mathrm{Z}_A(A') \otimes \mathrm{Z}_B(B')\,.$$

Proof. We have for every simple tensor $a \otimes b \in \mathrm{Z}_A(A') \otimes \mathrm{Z}_B(B')$ that

$$(a \otimes b)(a' \otimes b') = (aa') \otimes (bb') = (a'a) \otimes (b'b) = (a' \otimes b')(a \otimes b)$$

for every simple tensor $a' \otimes b' \in A' \otimes B'$. It follows that $(a \otimes b)x = x(a \otimes b)$ for every $x \in A' \otimes B'$, which shows that

$$\mathrm{Z}_A(A') \otimes \mathrm{Z}_B(B') \subseteq \mathrm{Z}_{A \otimes B}(A' \otimes B')\,.$$

To show the other inclusion let $x \in \mathrm{Z}_{A \otimes B}(A' \otimes B')$. We may write $x = \sum_{i=1}^n a_i \otimes b_i$ and assume w.l.o.g. that both $a_1, \dots, a_n$ and $b_1, \dots, b_n$ are linearly independent. For every $a' \in A'$ we then have that

$$\sum_{i=1}^n (a'a_i) \otimes b_i = (a' \otimes 1)x = x(a' \otimes 1) = \sum_{i=1}^n (a_i a') \otimes b_i$$

and therefore that $a_i a' = a' a_i$ for every $i = 1, \dots, n$ because $b_1, \dots, b_n$ are linearly independent (see Recall A1.19). This shows that $a_1, \dots, a_n \in \mathrm{Z}_A(A')$. In the same way we find that $b_1, \dots, b_n \in \mathrm{Z}_B(B')$. Together this shows that $x \in \mathrm{Z}_A(A') \otimes \mathrm{Z}_B(B')$. □

Corollary 27.7. Let A and B be k-algebras. Then

$$Z(A \otimes B) = Z(A) \otimes Z(B)\,.$$

Proof. We have that $\mathrm{Z}(A \otimes B) = \mathrm{Z}_{A \otimes B}(A \otimes B) = \mathrm{Z}_A(A) \otimes \mathrm{Z}_B(B) = \mathrm{Z}(A) \otimes \mathrm{Z}(B)$. □

Lemma 27.8. Let A be a central simple k-algebra and B be a simple k-algebra. Then $A \otimes B$ is again simple.

Proof. It follows from $A, B \neq 0$ that $A \otimes B \neq 0$. Let $I \trianglelefteq A \otimes B$ be a non-zero two-sided ideal. Every $u \in I$ can be written as $u = \sum_{i=1}^n a_i \otimes b_i$ where $b_1, \dots, b_n \in B$ are linearly independent. Let $x \in I$ with $x \neq 0$ for which the number of summands n is minimal with respect to all nonzero elements in I. Let

$$x = a_1 \otimes b_1 + a_2 \otimes b_2 + \dots + a_n \otimes b_n \tag{27.1}$$

be such a sum.

We will modify x such that $a_1 = 1$: We have that $n \geq 1$ because x is nonzero and $a_1 \neq 0$ by the minimality of n. It follows that the two-sided ideal $Aa_1A \trianglelefteq A$ is nonzero, and therefore that $Aa_1A = A$ because A is simple. We thus have that $1 \in Aa_1A$ which is why $1 = \sum_{i=1}^m c_i a_1 c_i'$ for suitable coefficients $c_i, c_i' \in C$. We then have that $x' \in I$ for

$$x' \coloneqq \sum_{i=1}^m (c_i \otimes 1)x(c_i' \otimes 1) = 1 \otimes b_1 + a_2' \otimes b_2 + \dots + a_n' \otimes b_n$$

with $a'_2, \dots, a'_n \in A$. We have that $x' \neq 0$ because $b_1, \dots, b_n$ are linearly independent.

Now we show that x' is already of the form $x' = 1 \otimes b$ for some $b \in B$: For every $a \in A$ the element

$$(a \otimes 1)x' - x'(a \otimes 1) = (aa'_2 - a'_2 a) \otimes b_2 + \cdots + (aa'_n - a'_n a) \otimes b_2$$

is contained in I. It thus follows from the minimality of n that

$$(a \otimes 1)x' - x'(a \otimes 1) = 0\,.$$

Because $b_2, \dots, b_n$ are linearly independent it follows that $aa'_i - a'_i a = 0$ for all $a \in A$ and $i = 2 \dots, n$. We therefore have that $a'_2, \dots, a'_n \in Z(A) = k$. It follows that

$$\begin{aligned} x' &= 1 \otimes b_1 + a'_2 \otimes b_2 + \cdots + a'_n \otimes b_n \\ &= 1 \otimes b_1 + 1 \otimes (a'_2 b_2) + \cdots + 1 \otimes (a'_n b_n) \\ &= 1 \otimes (b_1 + a'_2 b_2 + \cdots + a'_n b_n) \\ &= 1 \otimes b \end{aligned}$$

with $b \coloneqq b_1 + a'_2 b_2 + \cdots + a'_n b_n \in B$.

We have that $b \neq 0$ because $x' \neq 0$, and it follows that $BbB = B$ because B is simple. We therefore have that

$$I \supseteq (1 \otimes B)x'(1 \otimes B) = (1 \otimes B)(1 \otimes b)(1 \otimes B) = 1 \otimes (BbB) = 1 \otimes B\,.$$

It follows that

$$I \supseteq (A \otimes 1)(1 \otimes B) = A \otimes B\,.$$

This shows that $A \otimes B$ is the only non-zero two-sided ideals in $A \otimes B$. □

Remark 27.9. It can be shown more generally that if A is a central simple k-algebra and B is any k-algebra then every two-sided ideal of $A \otimes B$ is of the form $A \otimes J$ for a two-sided ideal $J \trianglelefteq B$. A proof of this can be found in [Cla12, Lemma 4.1].

Warning 27.10. For simple k-algebras A, B their tensor product $A \otimes B$ does not need to be simple. A counterexample is given by

$$\begin{aligned} \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \otimes \mathbb{R}[X]/(X^2+1) \cong \mathbb{C}[X]/(X^2+1) &= \mathbb{C}[X]/((X-1)(X+1)) \\ &\cong \mathbb{C}[X]/(X-1) \times \mathbb{C}[X]/(X+1) \cong \mathbb{C} \times \mathbb{C} \end{aligned}$$

where we use the chinese reminder theorem for the second to last isomorphism.

Proposition 27.11. If A, B are central simple k-algebras then $A \otimes B$ is again a central simple k-algebra, and if $A, B \in \mathrm{CSA}_k$ then $A \otimes B \in \mathrm{CSA}_k$.

Proof. It follows from Corollary 27.7 that

$$\mathrm{Z}(A \otimes B) = \mathrm{Z}(A) \otimes \mathrm{Z}(B) = k \otimes k = k\,,$$

and $A \otimes B$ is simple by Lemma 27.8. If both A, B are finite-dimensional then $A \otimes B$ is also finite-dimensional. □

27.12. Let $\widetilde{\mathrm{Br}}_k \coloneqq \mathrm{CSA}_k/{\cong}$. We have shown that

$$[A] \cdot [B] \coloneqq [A \otimes B]$$

is a well-defined binary operation on $\widetilde{\mathrm{Br}}(k)$. This operation is also associative, commutative and we have that

$$[k] \cdot [A] = [k \otimes A] = [A]\,,$$

which shows that $[k]$ is neutral. Altogether we have thus endowed $\widetilde{\mathrm{Br}}(k)$ with the structure of a commutative monoid.

27.2. Brauer Equivalence

27.13. This subsection is very much inspired by [Cla12, 4.2].

Notation 27.14. The class of finite-dimensional central division k-algebras is denoted by CDA_k.

27.15. By Wedderburn's theorem every finite-dimensional simple k-algebra is isomorphic to $\mathrm{M}_n(D)$ where D is a finite-dimensional division k-algebra, which is unique up to isomorphism. It follows from Lemma 23.3 that

$$\mathrm{Z}(D) \cong \mathrm{Z}(\mathrm{M}_n(D)) \cong \mathrm{Z}(A) \cong k\,,$$

which shows that D is already a central division k-algebra. It follows that there exists a well-defined map

$$\mathrm{CSA}_k/{\cong} \to \mathrm{CDA}_k/{\cong}$$

wich maps $[A]$ to $[D]$. This map is surjective because every $D \in \mathrm{CDA}_k$ is in particular a central simple k-algebra, for which the isomorphism class $[D] = [\mathrm{M}_1(D)] \in \mathrm{CSA}_k/{\cong}$ is mapped to $[D] \in \mathrm{CDA}_k/{\cong}$.

Definition 27.16. Two finite-dimensionl central simple k-algebras $A, B \in \mathrm{CSA}_k$ are *Brauer equivalent* if for the central divsion k-algebras D_1, D_2 with $A \cong \mathrm{M}_n(D_1)$ and $B \cong \mathrm{M}_m(D_2)$ (for suitable n, m) we have that $D_1 \cong D_2$. Brauer equivalence is denoted by $\sim$.

Corollary 27.17. Brauer equivalence is an equivalence relation on CSA_k and the map

$$\mathrm{CSA}_k/{\sim} \to \mathrm{CDA}_k/{\cong}\,, \quad [\mathrm{M}_n(D)] \mapsto [D]$$

is a well-defined bijection.

Proof. For any $A, B \in \mathrm{CSA}_k$ we have that $A \sim B$ if and only if A and B are mapped to the same element by the composition

$$\mathrm{CSA}_k \to \mathrm{CSA}_k/{\cong} \to \mathrm{CDA}_k/{\cong}\,.$$

It follows that $\sim$ is an equivalence relation. The above composition is surjective and thus descends to the desired bijection. □

Remark 27.18. Isomorphic central simple k-algebras are Brauer equivalent. By abuse of notation we will refer to the equivalence relation induced by $\sim$ on $\mathrm{CSA}_k/{\cong} = \widetilde{\mathrm{Br}}(k)$ also as Brauer equivalence and write for $A, B \in \widetilde{\mathrm{Br}}(k)$ that $[A] \sim [B]$ if $A \sim B$.

Notation 27.19. The set of Brauer equivalence classes is denoted by

$$\mathrm{Br}(k) \coloneqq \mathrm{CSA}_k/{\sim}\,.$$

By abuse of notation we will identify $\mathrm{Br}(k)$ with $\widetilde{\mathrm{Br}}(k)/{\sim}$ via the mapping $[[A]] \mapsto [A]$.

Recall 27.20. Let M be a (multiplicatively written) monoid and let $\sim$ be an equivalence relation on M. Then $\sim$ is a *congruence relation* if for all $m, m', n, n' \in M$ with $m \sim m'$ and $n \sim n'$ it follows that

$$m \cdot n \sim m' \cdot n'\,.$$

The equivalence relation $\sim$ is a congruence relation if and only if on the set of equivalence classes $M/{\sim}$ the binary operation

$$[m] \cdot [n] = [m \cdot n]$$

is well-defined.

27.21. We will now show that $\sim$ is a congruence relation on $\widetilde{\mathrm{Br}}(k)$, and that the induced monoid structure on $\widetilde{\mathrm{Br}}(k)/{\sim} = \mathrm{Br}(k)$ is already a group structure.

Lemma 27.22. Let $n, m \geq 0$.

a) If D is a k-algebra then $\mathrm{M}_n(D) \cong D \otimes \mathrm{M}_n(k)$ as k-algebras.

b) We have that $\mathrm{M}_n(k) \otimes \mathrm{M}_m(k) \cong \mathrm{M}_{nm}(k)$ as k-algebras.

Proof.

a) There exists a unique k-linear map $\varphi\colon D \otimes \mathrm{M}_n(k) \to \mathrm{M}_n(D)$ which is on simple tensors given by $d \otimes M \mapsto dM$ by the universal property of the tensor product. Let E_{ij} be the standard D-basis of $\mathrm{M}_n(D)$ and let E'_{ij} be the standard k-basis of $\mathrm{M}_n(k)$. Then

$$D \otimes \mathrm{M}_n(k) = D \otimes \bigoplus_{i,j=1}^{n} kE_{ij} \cong \bigoplus_{i,j=1}^{n} D \otimes (kE_{ij})$$

as k-vector spaces and φ maps $D \otimes (kE_{ij})$ isomorphically onto DE_{ij}. This shows that φ is an isomorphism of k-vector spaces. The multiplicativity of φ can be checked on simple tensors, for which we have that

$$\begin{aligned} \varphi((d \otimes M)(d' \otimes M')) = \varphi((dd') \otimes (MM')) &= dd'MM' \\ &= dMd'M' = \varphi(d \otimes M)\varphi(d'M')\,. \end{aligned}$$

We also have that $\varphi(1 \otimes I) = I$.

b) We have that

$$\begin{aligned}\mathrm{M}_n(k) \otimes \mathrm{M}_m(k) &\cong \mathrm{End}_k(k^n) \otimes \mathrm{End}_k(k^m) \\ &\cong \mathrm{End}_k(k^n \otimes k^m) \cong \mathrm{End}_k(k^{nm}) \cong \mathrm{M}_{nm}(k)\end{aligned}$$

where the second isomorphism is given by $f \otimes g \mapsto f \otimes g$. □

Remark 27.23. The above isomorphism $\mathrm{M}_n(k) \otimes \mathrm{M}_m(k) \to \mathrm{M}_{nm}(k)$ can be expressed on simple tensors by the Kronecker product

$$\varphi\colon\ \mathrm{M}_n(k) \otimes \mathrm{M}_m(k) \to \mathrm{M}_{nm}(k), \quad A \otimes B \mapsto \begin{bmatrix} A_{11}B & \cdots & A_{1n}B \\ \vdots & \ddots & \vdots \\ A_{n1}B & \cdots & A_{nn}B \end{bmatrix}.$$

It can also be checked by hand that this k-linear map is an isomorphis of k-algebras: The basis $E_{ij} \otimes E_{i'j'}$ with $i, j = 1, \dots, n$ and $i', j' = 1, \dots, m$ of $\mathrm{M}_n(k) \otimes \mathrm{M}_m(k)$ is mapped bijectively onto the analogous standard basis of $\mathrm{M}_{mn}(k)$, which shows that φ is bijective. We have that

$$\begin{aligned}&\varphi(A \otimes B)\varphi(A' \otimes B')) \\ &= \begin{bmatrix} A_{11}B & \cdots & A_{1n}B \\ \vdots & \ddots & \vdots \\ A_{n1}B & \cdots & A_{nn}B \end{bmatrix} \cdot \begin{bmatrix} A'_{11}B' & \cdots & A'_{1n}B' \\ \vdots & \ddots & \vdots \\ A'_{n1}B' & \cdots & A'_{nn}B' \end{bmatrix} \\ &= \begin{bmatrix} \sum_{j=1}^n A_{1j}BA'_{j1}B' & \cdots & \sum_{j=1}^n A_{1j}BA'_{jn}B' \\ \vdots & \ddots & \vdots \\ \sum_{j=1}^n A_{nj}BA'_{j1}B' & \cdots & \sum_{j=1}^n A_{nj}BA'_{jn}B' \end{bmatrix} \\ &= \begin{bmatrix} \sum_{j=1}^n A_{1j}A'_{j1}BB' & \cdots & \sum_{j=1}^n A_{1j}A'_{jn}BB' \\ \vdots & \ddots & \vdots \\ \sum_{j=1}^n A_{nj}A'_{j1}BB' & \cdots & \sum_{j=1}^n A_{nj}A'_{jn}BB' \end{bmatrix} \\ &= \begin{bmatrix} (AA')_{11}BB' & \cdots & (AA')_{1n}BB' \\ \vdots & \ddots & \vdots \\ (AA')_{n1}BB' & \cdots & (AA')_{nn}BB' \end{bmatrix} \\ &= \varphi((AA') \otimes (BB')) = \varphi((A \otimes B)(A' \otimes B'))\end{aligned}$$

for all simple tensors $A \otimes B, A' \otimes B' \in \mathrm{M}_n(k) \otimes \mathrm{M}_m(k)$, which shows that φ is multiplicative. We also have that $\varphi(I \otimes I) = I$.

Lemma 27.24. For $A, B \in \mathrm{CSA}_k$ the following are equivalent:

a) We have that $A \sim B$, i.e. there exist $n, m \geq 1$ and division k-algebras $D_1 \cong D_2$ with $A \cong \mathrm{M}_n(D_1)$ and $B \cong \mathrm{M}_m(D_2)$ as k-algebras.

b) There exist $n, m \geq 1$ and a division k-algebra D such that $A \cong \mathrm{M}_n(D)$ and $B \cong \mathrm{M}_m(D)$ as k-algebras.

c) There exists $n', m' \geq 1$ with $A \otimes \mathrm{M}_{n'}(k) \cong B \otimes \mathrm{M}_{m'}(k)$ as k-algebras.

Proof.

a) $\Longrightarrow$ b) Choose $D = D_1$.

b) $\Longrightarrow$ c) We can choose $n' = m$ and $m' = n$ because

$$\begin{aligned} A \otimes \mathrm{M}_m(k) &\cong \mathrm{M}_n(D) \otimes \mathrm{M}_m(k) \cong D \otimes \mathrm{M}_n(k) \otimes \mathrm{M}_m(k) \\ &\cong D \otimes \mathrm{M}_m(k) \otimes \mathrm{M}_n(k) \cong \mathrm{M}_m(D) \otimes \mathrm{M}_n(k) \cong B \otimes \mathrm{M}_n(k) \,. \end{aligned}$$

c) $\Longrightarrow$ a) Let D_1, D_2 be division k-algebras with $A \cong \mathrm{M}_n(D_1)$ and $B \cong \mathrm{M}_m(D_2)$ as k-algebras. Then

$$\begin{aligned} A \otimes \mathrm{M}_{n'}(k) \cong \mathrm{M}_n(D_1) \otimes \mathrm{M}_{n'}(k) &\cong D_1 \otimes \mathrm{M}_n(k) \otimes \mathrm{M}_{n'}(k) \\ &\cong D_1 \otimes \mathrm{M}_{nn'}(k) \cong \mathrm{M}_{nn'}(D_1) \end{aligned}$$

and similarly

$$B \otimes \mathrm{M}_{m'}(k) \cong \mathrm{M}_{mm'}(D_2) \,.$$

It follows from $\mathrm{M}_{nn'}(D_1) \cong \mathrm{M}_{mm'}(D_2)$ and the theorem of Artin–Wedderburn that $D_1 \cong D_2$ as k-algebras (and that $nn' = mm'$). □

Corollary 27.25. Brauer equivalence is an congruence relation on $\widetilde{\mathrm{Br}}(k)$, i.e. for $A, A', B, B' \in \mathrm{CSA}_k$ with $A \sim A'$ and $B \sim B'$ we have that $A \otimes B \sim A' \otimes B'$.

Proof. There exist $n, n', m, m' \geq 1$ with

$$A \otimes \mathrm{M}_n(k) \cong A' \otimes \mathrm{M}_{n'}(k) \quad \text{and} \quad B \otimes \mathrm{M}_m(k) \cong B' \otimes \mathrm{M}_{m'}(k)$$

by Lemma 27.24. It follows that

$$\begin{aligned} A \otimes B \otimes \mathrm{M}_{nm}(k) &\cong A \otimes B \otimes \mathrm{M}_n(k) \otimes \mathrm{M}_m(k) \\ &\cong A \otimes \mathrm{M}_n(k) \otimes B \otimes \mathrm{M}_m(k) \\ &\cong A' \otimes \mathrm{M}_{n'}(k) \otimes B' \otimes \mathrm{M}_{m'}(k) \\ &\cong A' \otimes B' \otimes \mathrm{M}_{n'}(k) \otimes \mathrm{M}_{m'}(k) \\ &\cong A' \otimes B' \otimes \mathrm{M}_{n'm'}(k) \,, \end{aligned}$$

which shows that $A \otimes B \sim A' \otimes B'$ by Lemma 27.24. □

Lemma 27.26. Let A be a central simple k-algebra.

a) The algebra A^{op} is again a central simple k-algebra and if $A \in \mathrm{CSA}_k$ then $A^{\mathrm{op}} \in \mathrm{CSA}_k$.

b) If $A \in \mathrm{CSA}_k$ then $A \otimes A^{\mathrm{op}} \cong \mathrm{End}_k(A)$ as k-algebras.

Proof.

a) The two-sided ideals of A^{op} are precisely the two-sided ideals of A, of which there are precisely two, and $\mathrm{Z}(A^{\mathrm{op}}) = \mathrm{Z}(A) = k$. If A is finite-dimensional then so is A^{op} because $\dim_k(A^{\mathrm{op}}) = \dim_k(A)$.

b) The left A-module structure of A itself corresponds to a k-algebra homomorphism $f\colon A \to \mathrm{End}_k(A)$ with $f(a)(x) = ax$ for all $a \in A$, $x \in A$. The right A-module structure of A itself corresponds to a left A^{op}-module structure of A, which in turn corresponds to a k-algebra homomorphism $f\colon A^{\mathrm{op}} \to \mathrm{End}_k(A)$ given by $f(b^{\mathrm{op}})(x) = xb$ for all $b \in A$, $x \in A$. Then f, g induce a well-defined k-linear map

$$\varphi\colon A \otimes A^{\mathrm{op}} \to \mathrm{End}_k(A)$$

which is given on simple tensors by

$$\varphi(a \otimes b^{\mathrm{op}})(x) = (f(a) \circ g(b^{\mathrm{op}}))(x) = axb$$

for all $a \otimes b^{\mathrm{op}} \in A \otimes A^{\mathrm{op}}$, $x \in A$. For all simple tensors $a_1 \otimes b_1^{\mathrm{op}}, a_2 \otimes b_2^{\mathrm{op}} \in A \otimes A^{\mathrm{op}}$ we have that

$$\begin{aligned}
\varphi(a_1 \otimes b_1^{\mathrm{op}})\varphi(a_2 \otimes b_2^{\mathrm{op}}) &= f(a_1) \circ g(b_1^{\mathrm{op}}) \circ f(a_2) \circ g(b_2^{\mathrm{op}}) \\
&= f(a_1) \circ f(a_2) \circ g(b_1^{\mathrm{op}}) \circ g(b_2^{\mathrm{op}} \\
&= f(a_1 a_2) \circ g(b_1^{\mathrm{op}} b_2^{\mathrm{op}}) \\
&= \varphi((a_1 a_2) \otimes (b_1^{\mathrm{op}} b_2^{\mathrm{op}})) \\
&= \varphi((a_1 \otimes b_1^{\mathrm{op}})(a_2 \otimes b_2^{\mathrm{op}}))
\end{aligned}$$

where we use for the second equality that $g(b_1^{\mathrm{op}})$ and $f(a_2)$ commute by the associativity of the multiplication of A. We also have that $\varphi(1 \otimes 1) = \mathrm{id}_A$.

Altogether this shows that φ is a homomorphism of k-algebras. The kernel $\ker(\varphi)$ is a nonzero two-sided ideal in the central simple k-algebra $A \otimes A^{\mathrm{op}}$. It follows that $\ker(\varphi) = 0$ which shows that φ is injective. We have that

$$\dim_k(A \otimes A^{\mathrm{op}}) = \dim_k(A)\dim_k(A^{\mathrm{op}}) = \dim_k(A)^2 = \dim_k \mathrm{End}_k(A)\,,$$

so it follows that φ is already an isomorphism. □

Example 27.27. The quaternions algebra $\mathbb{H}$ is a four-dimensional central simple $\mathbb{R}$-algebra and the quaternion conjugation $\mathbb{H} \to \mathbb{H}^{\mathrm{op}}$, $x \mapsto \overline{x}^{\mathrm{op}}$ is an isomorphism of $\mathbb{R}$-algebras. It follows that

$$\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H} \cong \mathbb{H} \otimes_{\mathbb{R}} \mathbb{H}^{\mathrm{op}} \cong \mathrm{End}_{\mathbb{R}}(\mathbb{H}) \cong \mathrm{M}_4(\mathbb{R})\,.$$

Theorem 27.28. The binary operation

$$[A] \cdot [B] \coloneqq [A \otimes B]$$

defines on $\mathrm{Br}(k)$ the structure of an abelian group. The neutral element is given by $[k]$ and the inverse of $[A] \in \mathrm{Br}(k)$ is given by $[A^{\mathrm{op}}]$.

Proof. Brauer equivalence is a congruence relation on $\widetilde{\mathrm{Br}}(k)$ by Corollary 27.25, from which it follows that this binary operation on $\mathrm{Br}(k)$ is well-defined. Since $\widetilde{\mathrm{Br}}(k)$ is a commutative monoid the same holds for $\mathrm{Br}(k)$. The neutral element of $\mathrm{Br}(k)$ is $[k]$. For every $[A] \in \mathrm{Br}(k)$ with $n = \dim_k A$ we have that

$$[A] \cdot [A^{\mathrm{op}}] = [A \otimes A^{\mathrm{op}}] = [\mathrm{End}_k(A)] = [\mathrm{M}_n(k)] = [k]\,,$$

which shows that $[A^{\mathrm{op}}]$ is inverse to $[A]$ in $\mathrm{Br}(k)$. □

Definition 27.29. The group $\mathrm{Br}(k)$ as described in Theorem 27.28 is the *Brauer group* of the field k.

Example 27.30.

a) If k is algebraically closed then every finite-dimensional division k-algebra is already k itself. It follows that the Brauer group $\mathrm{Br}(k)$ is trivial.

b) It is a classical result due to Frobenius that the only finite-dimensional division $\mathbb{R}$-algebras are $\mathbb{R}, \mathbb{C}, \mathbb{H}$. Both $\mathbb{R}$ and $\mathbb{H}$ are central, while $\mathbb{C}$ is not. It follows that $\mathrm{CDA}/{\cong} = [\mathbb{R}], [\mathbb{H}]$ has two elements. The Brauer group $\mathrm{Br}(\mathbb{R})$ is therefore the cyclic group of order two.

c) A theorem of Wedderburn (which is not to be confused with Wedderburn's theorem) states that every finite skew field is already commutative, and thus a field. It follows that for a finite field k the only central finite-dimensional division k-algebra is k itself. It follows that the Brauer group $\mathrm{Br}(k)$ is trivial.

27.3. The Skolem–Noether Theorem

27.31. The main ideas of this section are taken from [Cla12, 4.3]

Example 27.32. As a motivation for the upcoming theorem and its proof we first consider a special case:

Let $n \geq 1$ and let $\alpha\colon \mathrm{M}_n(k) \to \mathrm{M}_n(k)$ be a k-algebra automorphism. The usual matrix-vector multiplication makes k^n into a simple $\mathrm{M}_n(k)$-module which we will denote by M. By using the automorphism α we can "twist" this module structure, resulting in a $\mathrm{M}_n(k)$-module M_α whose underlying k-vector space is again k^n but whose multiplication is given by

$$A * x := \varphi(A)x$$

for all $A \in \mathrm{M}_n(k)$, $x \in k^n$. It follows from the surjectivity of α that M_α is also simple.

The k-algebra $\mathrm{M}_n(k)$ has only one simple module up to isomorphism (namely M), so it follows that $M \cong M_\alpha$. If $f\colon M \to M_\alpha$ is such an isomorphism then f is in particular k-linear and therefore given by multiplication with some invertible matrix $S \in \mathrm{GL}_n(k)$. The inverse f^{-1} is then given by multiplication with S^{-1}

It follows for every $A \in \mathrm{M}_n(k)$ that

$$\alpha(A)x = A * x = f(Af^{-1}(x)) = SAS^{-1}x$$

for every $x \in k^n$, and therefore that $\alpha(A) = SAS^{-1}$. We have thus found that α is an inner automorphism, given by conjugation with the unit $S \in \mathrm{M}_n(k)^\times$.

Lemma 27.33. If A is a finite-dimensional simple k-algebra and M, N are finite-dimensional A-module then M, N are isomorphic as A-modules if and only if they have the same k-dimension.

Proof. The algebra A is semisimple and there exists only one simple A-module E up to isomorphism, for which it follows from the finite-dimensionality of A that it is also finite-dimensional. It follows for $M \cong E^{\oplus m}$ and $N \cong N^{\oplus n}$ that

$$\dim_k M = m \dim_k E \qquad \text{and} \qquad \dim_k N = n \dim_k E$$

and therefore that

$$M \cong N \iff m = n \iff \dim_k M = \dim_k N$$

by the uniqueness of multiplicities. □

Corollary 27.34. If A is a finite-dimensional simple k-algebra then any two k-algebra homomorphisms $f, g \colon A \to \mathrm{M}_n(k)$ are conjugated, i.e. there exists some $S \in \mathrm{GL}_n(k)$ with $g(a) = Sf(a)S^{-1}$ for every $a \in A$.

Proof. The homomorphisms f, g correspond to A-module structures on k^n given by

$$a \cdot x = f(a)x \qquad \text{and} \quad a * x = g(a)x$$

for all $a \in A$, $x \in k^n$. We denote the resulting A-modules by M_f and M_g. It follows from Lemma 27.33 that M_f and M_g are isomorphic as A-modules. It follows in the same way as in Example 27.32 that there exists some $S \in \mathrm{GL}_n(k)$ with $g(a) = Sf(a)S^{-1}$ for every $a \in A$. □

Theorem 27.35 (Skolem–Noether)**.** Let A be a simple k-algebra and let B be a finite-dimensional central simple k-algebra Then any two k-algebra homomorphisms $f, g \colon A \to B$ are conjugated, i.e. there exists a unit $u \in B^\times$ with $g(a) = uf(a)u^{-1}$ for every $a \in A$.

Proof. The k-algebra A must also be finite-dimensional: The kernel $\ker(f)$ is a proper two-sided ideal of A because $B \neq 0$. It follows that $\ker(f) = 0$ and therefore that $\dim_k B \leq \dim_k A$ by the injectivity of f

By observing that $B \otimes B^{\mathrm{op}} \cong \mathrm{End}_k(B)$ we can now apply Corollary 27.34 to the extended k-algebra homomorphisms

$$f \otimes \mathrm{id}, g \otimes \mathrm{id} \colon A \otimes B^{\mathrm{op}} \to B \otimes B^{\mathrm{op}}$$

to conclude that $f \otimes \mathrm{id}$ and $g \otimes \mathrm{id}$ are conjugated: There exists some $x \in B \otimes B^{\mathrm{op}}$ with

$$g(a) \otimes b = x(f(a) \otimes b)x^{-1} \tag{27.2}$$

for all $a \in A$, $b \in B^{\mathrm{op}}$. By setting $a = 1$ we find that

$$1 \otimes b = x(1 \otimes b)x^{-1}$$

for all $b \in B$, which shows that $x, x^{-1} \in \mathrm{Z}_{B \otimes B^{\mathrm{op}}}(1 \otimes B^{\mathrm{op}}) = \mathrm{Z}_{B \otimes B^{\mathrm{op}}}(k \otimes B^{\mathrm{op}})$. It follows from Lemma 27.6 that

$$\mathrm{Z}_{B \otimes B^{\mathrm{op}}}(k \otimes B^{\mathrm{op}}) = \mathrm{Z}_B(k) \otimes \mathrm{Z}_{B^{\mathrm{op}}}(B^{\mathrm{op}}) = \mathrm{Z}_B(k) \otimes \mathrm{Z}(B^{\mathrm{op}}) = B \otimes k\,.$$

We therefore have that $x = u \otimes 1$ and $x^{-1} = u' \otimes 1$ for some $u, u' \in B$. It follows from

$$1 \otimes 1 = xx^{-1} = (u \otimes 1)(u' \otimes 1) = (uu') \otimes 1$$

that $uu' = 1$ and similarly that $u'u = 1$. This shows that $u \in B^{\times}$ is a unit with $u' = u^{-1}$. By setting $b = 1$ in (27.2) we find that

$$g(a) \otimes 1 = (u \otimes 1)(f(a) \otimes 1)(u^{-1} \otimes 1) = (uf(a)u^{-1}) \otimes 1$$

and therefore $g(a) = uf(a)u^{-1}$ for every $a \in A$. □

Corollary 27.36. Every k-algebra automorphism of a finite-dimensional central simple k-algebra A is inner, i.e. given by conjugation with an element $u \in A^{\times}$.

Proof. Every automorphism is conjugated to the identity id_A by the Skolem–Noether theorem. □

Corollary 27.37. If A is a finite-dimensional central simple k-algebra then

$$\mathrm{Aut}_{k\text{-}\mathbf{Alg}}(A) \cong A^{\times} / \mathrm{Z}(A)^{\times}$$

where $[u] \in A^{\times} / \mathrm{Z}(A)^{\times}$ acts on A by conjugation.

Proof. The map

$$A^{\times} \to \mathrm{Aut}_{k\text{-}\mathbf{Alg}}(A), \quad [u] \mapsto (a \mapsto uau^{-1})$$

is a group homomorphisms which is surjective by Corollary 27.36. Its kernel is given by

$$A^{\times} \cap \mathrm{Z}(A) = \mathrm{Z}(A)^{\times}$$

because for every $u \in \mathrm{Z}(A)$ which is a unit in A its inverse u^{-1} is again central. □

Example 27.38. We have that $\mathrm{M}_n(k)^{\times} = \mathrm{GL}_n(k)$. We also have that $\mathrm{Z}(\mathrm{M}_n(k)) = kI$ by Lemma 23.3, and therefore that $\mathrm{Z}(\mathrm{M}_n(k))^{\times} = k^{\times} I$. It follows that

$$\mathrm{Aut}_{k\text{-}\mathbf{Alg}}(\mathrm{M}_n(k)) \cong \mathrm{GL}_n(k)/(k^{\times} I) = \mathrm{PGL}_n(k)$$

where $\mathrm{PGL}_n(k)$ acts on $\mathrm{M}_n(k)$ by conjugation.

Remark 27.39. The Skolem–Noether theorem can be used to give a short and otherwise self-contained proof of the aforementioned theorem of Frobenius that $\mathbb{R}, \mathbb{C}, \mathbb{H}$ are the only finite-dimensional divison $\mathbb{R}$-algebras up to isomorphism. We will not give this proof here but refer to [Kna16, Theorem 2.50].

28. Modules over Tensor Products

Conventions 28.1. In the following k denotes a field and A, B are two k-algebras. We abbreviate $\otimes_k =: \otimes$.

28.2. The tensor product $A \otimes B$ is again a k-algebra with multiplication given by

$$(a_1 \otimes b_1) \cdot (a_2 \otimes b_2) = (a_1 a_2) \otimes (b_1 b_2) .$$

for all simple tensors $a_1 \otimes b_1, a_2 \otimes b_2 \in A \otimes B$, as explained in A1.26. The two maps

$$\begin{aligned} A &\to A \otimes B, \quad a \mapsto a \otimes 1 , \\ B &\to A \otimes B, \quad b \mapsto 1 \otimes b \end{aligned}$$

are injective k-algebra homomorphism. We may therefore regard A and B as k-subalgebras of $A \otimes B$ by identifying them with $A \otimes 1$ and $1 \otimes B$.

Note that when we identify an element $a \in A$ with $a \otimes 1 \in A \otimes B$ and an element $b \in B$ with $1 \otimes b \in A \otimes B$ then the "the elements a and b commute in $A \otimes B$" in the sense that

$$(a \otimes 1)(1 \otimes b) = a \otimes b = (1 \otimes b)(a \otimes 1) .$$

This observations leads to the following:

28.3. Let C be another k-algebra.

If $f \colon A \otimes B \to C$ is a homomorphism of k-algebras then the restrictions of f to A and B result in k-algebra homomorphisms

$$\begin{aligned} f_1 \colon A &\to C, \quad a \mapsto f(a \otimes 1) , \\ f_2 \colon B &\to C, \quad b \mapsto f(1 \otimes b) . \end{aligned}$$

The images of f_1 and f_2 commute with each other in the sense that

$$\begin{aligned} f_1(a) f_2(b) = f(a \otimes 1) f(1 \otimes b) &= f((a \otimes 1)(1 \otimes b)) = f(a \otimes b) \\ &= f((1 \otimes b)(a \otimes 1)) = f(1 \otimes b) f(a \otimes 1) = f_2(b) f_1(a) \end{aligned}$$

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

Suppose on the other hand that $f_1 \colon A \to C$ and $f_2 \colon B \to C$ are two k-algebra homomorphisms with

$$f_1(a) f_2(b) = f_2(b) f_1(a)$$

for all $a \in A$, $b \in B$. It then follows that the k-linear map

$$f \colon A \otimes B \to C, \quad a \otimes b \mapsto f_1(a) f_2(b)$$

is a homomorphism of k-algebras because $f(1 \otimes 1) = 1$ and

$$\begin{aligned} f(a \otimes b) f(a' \otimes b') &= f_1(a) f_2(b) f_1(a') f_2(b') = f_1(a) f_1(a') f_2(b) f_2(b') \\ &= f_1(aa') f_2(bb') = f((aa') \otimes (bb')) = f((a \otimes b)(a' \otimes b')) \end{aligned}$$

for all simple tensors $a \otimes b, a' \otimes b' \in A \otimes B$.

These two constructions are mutually inverse. This shows that a k-algebra homomorphism $A \otimes B \to C$ is "the same" as a pair of k-algebra homomorphisms $A \to C$, $B \to C$ whose images commute with each other.

Remark 28.4. The above discussions shows that if A, B are commutative then $A \otimes B$ is the coproduct of A and B in the category of commutative k-algebras.

28.5. If P is a k-vector space then $(A \otimes B)$-module structures on P are in 1:1-correspondence with k-algebra homomorphisms $A \otimes B \to \operatorname{End}_k(P)$, where for every k-algebra homomorphism $f \colon A \otimes B \to \operatorname{End}_k(P)$ the corresponding module structure is given by

$$(a \otimes b) \cdot p = f(a \otimes b)(p)$$

for every simple tensor $a \otimes b \in A \otimes B$ and every $p \in P$. It follows from 28.3 that a $(A \otimes B)$-module structure on P is "the same" as a pair of commuting A-module an B-module structures on P.

Let's be more explicit: Every $(A \otimes B)$-module structure on P restricts to A- and B-module structures on P given by

$$a \cdot p = (a \otimes 1)p \quad \text{and} \quad b \cdot p = (1 \otimes b)p$$

for all $a \in A$, $b \in B$, $p \in P$. These actions of A, B on P commute in the sense that

$$\begin{aligned} a \cdot (b \cdot p) &= (a \otimes 1) \cdot ((1 \otimes b) \cdot p) = ((a \otimes 1)(1 \otimes b)) \cdot p \\ &= (a \otimes b) \cdot p = ((1 \otimes b)(a \otimes 1)) \cdot p = (1 \otimes b) \cdot ((a \otimes 1) \cdot p) = b \cdot (a \cdot p) \end{aligned}$$

for all $a \in A$, $b \in B$, $p \in P$. If on the other hand P carries both an A-module structure and a B-module structure such that

$$a \cdot (b \cdot p) = b \cdot (a \cdot p)$$

for all $a \in A$, $b \in B$, $p \in P$, then

$$(a \otimes b) \cdot p = a \cdot (b \cdot p) = b \cdot (a \cdot p)$$

for all simple tensors $a \otimes b \in A \otimes B$ and all $p \in P$ defines an $(A \otimes B)$-module structure on P: We have that $(1 \otimes 1) \cdot p = p$ for every $p \in P$, and for all simple tensors $a \otimes b, a' \otimes b' \in A \otimes B$ and all $p \in P$ we have that

$$\begin{aligned} (a \otimes b) \cdot ((a' \otimes b') \cdot p) &= a \cdot (b \cdot (a' \cdot (b' \cdot p))) = a \cdot (a' \cdot (b \cdot (b' \cdot p))) \\ &= (aa') \cdot ((bb') \cdot p) = ((aa') \otimes (bb')) \cdot p = ((a \otimes a')(b \otimes b')) \cdot p \,. \end{aligned}$$

With this we have seen that the following data are equivalent:

a) An $(A \otimes B)$-module structure on A.

b) A pair of commuting A-module and B-module structures on A.

c) A k-algebra homomorphism $A \otimes B \to \operatorname{End}_k(P)$.

d) A pair of k-algebra homomorphisms $A \to \operatorname{End}_k(P)$ and $B \to \operatorname{End}_k(P)$ whose images commute with each other.

We can also give yet another description of $(A \otimes B)$-modules: A pair of A-module and B-module structures on P commute if and only if for every $a \in A$ the map $P \to P$, $p \mapsto ap$ is a homomorphism of B-modules, and equivalently if for every $b \in B$ the map $P \to P$, $p \mapsto bp$ is a homomorphism of A-modules. This is equivalent to the k-algebra homomorphisms $A \to \operatorname{End}_k(P)$ restricting to a homomorphism $A \to \operatorname{End}_B(P)$, and equivalently to the k-algebra homomorphisms $B \to \operatorname{End}_k(P)$ restricting to a homomorphism $B \to \operatorname{End}_A(P)$. With this we can continue the above list:

e) An A-module structure on P and a k-algebra homomorphism $B \to \operatorname{End}_A(P)$.

f) A B-module structure on P and a k-algebra homomorphism $A \to \operatorname{End}_B(P)$.

28.6. Let M be an A-module and let N be an B-module. Then the tensor product $M \otimes N$ carries the structure of an A-module via

$$a \cdot (m \otimes n) = (am) \otimes n$$

for all $a \in A$ and simple tensors $m \otimes n \in M \otimes N$, as well as the structure of an B-module via

$$b \cdot (m \otimes n) = m \otimes (bn)$$

for all $b \in B$ and simple tensors $m \otimes n \in M \otimes N$. These two module structures commute because

$$a \cdot (b \cdot (m \otimes n)) = (am) \otimes (bn) = b \cdot (a \cdot (m \otimes n))$$

for all $a \in A$, $b \in B$, $m \otimes n \in M \otimes N$. It follows from 28.5 that $M \otimes N$ carries the structure of an $(A \otimes B)$-module via

$$(a \otimes b) \cdot (m \otimes n) = (am) \otimes (bn)$$

for all simple tensors $a \otimes b \in A \otimes B$ and $m \otimes n \in M \otimes N$. We will denote this $(A \otimes B)$-module by

$$M \boxtimes N \,.$$

Note that $A \otimes B = A \boxtimes B$ as $(A \otimes B)$-modules.

Lemma 28.7. If M is an A-module and N is a B-module such that $M \boxtimes N$ is simple as an $(A \otimes B)$-module then both M and N are simple.

Proof. It follows that $M, N \neq 0$ because $M \boxtimes N \neq 0$. If M were not simple then there would exist a proper nonzero A-submodule $M' \lneq M$. Then $M' \boxtimes N$ would be a proper nonzero $(A \otimes B)$-submodule of $M \boxtimes N$, which would contradict $M \boxtimes N$ being simple. This shows that M is simple and we find in the same way that N is simple. □

Lemma 28.8. If k is algebraically closed, M is a finite-dimensional simple A-module and N is a finite-dimensional simple B-module then the $(A \otimes B)$-module $M \boxtimes N$ is also simple.

Proof. By the density theorem the k-algebra homomorphisms $\Phi\colon A \to \operatorname{End}_k(M)$ and $\Psi\colon B \to \operatorname{End}_k(M)$ corresponding to the module structures are surjective. It follows that the k-algebra homomorphism

$$\Phi \otimes \Psi\colon A \otimes B \to \operatorname{End}_k(M) \otimes \operatorname{End}_k(N) \xrightarrow[f\otimes g \mapsto f \otimes g]{\sim} \operatorname{End}_k(M \otimes N)$$

is also surjective. This is the k-algebra homomorphism corresponding to the module structure of $M \boxtimes N$ so it follows from the density theorem that $M \boxtimes N$ is simple. □

Warning 28.9. Lemma 28.8 does not hold for non-algebraically closed fields: If k is not algebraically closed then there exists a finite-dimensional field extension L/k of degree $\dim_k L > 1$. Then L itself is simple as an L-module, but $L \otimes L$ is not simple as an $(L \otimes L)$-module: The kernel of the multiplication map $m\colon L \otimes L \to L$, $x \otimes y \to xy$ is a proper nonzero ideal because m is surjective but for dimension reasons not injective. Thus $\ker(m)$ is a proper nonzero $(L \otimes L)$-submodule of $L \otimes L$.

Corollary 28.10. Let k be algebraically closed.

a) Let M be a semisimple finite-dimensional A-module and let N be a semisimple finite-dimensional B-module. Then $M \boxtimes N$ is semisimple as an $(A \otimes B)$-module.

b) If A, B are finite-dimensional and semisimple then $A \otimes B$ is again semisimple.

Proof.

a) Let $M = \bigoplus_{i=1}^m M_i$ and $N = \bigoplus_{j=1}^n N_j$ be a decomposition into simple submodules. Then

$$M \boxtimes N = \left(\bigoplus_{i=1}^m M_i \right) \boxtimes \left(\bigoplus_{j=1}^n N_j \right) = \bigoplus_{i=1}^m \bigoplus_{j=1}^n M_i \boxtimes N_j$$

is a decomposition of $M \boxtimes N$ into simple $(A \otimes B)$-submodules.

b) This follows from part a) because $A \otimes B = A \boxtimes B$ as $(A \otimes B)$-modules. □

Warning 28.11. The tensor product of two finite-dimensional semisimple k-algebras is in general not again semisimple:

Consider the field $k = \mathbb{F}_p(t)$ with p prime. The polynomial $f \in k[X]$ given by $f(X) = X^p - t$ is irreducible and the finite field extension $L := k[X]/f$ is a finite-dimensional semisimple k-algebra. If $L \otimes L$ were again semisimple then

$$L \otimes L \cong k_1 \times \cdots \times k_n$$

for some fields $k_1, \dots, k_n$ by the theorem of Artin–Wedderburn because $L \otimes L$ is commutative. But it follows for the root $\alpha := \overline{X} \in L$ of f that

$$f(X) = X^p - t = X^p - \alpha^p = (X - \alpha)^p$$

and therefore that

$$L \otimes L = L \otimes k[X]/f \cong L[X]/f = L[X]/(X-\alpha)^p\,.$$

It follows that $L \otimes L$ contains nonzero nilpotent elements, which contradicts the isomorphism $L \cong k_1 \times \cdots \times k_n$.

Remark 28.12. It can be shown that if A is a finite-dimensional semisimple k-algebra and L/k is a finite seperable field extension then $L \otimes A$ is again semisimple. A proof of this can be found in [Lan05, XVII, Theorem 6.2].

Theorem 28.13. If k is algebraically closed then the map

$$\Phi\colon \operatorname{irr}(A) \times \operatorname{irr}(B) \to \operatorname{irr}(A \otimes B), \quad ([M],[N]) \mapsto [M \boxtimes N]$$

is a well-defined bijection. In other words, every finite-dimensional simple $(A \otimes B)$-module is up to isomorphism of the form $M \boxtimes N$ for a finite-dimensional simple A-module M and a finite-dimensional simple B-module N, and M, N are unique up to isomorphism.

Proof. That Φ is well-defined follows from Lemma 28.8.

To see that Φ is injective let $[M],[M'] \in \operatorname{irr}(A)$ and $[N],[N'] \in \operatorname{irr}(B)$ such that $M \boxtimes N \cong M' \boxtimes N'$. Then $M \boxtimes N \cong M' \boxtimes N'$ as A-modules where A acts on $M \boxtimes N$ via $a \cdot (m \otimes n) = (am) \otimes n$ for all $a \in A$ and simple tensors $m \otimes n \in M \otimes N$, and similarly for $M' \boxtimes N'$. We then have that

$$M \boxtimes N \cong \underbrace{M \oplus \cdots \oplus M}_{\dim(N) \text{ many}}$$

and

$$M' \boxtimes N' \cong \underbrace{M' \oplus \cdots \oplus M'}_{\dim(N') \text{ many}}$$

as A-modules. It then follows that $M \cong M'$ as A-modules because M, M' are simple. It can be shown in the same way that $N \cong N'$ as B-modules.

To see that Φ is surjective let $[P] \in \operatorname{irr}(A \otimes B)$. We can regard P as a B-module by restriction, i.e. via the action given by

$$b \cdot p = (1 \otimes b)p$$

for all $b \in B$, $p \in P$. Then P is a finite-dimensional B-module and therefore contains a simple B-submodule $N \leq P$. It follows from Proposition 22.53 that the evaluation map

$$\psi\colon \operatorname{Hom}_B(N,P) \otimes N \to P, \quad f \otimes n \mapsto f(n)$$

is a homomorphis of B-modules which restrict to an isomorphism $\operatorname{Hom}_B(N,P) \to N_P$, where B acts on $\operatorname{Hom}_B(N,P) \otimes N$ via

$$b \cdot (f \otimes n) = f \otimes (bn)$$

for all $b \in B$ and simple tensors $f \otimes n \in \operatorname{Hom}_B(N, P) \otimes N$.

The $(A \otimes B)$-module structure on P also corresponds to a k-algebra homomorphism $A \to \operatorname{End}_B(P)$ given by $b \mapsto (p \mapsto bp)$ as seen in 28.5. The multiplicity space $\operatorname{Hom}_B(N, P)$ carries the structure of a left $\operatorname{End}_B(P)$-module via postcomposition, so it follows that $\operatorname{Hom}_B(N, P)$ carries the structure of an A-module via

$$(a \cdot f)(n) = a \cdot f(n)$$

for all $a \in A$, $f \in \operatorname{Hom}_B(N, P)$, $n \in N$. We can therefore enhance the k-vector space $\operatorname{Hom}_B(N, P) \otimes N$ to the $(A \otimes B)$-module $\operatorname{Hom}_B(N, P) \boxtimes N$. The k-linear map

$$\psi\colon \operatorname{Hom}_B(N, P) \boxtimes N \to P$$

is then a homomorphism of $(A \otimes B)$-modules because

$$\begin{aligned} \psi((a \otimes b) \cdot (f \otimes n)) &= \psi((af) \otimes (bn)) = (af)(bn) = af(bn) \\ &= abf(n) = (a \otimes 1)(1 \otimes b)f(n) = (a \otimes b)f(n) = (a \otimes b)\psi(f \otimes n) \end{aligned}$$

for all simple tensors $a \otimes b \in A \otimes B$ and $f \otimes n \in \operatorname{Hom}_B(N, P) \otimes N$.

Because P is simple and ψ is nonzero it follows that ψ is surjective. Together with the injectivity of ψ this shows that ψ is an isomorphism of $(A \otimes B)$-modules, which shows that $P \cong \operatorname{Hom}_B(N, P) \boxtimes N$ as $(A \otimes B)$-modules. It follows from Lemma 28.7 that both $\operatorname{Hom}_B(N, P)$ and N are already simple themselves. This shows that Φ is surjective. □

29. Characters

29.1. General Definitions and Properties

Conventions 29.1. In the following k denotes a field, A denotes a k-algebra and M, N denote finite-dimensionl A-modules.

Definition 29.2. Let

$$\rho\colon A \to \operatorname{End}_k(M), \quad a \mapsto (m \mapsto am)$$

be the canonical homomorphism. Then the *character* of M is the k-linear map

$$\chi_M\colon A \to k, \quad a \mapsto \operatorname{tr} \rho(a)\,.$$

Lemma 29.3.

a) We have that $\chi_M(1) = \dim M \cdot 1_k$.

b) If $M \cong N$ as A-modules then $\chi_M = \chi_N$.

c) We have that $\chi_{M \oplus N} = \chi_M + \chi_N$.

d) If N is a submodule of M then $\chi_M = \chi_N + \chi_{M/N}$.

Proof. For every occuring module P of A let

$$\rho_P \colon A \to \operatorname{End}_k(P), \quad a \mapsto (p \mapsto ap)$$

be the corresponding canonical homomorphism.

a) This follows from $\rho_M(1) = \mathrm{id}_M$.

b) Let $m_1, \dots, m_r$ be a k-basis of M and let $\varphi \colon M \to N$ be an isomorphism of A-modules. Then φ is in particular an isomorphism of k-vector spaces and it follows that $\varphi(m_1), \dots, \varphi(m_r)$ is a k-basis of N. Let $a \in A$ and let $B \in \mathrm{M}_r(k)$ be the matrix which represents the endomorphisms $\rho_M(a) \colon M \to M$ with respect to the basis $m_1, \dots, m_r$. Then B also represents the endomorphism $\rho_N(a)$ with respect to the basis $\varphi(m_1), \dots, \varphi(m_r)$ bcause φ is an isomorphism of A-modules. It follows that

$$\chi_M(a) = \operatorname{tr} \rho_M(a) = \operatorname{tr} B = \operatorname{tr} \rho_N(a) = \chi_N(a)\,.$$

c) Let $m_1, \dots, m_r$ be a k-basis of M and let $n_1, \dots, n_s$ be a k-basis of N. Let $a \in A$, let $B_1 \in \mathrm{M}_r(k)$ be the matrix which represents the endomorphism $\rho_M(a)$ with respect to the basis $m_1, \dots, m_r$ and let $B_2 \in \mathrm{M}_s(k)$ be the matrix which represents the endomorphism $\rho_N(a)$ with respect to the basis $n_1, \dots, m_s$. It follows that

$$B := \begin{bmatrix} B_1 & 0 \\ 0 & B_2 \end{bmatrix} \in \mathrm{M}_{r+s}(k)$$

is the matrix which represents the endomorphism $\rho_{M \oplus N}(a)$ with respect to the basis $(m_1, 0), \dots, (m_r, 0), (0, n_1), \dots, (0, n_s)$ of $M \oplus N$. It follows that

$$\begin{aligned} \chi_{M \oplus N}(a) &= \operatorname{tr} \rho_{M \oplus N}(a) = \operatorname{tr} B = \operatorname{tr} B_1 + \operatorname{tr} B_2 \\ &= \operatorname{tr} \rho_M(a) + \operatorname{tr} \rho_N(a) = \chi_M(a) + \chi_N(a)\,. \end{aligned}$$

d) Let $m_1, \dots, m_r$ be a basis of M such that for $s = \dim N$ the vectors $m_1, \dots, m_s$ form a basis of N. Then the residue classes $\overline{m_{s+1}}, \dots, \overline{m_r}$ form a k-basis of V/U. Let $a \in A$ and let $B \in \mathrm{M}_r(k)$ be the matrix which represents $\rho_M(a)$ with respect to the basis $m_1, \dots, m_r$. Then B is of the form

$$B = \begin{bmatrix} B_1 & * \\ 0 & B_2 \end{bmatrix}$$

where $B_1 \in \mathrm{M}_s(k)$ is the matrix which represents $\rho_N(a)$ with respect to the basis $m_1, \dots, m_s$ and $B_2 \in \mathrm{M}_{r-s}(k)$ is the matrix which represents $\rho_{M/N}(a)$ with respect to the basis $\overline{m_{s+1}}, \dots, \overline{m_r}$. It follows that

$$\begin{aligned} \chi_M(a) &= \operatorname{tr} \rho_M(a) = \operatorname{tr} B = \operatorname{tr} B_1 + \operatorname{tr} B_2 \\ &= \operatorname{tr} \rho_N(a) + \operatorname{tr} \rho_{V/U}(a) = \chi_U(a) + \chi_{V/U}(a). \end{aligned}$$

This proves the claim. □

Remark 29.4. It follows from part d) that $\chi_M = \chi_N + \chi_P$ for every short exact sequence of finite-dimensional A-modules

$$0 \to N \to M \to P \to 0 .$$

Part c) then follows from part d) by using the standard split short exact sequence

$$0 \to M \to M \oplus N \to N \to 0 .$$

Recall 29.5. Recall from linear algebra that for any two endomorphisms $f, g\colon V \to V$ of a finite-dimensional k-vector space V it holds that

$$\operatorname{tr}(fg) = \operatorname{tr}(gf) .$$

Warning 29.6. It does not hold that

$$\operatorname{tr}(f_1 \cdots f_n) = \operatorname{tr}(f_{\sigma(1)} \cdots f_{\sigma(n)})$$

for all endomorphisms $f_1, \dots, f_n\colon V \to V$ and every permutation $\sigma \in S_n$. The above formula only generalizes to

$$\operatorname{tr}(f_1 f_2 \cdots f_{n-1} f_n) = \operatorname{tr}(f_2 f_3 \cdots f_n f_1) = \cdots = \operatorname{tr}(f_n f_1 \cdots f_{n-2} f_{n-1}) ,$$

i.e. we need σ to be a power of the cycle $(1, 2, \dots, n)$.

Definition 29.7. The *commutator* of two elements $a, b \in A$ is the element

$$[a, b] \coloneqq ab - ba .$$

The *commutator* subspace of A is

$$[A, A] \coloneqq \langle [a, b] \mid a, b \in A \rangle_k .$$

For all $n \geq 1$ we set

$$\mathfrak{sl}_n(k) \coloneqq [\mathrm{M}_n(k), \mathrm{M}_n(k)] .$$

Remark 29.8. One can define more generally for every two subsets $X, Y \subseteq A$ the commutator $[X, Y] = \langle [x, y] \mid x \in X, y \in Y \rangle_k$, but we will not need this here.

Lemma 29.9. We have for all $n \geq 1$ that $\mathfrak{sl}_n(k) = \ker(\operatorname{tr})$, which is a subspace of $\mathrm{M}_n(k)$ of codimension 1.

Proof. For all $A, B \in \mathrm{M}_n(k)$ we have that

$$\operatorname{tr}([A, B]) = \operatorname{tr}(AB - BA) = \operatorname{tr}(AB) - \operatorname{tr}(BA) = \operatorname{tr}(AB) - \operatorname{tr}(AB) = 0 .$$

This shows that $\mathfrak{sl}_n(k) \subseteq \ker(\operatorname{tr})$.

To show the other inclusion let $(E_{ij})_{1 \leq i,j \leq n}$ be standard basis of $\mathrm{M}_n(k)$. Then the matrices E_{ij} for $i \neq j$ together with the matrices $E_{ii} - E_{i+1,i+1}$ for $i = 1, \dots, n-1$ form a k-basis of $\ker(\operatorname{tr})$. For all $i \neq j$ we have that

$$E_{ij} = E_{ii} E_{ij} - \underbrace{E_{ij} E_{ii}}_{=0} = [E_{ii}, E_{ij}] \in \mathfrak{sl}_n(k) ,$$

and for all $i = 1, \dots, n-1$ we have that

$$E_{ii} - E_{i+1,i+1} = E_{i,i+1}E_{i+1,i} - E_{i+1,i}E_{i,i+1} = [E_{i,i+1}, E_{i+1,i}] \in \mathfrak{sl}_n(k)\,.$$

This shows that $\ker(\mathrm{tr}) \subseteq \mathfrak{sl}_n(k)$.

That $\mathfrak{sl}_n(k) = \ker(\mathrm{tr})$ has codimension 1 in $\mathrm{M}_n(k)$s follows from the fact that $\mathrm{tr}\colon \mathrm{M}_n(k) \to k$ is a surjective linear map. □

Remark 29.10. The notation $\mathfrak{sl}_n(k)$ stems from the fact that $\mathfrak{sl}_n(k)$ is the Lie algebra of the special linear group $\mathrm{SL}_n(k)$.

Remark 29.11. It can be shown that every element of $\mathfrak{sl}_n(K)$ is already a commutator itself, so that

$$\mathfrak{sl}_n(k) = \{[A,B] \mid A, B \in \mathrm{M}_n(k)\}\,.$$

This is proven in [AM57].

Lemma 29.12. Let A and B be k-algebras. Then

$$[A \times B, A \times B] = [A, A] \oplus [B, B].$$

as k-vector subspaces of $A \times B$.

Proof. For all $a, a' \in A$ and $b, b' \in B$ we have that

$$\begin{aligned}[(a,b),(a',b')] &= (a,b)(a',b') - (a',b')(a,b) = (aa', bb') - (a'a, b'b) \\ &= (aa' - a'a, bb' - b'b) = ([a,a'],[b,b'])\,.\end{aligned}$$

It follows that

$$\begin{aligned}[A \times B, A \times B] &= \langle [(a,b),(a',b')] \mid (a,b),(a',b') \in A \times B \rangle_k \\ &= \langle ([a,a'],[b,b']) \mid a, a' \in A \text{ and } b, b' \in B \rangle_k \\ &= \langle [a,a'] \mid a, a' \in A \rangle_k \oplus \langle [b,b'] \mid b, b' \in B \rangle_k \\ &= [A,A] \oplus [B,B]\end{aligned}$$

which proves the claim. □

Corollary 29.13. For all $r \geq 0$ and $n_1, \dots, n_r \geq 1$ the commutator of

$$A \coloneqq \mathrm{M}_{n_1}(k) \times \cdots \times \mathrm{M}_{n_r}(k)$$

is the k-linear subspace of codimension r given by

$$[A, A] = \mathfrak{sl}_{n_1}(k) \oplus \cdots \oplus \mathfrak{sl}_{n_r}(k)\,.$$

Lemma 29.14. We have that $\chi_M(a) = 0$ for every $a \in [A, A]$.

Proof. Let $a, b \in A$. Then

$$\begin{aligned}\chi_M([a,b]) &= \chi_M(ab - ba) = \chi_M(ab) - \chi_M(ba) \\ &= \operatorname{tr}\rho(ab) - \operatorname{tr}\rho(ba) = \operatorname{tr}(\rho(a)\rho(b)) - \operatorname{tr}(\rho(b)\rho(a)) = 0\,.\end{aligned}$$

Since $[A, A]$ is generated by the commutators $[a, b]$ as a k-vector space it follows that $\chi_M(a) = 0$ for all $a \in [A, A]$. □

29.15. It follows from Lemma 29.14 that every character $\chi_M \colon A \to k$ factors through a k-linear map $A/[A, A] \to k$, and can therefore be regarded as an element of $(A/[A, A])^*$. We will often not distinguish between χ_M and the corresponding element of $(A/[A, A])^*$.

Definition 29.16. The character χ_M is *irreducible* is M is simple.

Theorem 29.17.

a) If $\operatorname{char}(k) = 0$ or k is algebraically closed then the irreducible characters of pairwise non-isomorphic finite-dimensional simple A-modules are linearly independent.

b) If k is algebraically closed and A is finite-dimensional and semisimple then the irreducible chararacters form a k-basis of $(A/[A, A])^*$.

Proof.

a) Let $M_1, \dots, M_r$ be pairwise non-isomorphic finite-dimensional simple A-modules and let $\sum_{i=1}^r \lambda_i \chi_{M_i} = 0$.

   Suppose first that $\operatorname{char}(k) = 0$. Then there exists by Corollary 26.17 for every $i = 1, \dots, r$ some $a_i \in A$ which acts on M_i as the identity and on M_j for $j \neq i$ as the zero endomorphism. It follows that

$$\chi_{M_i}(a_j) = \delta_{ij} \dim M_i$$

   for all $i, j = 1, \dots, r$ and therefore that

$$0 = \sum_{i=1}^r \lambda_i \chi_{M_i}(a_j) = \lambda_i \dim M_i$$

   for all $i = 1, \dots, r$. It follows that $\lambda_i = 0$ for all $i = 1, \dots, r$ because $\operatorname{char}(k) \neq 0$.

   Suppose that k is algebraically closed. For every $i = 1, \dots, r$ let $f_i \in \operatorname{End}_k(M_i)$ be an endomorphism with $\operatorname{tr}(f_i) = 1$. It follows from the density theorem that there exists for every $i = 1, \dots, r$ some $a_i \in A$ which acts on M_i by f_i and on M_j with $j \neq i$ by the zero endomorphism. It follows that

$$\chi_{M_i}(a_j) = \delta_{ij}$$

   and therefore that

$$0 = \sum_{i=1}^r \lambda_i \chi_{M_i}(a_j) = \lambda_i$$

   for all $i = 1, \dots, r$.

b) There exists some $r \geq 0$ and $n_1, \dots, n_r \geq 1$ such that $A \cong \mathrm{M}_{n_1}(k) \times \cdots \times \mathrm{M}_{n_r}(k)$ as k-algebras by Corollary 26.10. It follows that there exists precisely r isomorphism classes of simple A-modules, whose characters are linearly independent by part a). It also follows from Corollary 29.13 that $\dim A/[A,A] = r$ and therefore that $\dim(A/[A,A])^* = r$. It follows that the irreducible characters already form a k-basis of $(A/[A,A])^*$. □

Corollary 29.18. Suppose that $\mathrm{char}(k) = 0$. If M, N are semisimple with $\chi_M = \chi_N$ then $M \cong N$.

Proof. Let $M \cong E_1^{\oplus m_1} \oplus \cdots \oplus E_r^{\oplus m_r}$ and $N \cong E_1^{\oplus n_1} \oplus \cdots \oplus E_r^{\oplus n_r}$ as A-modules for pairwise non-isomorphic finite-dimensional simple A-modules $E_1, \dots, E_r$. Then

$$\begin{aligned} \chi_M &= m_1 \chi_{E_1} + \cdots + m_r \chi_{E_r} \\ \chi_N &= n_1 \chi_{E_1} + \cdots + n_r \chi_{E_r} \end{aligned}$$

and it follows that $m_i \cdot 1_k = n_i \cdot 1_k$ for all $i = 1, \dots, r$. It follows from $\mathrm{char}(k) = 0$ that already $m_i = n_i$ for all $i = 1, \dots, r$. □

29.19. We have seen that finite-dimensional semisimple A-modules can be distinguished by their characters if $\mathrm{char}(k) = 0$. For non-semisimple modules this cannot work because every finite-dimensional A-modules shares its character with some semi-simple A-module, as we will now show.

Corollary 29.20. Let

$$0 = M_0 \leq M_1 \leq \cdots \leq M_r = M$$

be a filtration of M with factors $N_i = M_i/M_{i-1}$ for all $i = 1, \dots, r$. Then

$$\chi_M = \chi_{N_1} + \cdots + \chi_{N_r} .$$

Proof. This follows from part d) of Lemma 29.3 by induction on r □

Corollary 29.21 ([Pie82, 5.6, Exercise 1, (e)])**.** There exists a finite-dimensional semisimple module M' with $\chi_M = \chi_{M'}$.

Proof. It follows from the finite-dimensionality of M that there exist a composition series

$$0 = M_0 \lneq M_1 \lneq \cdots \lneq M_r = M$$

of M, i.e. the factors $M'_i \coloneqq M_i/M_{i-1}$ are simple for all $i = 1, \dots, r$. It then follows from Corollary 29.20 that

$$\chi_M = \chi_{M'_1} + \cdots + \chi_{M'_r} = \chi_{M'_1 \oplus \cdots \oplus M'_r} = \chi_{M'}$$

with $M' \coloneqq M'_1 \oplus \cdots \oplus M'_r$ being semisimple. □

29.2. Frobenius Algebras

29.22. We will now show that for certain kind of particularly nice k-algebras the space $(A/[A,A])^*$ can be identified with the center $\mathrm{Z}(A)$.

Definition 29.23. A bilinear form $(-,-)\colon A \times A \to k$ is *associative* if $(ab,c) = (a,bc)$ for all $a,b,c \in A$.

Recall 29.24. If V is a k-vector space then a k-linear map $V \to k$ is a (k-)*linear form*.

Lemma 29.25. The maps

$$\begin{aligned} \{\text{associative bilinear forms } A \times A \to k\} &\longleftrightarrow \{\text{linear forms } A \to k\} \\ (-,-) &\longmapsto (1,-) \\ ((a,b) \mapsto \varepsilon(ab)) &\leftarrow\!\shortmid \varepsilon \end{aligned}$$

are well-defined mutually inverse bijections.

Proof. Both maps are well-defined. If $(-,-)\colon A \times A \to k$ is an associative bilinear form then for $\varepsilon\colon A \to k$ we have that

$$\varepsilon(ab) = (1,ab) = (a,b)$$

for all $a,b \in A$. If $\varepsilon\colon A \to k$ is a linear form then for the bilinear map $(-,-)\colon A\times A \to k$ with $(a,b) = \varepsilon(ab)$ we have that

$$(1,-) = \varepsilon(1\cdot(-)) = \varepsilon(-) = \varepsilon\,.$$

This shows that the maps are mutually inverse. □

Remark 29.26. If $(-,-)\colon A \times A \to k$ is an associative bilinear form then

$$(1,a) = (1, a\cdot 1) = (1\cdot a, 1) = (1,a)$$

for all $a \in A$, and thus $(1,-) = (-,1)$. We have therefore made no unnecessary choice by using $(1,-)$ instead of $(-,1)$ in Lemma 29.25.

Definition 29.27. A linear form $\varepsilon\colon A \to k$ is *symmetric* if $\varepsilon(ab) = \varepsilon(ba)$ for all $a,b \in A$.

Lemma 29.28. An associative bilinear form $(-,-)\colon A \times A \to k$ is symmetric if and only if the corresponding linear form $\varepsilon\colon A \to k$ is symmetric.

Recall 29.29. Recall from linear algebra that a bilinear form $(-,-)\colon V \times W \to k$ on k-vector spaces V,W is *non-degenerate in the first variable* if one (and thus all) of the following equivalent conditions are satisfied:

a) For all $v_1, v_2 \in V$ with $v_1 \neq v_2$ there exists some $w \in W$ with $(v_1,w) \neq (v_2,w)$.

b) For every nonzero $v \in V$ there exists some $w \in W$ with $(v,w) \neq 0$.

c) The linear map $V \to W^*$, $v \mapsto (v, -)$ is injective.

That $(-,-)$ is *non-degenerate in the second variable* is defined is a similar way. The bilinear form $(-,-)$ is *non-degenerate* if it is non-degenerate in both variables.

If V, W are finite-dimensional with $\dim V = \dim W$ then $(-,-)$ is non-degenerate in the first variable if and only if it is non-degenerate in the second variable. In this case all three of the above notions coincide.

If V, W are finite-dimensional then the bilinear form $(-,-)$ is non-degenerate if and only if $\dim V = \dim W$ and for some basis $v_1, \dots, v_n$ of V there exists a dual basis $w_1, \dots, w_n$ of W with

$$(v_i, w_j) = \delta_{ij}$$

for all $i, j = 1, \dots, n$. It then follows that there exists for every basis of V a unique corresponding dual basis of W, which then leads to a bijection between the bases of V and bases of W.

Lemma 29.30. Let $(-,-)\colon A \times A \to k$ be an associative bilinear form with corresponding linear form $\varepsilon\colon A \to k$. Then the following conditions are equivalent:

a) The bilinear form $(-,-)$ is non-degenerate in the first variable.

b) For every nonzero $a \in A$ there exists some $b \in A$ with $\varepsilon(ab) \neq 0$.

c) The kernel $\ker \varepsilon$ contains no nonzero right ideal of A.

Similarly, the following conditions are equivalent:

a) The bilinear form $(-,-)$ is non-degenerate in the second variable.

b) For every nonzero $a \in A$ there exists some $b \in A$ with $\varepsilon(ba) \neq 0$.

c) The kernel $\ker \varepsilon$ contains no nonzero left ideal of A.

Proof.

a) $\iff$ b) This follows from the fact that $(a, b) = \varepsilon(ab)$ for all $a, b \in A$.

b) $\iff$ c) That $\ker \varepsilon$ contains no nonzero right ideal is equivalent to $\ker \varepsilon$ containing no nonzero principal right ideal, i.e. no nonzero right ideal of the form aA with $a \in A$. This happens if and only if for every $a \in A$ there exists some $b \in A$ with $ab \notin \ker \varepsilon$, i.e. $\varepsilon(ab) \neq 0$.

The eqivalence of the other three conditions can be shown in the same way. □

Corollary 29.31. A bilinear form $(-,-)\colon A \times A \to k$ is associative, symmetric and non-degenerate if and only if the corresponding linear form $\varepsilon\colon A \to k$ is symmetric and satisfies one (and thus all) of the conditions from Lemma 29.30.

Definition 29.32. A bilinear form $(-,-)\colon A \times A \to k$ which is associative, symmetric and non-degenerate is a *Frobenius bilinear form.* The corresponding linear form $\varepsilon\colon A \to k$ is a *Frobenius linear form.* The term *Frobenius form* refers to both a Frobenius bilinear form and its associated Frobenius linear form.

Definition 29.33. A *Frobenius algebra* is a finite-dimesional k-algebra A together with Frobenius form on A.

Remark 29.34. Let A be a Frobenius algebra with Frobenius form $(-,-)\colon A \times A \to k$. Then the map

$$\varphi\colon A \to A^*, \quad a \mapsto (a,-)$$

is injective because $(-,-)$ is non-degenerate,. It follows that φ is an isomorphism because A is finite-dimensional.

Example 29.35.

a) If G is a finite group then the group algebra $k[G]$ can be endowed with the structure of a Frobenius algebra via the map $\varepsilon\colon k[G] \to k$ given on the basis G of $k[G]$ by

$$\varepsilon(g) = \begin{cases} 1 & \text{if } g = e\,, \\ 0 & \text{otherwise}\,, \end{cases}$$

for every $g \in G$. In other words, $\varepsilon(\sum_{g \in G} a_g g) = a_e$ is the coefficient of the identity $e \in G$.

For all $a, b \in kG$ with $a = \sum_{g \in G} \lambda_g g$ and $b = \sum_{g \in G} \mu_g g$ we have that

$$\varepsilon(ab) = \sum_{g \in G} \lambda_g \mu_{g^{-1}} = \sum_{h \in G} \mu_h \lambda_{h^{-1}} = \varepsilon(ba)$$

which shows that ε is symmetric. If $a = \sum_{g \in G} a_g g \in k[G]$ with $a \neq 0$ then $a_g \neq 0$ for some $g \in G$ and it follows that

$$\varepsilon(ag^{-1}) = \varepsilon\left(\sum_{h \in G} a_h h g^{-1}\right) = \varepsilon\left(\sum_{h' \in G} a_{h'g} h'\right) = a_g \neq 0\,.$$

Together this shows that ε does indeed define a Frobenius form on $k[G]$.

That the bilinear form $(-,-)\colon k[G] \times k[G] \to k$ corresponding to the linear form ε is non-degenerate can also be seen by noticing that the bases $(g)_{g \in G}$ and $(g^{-1})_{g \in G}$ of $k[G]$ are dual to each other with respect to $(-,-)$.

b) Let k be a field and $n \geq 0$. Then $\mathrm{M}_n(k)$ can be endowed with the structure of a Frobenius algebra via the trace $\mathrm{tr}\colon \mathrm{M}_n(k) \to k$:

We already know that $\mathrm{tr}(AB) = \mathrm{tr}(BA)$ for all $A, B \in \mathrm{M}_n(k)$. To show that the bilinear form $(-,-)\colon \mathrm{M}_n(k) \times \mathrm{M}_n(k)$ corresponding to ε is non-degenerate we use the standard basis E_{ij}, $i, j = 1, \dots, n$ of $\mathrm{M}_n(k)$. We have that

$$\mathrm{tr}(E_{ij} E_{pq}) = \mathrm{tr}(\delta_{jp} E_{iq}) = \delta_{jp}\, \mathrm{tr}(E_{iq}) = \delta_{jp} \delta_{iq}\,.$$

For all $i, j, p, q = 1, \dots, n$, which shows that th two bases $(E_{ij})_{i,j=1,\dots,n}$ and $(E_{ji})_{i,j=1,\dots,n}$ of $\mathrm{M}_n(k)$ are dual to each other with respect to $(-,-)$. Altogether this shows that tr is a Frobenius form on $\mathrm{M}_n(k)$.

Lemma 29.36. If $(-,-)$ is an associative symmetric bilinear form on A then $(-,-)$ is also associative with respect to $[-,-]$ in the sense that

$$([a,b],c) = (a,[b,c])$$

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

Proof. We have that

$$\begin{aligned} ([a,b],c) &= (ab-ba,c) = (ab,c) - (ba,c) = (ab,c) - (c,ba) \\ &= (ab,c) - (cb,a) = (a,bc) - (a,cb) = (a,bc-cb) = (a,[b,c]) \end{aligned}$$

for all $a,b,c \in A$. □

Proposition 29.37. If A is a Frobenius algebra with Frobenius form $(-,-)$ then

$$\psi \colon Z(A) \to (A/[A,A])^*, \quad a \mapsto (a,-)$$

is a well-defined isomorphism of k-vector spaces.

Proof. The map

$$\varphi \colon A \to A^*, \quad a \mapsto (a,-)$$

is an isomorphism of k-vector spaces because A is finite-dimensional and $(-,-)$ is non-degenerate. By using Lemma 29.36 and that $(-,-)$ is non-degenerate it follows that

$$\begin{aligned} \varphi(z)\Big|_{[A,A]} = 0 &\iff \forall a,b \in A : \varphi(z)([a,b]) = 0 \\ &\iff \forall a,b \in A : (z,[a,b]) = 0 \\ &\iff \forall a,b \in A : ([z,a],b) = 0 \\ &\iff \forall a \in A : [z,a] = 0 \\ &\iff z \in \mathrm{Z}(A)\,. \end{aligned}$$

It follows that φ induces the claimed bijection. □

30. Applications to Group Representations

30.1. We will now apply our previous results to the representation theory of groups and also enhance some our previous results. In the following we will not distinguish between representations of a group G over a field k and $k[G]$-modules.

Conventions 30.2. In the following, k denotes a field, G, H denote groups and V denotes a representation of G over k. We abbreviate $\dim_k =: \dim$ and $\otimes_k =: \otimes$.

30.1. Consequences for Group Algebras

30.3. We start by collecting some direct consequences of our previous results.

Lemma 30.4. If k is algebraically closed then the following are equivalent:

a) The representation V is irreducible.

b) The representation V is simple as a $k[G]$-module.

c) The algebra homomorphism $k[G] \to \operatorname{End}_k(V)$, $a \mapsto (v \mapsto av)$ is surjective.

Proof. We have already remarked on the equivalence of a) and b) in part a) of Example 22.4. The equivalence of b) and c) follows from the density theorem. □

Definition 30.5. We set

$$\operatorname{Irr}_k(G) := \{\text{isomorphism classes of irreducible } k\text{-representations of } G\}$$

and

$$\operatorname{irr}_k(G) := \{[V] \in \operatorname{Irr}_k(G) \mid V \text{ is finite-dimensional}\}\,.$$

Lemma 30.6. Let G be finite with $\operatorname{char}(k) \nmid |G|$.

a) We have that

$$|G| = \sum_{i=1}^{n} \frac{(\dim_k V_i)^2}{\dim \operatorname{End}_G(V_i)}$$

where $V_1, \dots, V_n$ is a set of representatives for the isomorphism classes of irreducible k-representations of G.

b) If k is algebraically closed then $|G| = \sum_{i=1}^{n} (\dim_k V_i)^2$.

Proof. This follows from Propositon 26.9 because the group algebra $k[G]$ is semisimple with $\dim k[G] = |G|$. □

Lemma 30.7. The k-linear map

$$\varphi\colon k[G \times H] \to k[G] \otimes k[H], \quad (g, h) \mapsto g \otimes h$$

is a well-defined isomorphism of k-algebras.

Proof. That φ is well-defined follows from $G \times H$ being a basis of $k[G \times H]$. This basis is bijectively mapped onto the basis $(g \otimes h)_{g \in G, h \in H}$ of $k[G] \otimes k[H]$, which shows that φ is bijective. For all $(g_1, h_1), (g_2, h_2) \in G \times H$ we have that

$$\begin{aligned}\varphi((g_1, h_1)(g_2, h_2)) &= \varphi((g_1 g_2, h_1 h_2)) = (g_1 g_2) \otimes (h_1 h_2) \\ &= (g_1 \otimes h_1)(g_2 \otimes h_2) = \varphi((g_1, h_1))\varphi((g_2, h_2))\end{aligned}$$

which shows that φ is multiplicative. □

Definition 30.8. The k-representations $V \boxtimes W$ of $G \times H$ is the k-vector space $V \otimes W$ together with the (linear) group action given by

$$(g, h).(v \otimes w) = (g.v) \otimes (h.w)$$

for all $(g, h) \in G \times H$ and simple tensors $v \otimes w \in V \otimes W$.

Remark 30.9. If we regard V is a $k[G]$-module and W as a $k[H]$-module then the above definition of $V \boxtimes W$ coincides with the one given in 28.6.

Corollary 30.10. If k is algebraically closed then the map

$$\operatorname{irr}_k(G) \times \operatorname{irr}_k(H) \to \operatorname{irr}_k(G \times H), \quad ([V], [W]) \mapsto [V \boxtimes W]$$

is a well-defined bijection.

Proof. This follows from Theorem 28.13 because of Lemma 30.7 and Remark 30.9. □

Lemma 30.11. If k is algebraically closed and G is finite with $\operatorname{char}(k) \nmid |G|$ then the following conditions are equivalent:

a) The group G is abelian.

b) All irreducible representations of G are one-dimensional.

c) The group G has precisely $|G|$ many irreducible representations up to isomorphism.

Proof. This follows from Corollary 26.10 because $\dim k[G] = |G|$ and the group algebra $k[G]$ is commutative if and only if the group G is abelian. □

30.2. Characters

30.12. We now revisit the theory of characters, which has many nice properties for representations of groups.

If V is finite-dimensional then we have previously defined its character (as a finite-dimensional $k[G]$-module) as the k-linear map $\chi_V : k[G] \to k$ given by $\chi_V(a) = \operatorname{tr}(\rho(a))$, where $\rho \colon k[G] \to \operatorname{End}_k(V)$ is the k-algebra homomorphism $a \mapsto (v \mapsto av)$ associated to the $k[G]$-module structure of V. We can now equivalently regard ρ as a group homomorphism $G \to \operatorname{GL}(V)$ and the character χ_V as a map $G \to k$.

Definition 30.13. A function $f \colon G \to k$ is a *class function* if it is constant on conjugacy classes, i.e. if it is invariant under conjugation. The k-vector space of class function $G \to k$ is denoted by $C(G)$.

Lemma 30.14. Let $f \colon G \to k$ be a map and let $F \colon k[G] \to k$ be its k-linear extension given by $F(\sum_{g \in G} a_g g) = \sum_{g \in G} a_g f(g)$. Then the following are equivalent:

a) The map f is a class function, i.e. it holds that $f(hgh^{-1}) = f(g)$ for all $g, h \in G$.

b) It holds that $f(gh) = f(hg)$ for all $g, h \in G$.

c) It holds that $F(ab) = F(ba)$ for all $a, b \in k[G]$.

d) The restriction $F|_{[k[G],k[G]]}$ is the zero map.

If G is finite we additionally have the following equivalent condition:

e) The element $\sum_{g \in G} f(g)g \in k[G]$ is central.

Proof.

a) $\implies$ b) We have that $f(gh) = f(g^{-1}ghg) = f(hg)$.

b) $\implies$ a) We have that $f(ghg^{-1}) = f(hg^{-1}g) = f(h)$.

b) $\iff$ c) This follows from G being a basis of $k[G]$.

c) $\iff$ d) We have for all $a, b \in k[G]$ that $F([a, b]) = F(ab) - F(ba)$, so the equivalence follows from $[k[G], k[G]]$ being generated by $[a, b]$ with $a, b \in k[G]$.

b) $\iff$ e) We have for $x := \sum_{g \in G} f(g)g$ for every $h \in G$ that

$$hx = \sum_{g \in G} f(h^{-1}g)g \quad \text{and} \quad xh = \sum_{g \in G} f(gh^{-1})g\,.$$

It follows that x is central if and only if $f(h^{-1}g) = f(gh^{-1})$ for all $h \in G$. □

30.15. By using Lemma 30.14 we may identify $(k[G]/[k[G], k[G]])^*$ with $C(G)$, and when G is finite also with $\mathrm{Z}(k[G])$.

Proposition 30.16. Let k be algebraically closed and let G be finite with $\mathrm{char}(k) \nmid |G|$.

a) The characters of the irreducible representations of G form a k-basis of $C(G)$.

b) The number of irreducible representations of G coincides with the number conjugacy classes of G.

c) The number of irreducible representations of G coincides with $\dim_k Z(k[G])$.

Proof.

a) This follows from Theorem 29.17 by identifying $(k[G]/[k[G], k[G]])^*$ with $C(G)$.

b) If $\mathcal{O}_1, \dots, \mathcal{O}_n$ are the conjugacy classes of G then the characteristic functions $\chi_{\mathcal{O}_1}, \dots, \chi_{\mathcal{O}_n}$ form a k-basis of $C(G)$ so the claim follows from part a).

c) This follows from part a) by identifying $C(G)$ with $\mathrm{Z}(k[G])$, as well as from Corollary 26.11. □

Remark 30.17. Let k be algebraically closed and let G be finite with $\operatorname{char}(k) \nmid |G|$.

We have shown that the number of isomorphism classes of irreducible representations of G coincides with the number of conjugacy classes of G. We have done so by giving two bases of $C(G)$, namely the irreducible characters and the characteristic functions of the conjugacy classes.

But it needs to be pointed out that this does not give us a bijection between $\operatorname{Irr}(G)$ and the conjugacy classes of G, and that for an arbitrary finite group G with $\operatorname{char}(k) \nmid |G|$ there is canonical way to associate to a conjugacy class of G a “corresponding” irreducible representation.

Example 30.18. If k is algebraically closed and G is finite with $\operatorname{char}(k) \nmid |G|$ and abelian then G has up to isomorphism precisely $|G|$ many irreducible representations. We can see this in various ways:

a) This follows from part b) of Proposition 30.16 because G has $|G|$ conjugacy classes.

b) This follows from part c) of Proposition 30.16 because the group algebra $k[G]$ is abelian and thus $\dim_k \mathrm{Z}(k[G]) = \dim_k k[G] = |G|$.

c) This is part of Lemma 30.11.

d) … and many more.

For $G = \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_r$ with $n_1, \dots, n_r \geq 1$ we can describe the irreducible representations of G explicitely: It follows from $\operatorname{char}(k) \nmid |G| = n_1 \cdots n_r$ that $\operatorname{char}(k) \nmid n_i$ for all $i = 1, \dots, r$, which is why the n_i-th roots of unity $\omega_{i,1}, \dots, \omega_{i,n_i} \in k^\times$ are pairwise different. It follows from Example 4.11 and Corollary 30.10 that the irreducible representations of G are given by $V_{j_1,\dots,j_r}$ with $j_i = 1, \dots, n_i$, each of which is one-dimension and with the action of G being given by

$$(\overline{m_1}, \dots, \overline{m_r}).x = \omega_{1,j_1}^{m_1} \cdots \omega_{r,j_r}^{m_r} x$$

for all $(\overline{m_1}, \dots, \overline{m_r}) \in G$, $x \in V_{j_1,\dots,j_r}$.

Example 30.19. The conjugacy classes of the symmetric group S_n correspond bijectively to partitions of n, as we will now explain:

We can write every permutation $\pi \in S_n$ as a product of cycles

$$\pi = \left(x_1^1, \dots, x_{n_1}^1\right) \cdots \left(x_1^r, \dots, x_{n_r}^r\right)$$

with $n_1 \geq \cdots \geq n_r \geq 1$, and this decomposition is unique up to permutation of cycles of the same length as well as cyclic permuation of $x_1^i, \dots, x_{n_i}^i$. It follows that the partition $(n_1, \dots, n_r)$ of n does only depend on π and not on the choice of decomposition. This partition is the *cycle type* of π. For every $\sigma \in S_n$ we have that

$$\sigma\pi\sigma^{-1} = \left(\sigma(x_1^1), \dots, \sigma(x_{n_1}^1)\right) \cdots \left(\sigma(x_1^r), \dots, \sigma(x_{n_r}^r)\right) ,$$

which shows that conjugated permutations have the same cycle type. The converse also holds:

Claim. Two permutations $\pi_1, \pi_2 \in S_n$ are conjugated if and only if they have the same cycle type.

Proof. We have already seen that conjugated permutations have the same cycle type. Suppose on the other hand that $\pi_1, \pi_2 \in S_n$ have the same cycle type $(n_1, \dots, n_r)$. Then both π_1 and π_2 are conjugated to the permutation

$$(1, \dots, n_1) \cdot (n_1 + 1, \dots, n_1 + n_2) \cdots (n_1 + \cdots + n_{r-1} + 1, \dots, n_1 + \cdots + n_r)\,,$$

and are therefore also conjugated to each other. □

We thus find that the permutations

$$(1, \dots, n_1) \cdot (n_1 + 1, \dots, n_1 + n_2) \cdots (n_1 + \cdots + n_{r-1} + 1, \dots, n_1 + \cdots + n_r)\,,$$

with $(n_1, \dots, n_r) \in \mathrm{Par}(n)$ are a set of representatives of the conjugacy classes of S_n.

It follows that the number of irreducible representations of S_n over an algebraically closed field k with $\mathrm{char}(k) \nmid |S_n| = n!$ (i.e. $\mathrm{char}(k) = 0$ or $\mathrm{char}(k) > n$) is precisely the number of partitions of n.

Orthogonality of Irreducible Characters

Conventions 30.20. In the following V, W denote finite-dimensional representations of G over k.

Lemma 30.21.

a) We have that $\chi_{V \otimes W}(g) = \chi_V(g)\chi_W(g) = (\chi_V \chi_W)(g)$ for every $g \in G$.

b) We have that $\chi_{V^*}(g) = \chi_V(g^{-1})$ for every $g \in G$.

c) We have that $\chi_{\mathrm{Hom}(V,W)}(g) = \chi_V(g^{-1})\chi_W(g)$ for every $g \in G$.

d) If $k = \mathbb{C}$ then $\chi_V(g^{-1}) = \overline{\chi_V(g)}$ for every $g \in G$.

Proof. Let $\rho_V \colon G \to \mathrm{GL}(V)$ and $\rho_W \colon G \to \mathrm{GL}(W)$ be the corresponding group homomorphisms.

a) For every $g \in G$ the action of g on $V \otimes W$ is given by $\rho_V(g) \otimes \rho_W(g)$ and it follows that

$$\chi_{V \otimes W}(g) = \mathrm{tr}(\rho_V(g) \otimes \rho_W(g)) = \mathrm{tr}(\rho_V(g))\,\mathrm{tr}(\rho_W(g)) = \chi_V(g)\chi_W(g)\,.$$

b) The action of $g \in G$ on V^* is given by $\rho(g^{-1})^*$ and it follows that

$$\chi_{V^*}(g) = \mathrm{tr}\,\rho_V(g^{-1})^* = \mathrm{tr}\,\rho_V(g^{-1}) = \chi_V(g^{-1})\,.$$

c) This follows from the previous two parts because $\mathrm{Hom}(V, W) \cong V^* \otimes W$ as seen in Example 4.3.

d) We have seen in 5.9 that there exists a G-invariant inner product $\langle -, - \rangle$ on V. It follows that $\rho_V(g)$ is unitary with respect to $\langle -, - \rangle$ for every $g \in G$. It further follows from linear algebra that $\rho_V(g)$ is diagonalizable with eigenvalues $\lambda_1, \dots, \lambda_n \in \mathbb{C}$ for which $|\lambda_i| = 1$ for all $i = 1, \dots, n$. Then $\rho(g)^{-1}$ is diagonalizable with eigenvalues $\lambda_1^{-1}, \dots, \lambda_n^{-1}$ and it follows that

$$\begin{aligned} \chi_V(g^{-1}) = \operatorname{tr} \rho_V(g^{-1}) = \operatorname{tr} \rho_V(g)^{-1} &= \sum_{i=1}^n \lambda_i^{-1} \\ &= \sum_{i=1}^n \overline{\lambda_i} = \overline{\sum_{i=1}^n \lambda_i} = \overline{\operatorname{tr} \rho_V(g)} = \overline{\chi_V(g)} \end{aligned}$$

as claimed. □

Conventions 30.22. In the following G is finite with $\operatorname{char}(k) \nmid |G|$.

Lemma 30.23. We have that

$$\dim V^G = \frac{1}{|G|} \sum_{g \in G} \chi_V(g) \,.$$

Proof. The Reynolds operator $R \colon V \to V$ given by

$$R(v) := \frac{1}{|G|} \sum_{g \in G} g.v$$

is a projection onto V^G, which is why

$$\dim V^G = \operatorname{tr} R \,.$$

Note that $R = |G|^{-1} \sum_{g \in G} \rho(g)$ where $\rho \colon G \to \mathrm{GL}(V)$ is the group homomorphism corresponding to the representation V. It follows that

$$\dim V^G = \operatorname{tr} R = \frac{1}{|G|} \sum_{g \in G} \operatorname{tr} \rho(g) = \frac{1}{|G|} \sum_{g \in G} \chi_V(g)$$

as desired. □

Corollary 30.24. We have that

$$\dim \operatorname{Hom}_G(V, W) = \frac{1}{|G|} \sum_{g \in G} \chi_V(g^{-1}) \chi_W(g) \,.$$

Proof. It follows from Lemma 30.23 that

$$\begin{aligned} \dim \operatorname{Hom}_G(V, W) = \dim \operatorname{Hom}(V, W)^G &= \frac{1}{|G|} \sum_{g \in G} \chi_{\operatorname{Hom}(V,W)}(g) \\ &= \frac{1}{|G|} \sum_{g \in G} \chi_V(g^{-1}) \chi_W(g) \end{aligned}$$

as claimed. □

30.25. We set

$$(f_1, f_2) \coloneqq \frac{1}{|G|} \sum_{g \in G} f_1(g^{-1}) f_2(g)$$

for all $f_1, f_2 \in C(G)$. Then $(-,-)$ is a symmetric bilinear form on $C(G)$ and we have shown that

$$(\chi_V, \chi_W) = \dim \operatorname{Hom}_G(V, W) \,.$$

Theorem 30.26. Let k be algebraically closed.

a) The irreducible characters of G form an orthonormal basis of $C(G)$ with respect to the bilinear form $(-,-)$.

b) If $V \cong V_1^{\oplus n_1} \oplus \cdots \oplus V_r^{\oplus n_r}$ and $W \cong V_1^{\oplus m_1} \oplus \cdots \oplus V_r^{\oplus m_r}$ for pairwise non-isomorpic irreducible representations $V_1, \dots, V_r$ and $n_1, \dots, n_r, m_1, \dots, m_r \geq 0$ then

$$(\chi_V, \chi_W) = \sum_{i=1}^{r} n_i m_i \,.$$

It follows in particular that $(\chi_{V_i}, \chi_V) = n_i$ is the multiplicity of V_i in V.

c) If $\operatorname{char}(k) = 0$ then the representation V is irreducible if and only if $(\chi_V, \chi_V) = 1$.

Proof.

a) The irreducible characters form a basis of $C(G)$ by Propositon 30.16 and they are orthonormal with respect to $(-,-)$ by Corollary 30.24 and Schur's Lemma.

b) This follows from part a) because $\chi_V = \sum_{i=1}^r n_i \chi_{V_i}$ and $\chi_W = \sum_{i=1}^r m_i \chi_{V_i}$.

c) If $V = V_1^{\oplus n_1} \oplus \cdots \oplus V_r^{n_r}$ for pairwise non-isomorphic irreducible representations $V_1, \dots, V_r$ and $n_1, \dots, n_r \geq 0$ then

$$(\chi_V, \chi_V) = \sum_{i=1}^{r} n_i^2$$

and it follows that $(\chi_V, \chi_V) = 1$ if and only if there exists some $i = 1, \dots, r$ with $n_i = 1$ and $n_j = 0$ for $j \neq i$. □

Remark 30.27. If k is algebraically closed then $C(G)$ has the irreducible characters as a basis, so we may think about $C(G)$ as the free vector space on the isomorphism classes of irreducible representations of G. The bilinear form $(-,-)$ is then the unique k-bilinear extension of $\dim \operatorname{Hom}_G(-,-)$ and the orthonormality of the irreducible characters with respect to $(-,-)$ corresponds to the orthonormality of the isomorphism classes of irreducible representations of G with respect to $\operatorname{Hom}_G(-,-)$.

30.28. For $k = \mathbb{C}$ we also have an inner product $\langle -,- \rangle$ on $C(G)$ which is given by

$$\langle f_1, f_2 \rangle \coloneqq \frac{1}{|G|} \sum_{g \in G} \overline{f_1(g)} f_2(g)$$

for all $f_1, f_2 \in C(G)$ and by Lemma 30.21 we have that $(\chi_V, \chi_W) = \langle \chi_V, \chi_W \rangle$. We may therefore replace $(-,-)$ by $\langle -,- \rangle$ in the above discussion.

30.3. Character Tables

30.29. Let k be algebraically closed and let G be finite with $\operatorname{char}(k) \nmid |G|$.

Let $g_1, \dots, g_r$ be a set of representatives for the conjugacy classes of G such that the conjugacy class of g_i has n_i elements. Let $V_1, \dots, V_r$ be a set of representatives for the isomorphism classes of irreducible representations of G over k with corresponding irreducible characters $\chi_1, \dots, \chi_r$. Then the table

G/k		V_1	$\cdots$	V_n
g_1	n_1	$\chi_1(g_1)$	$\cdots$	$\chi_n(g_1)$
g_2	n_2	$\chi_1(g_2)$	$\cdots$	$\chi_n(g_2)$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
g_r	n_r	$\chi_1(g_r)$	$\cdots$	$\chi_n(g_r)$

is the *character table* of G over k. In the case of $k = \mathbb{C}$ the orthonormality of the irreducible characters then reads

$$\delta_{ij} = \frac{1}{|G|} \sum_{m=1}^{r} n_m \overline{\chi_i(g_m)} \chi_j(g_m)$$

for all $i, j = 1, \dots, n$. This means that the columns of the character table are orthonormal with respect to the inner product $\langle -, - \rangle'$ on $\mathbb{C}^r$ which is given by

$$\langle x, y \rangle' = \frac{1}{|G|} \sum_{m=1}^{r} n_m \overline{x_m} y_m \,.$$

We will now determine the character tables of some groups over the ground field $k = \mathbb{C}$.

Example 30.30 (Character table of $\mathbb{Z}/n$)**.** Let $n \geq 1$ and let $\omega_0, \dots, \omega_{n-1} \in \mathbb{C}^\times$ be the n-th roots of unity with $\omega_k = e^{2\pi i k/n}$ for all $k = 0, \dots, n-1$. By Example 30.18 the irreducible representations of $\mathbb{Z}/n$ are $V_0, \dots, V_{n-1}$ where each V_k is irreducible and $\overline{m} \in \mathbb{Z}/n$ acts on V_k by multiplication with ω_k^m. The character table of $\mathbb{Z}/n$ is thus as follows:

$\mathbb{Z}/n$		$V_0 = \text{triv}$	V_1	$\cdots$	V_{n-1}
$\overline{0}$	1	1	1	$\cdots$	1
$\overline{1}$	1	1	ω_1	$\cdots$	ω_{n-1}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$\overline{n-1}$	1	1	ω_1^{n-1}	$\cdots$	ω_{n-1}^{n-1}

Example 30.31 (Character table of $\mathbb{Z}/2 \times \mathbb{Z}/2$)**.** Let triv be the trivial irreducible representation of $\mathbb{Z}/2$ and let sgn be the sign representation of $\mathbb{Z}/2$, i.e. sgn is one-dimensional and $\overline{1} \in \mathbb{Z}/2$ acts on sgn by multiplication with -1. It then follows from

Example 30.18 that the character table of $\mathbb{Z}/2 \times \mathbb{Z}/2$ is as follows:

$\mathbb{Z}/2 \times \mathbb{Z}/2$		$\mathrm{triv} \boxtimes \mathrm{triv}$	$\mathrm{triv} \boxtimes \mathrm{sgn}$	$\mathrm{sgn} \boxtimes \mathrm{triv}$	$\mathrm{sgn} \boxtimes \mathrm{sgn}$
$(\bar{0}, \bar{0})$	1	1	1	1	1
$(\bar{1}, \bar{0})$	1	1	1	-1	-1
$(\bar{0}, \bar{1})$	1	1	-1	1	-1
$(\bar{1}, \bar{1})$	1	1	-1	-1	1

Example 30.32 (Character table of S_3)**.** Let triv be the irreducible trivial representation of S_3 and let sgn be the sign representation. The groups S_3 acts on $\mathbb{C}^3$ by permutation of the entries, i.e. via

$$\sigma.e_i = e_{\sigma(i)}$$

for all $\sigma \in S_n$, $i = 1, 2, 3$, and it follows from Example 5.3 that

$$V = \{(x_1, x_2, x_3) \in \mathbb{C}^3 \mid x_1 + x_2 + x_3 = 0\}$$

is a two-dimensional irreducible subrepresentation. With respect to the basis b_1, b_2 of V with $b_1 := e_1 - e_2$ and $b_2 := e_2 - e_3$ the action of the elements of S_3 on V is represented by the following matrices:

$$\begin{array}{cccccc} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & \begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix} & \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} & \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix} & \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} & \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix} \\ \mathrm{id} & (1,2) & (1,3) & (2,3) & (1,2,3) & (1,3,2) \end{array} \tag{30.1}$$

We can directy read off the character χ_V from this. The representations $\mathrm{triv}, \mathrm{sgn}, V$ are a set of representatives for the isomorphism classes of irreducible complex representatinos of S_3 as can be seen in the following ways:

- We have that

  $$(\dim \mathrm{triv})^2 + (\dim \mathrm{sgn})^2 + (\dim V)^2 = 1 + 1 + 4 = 6 = |S_3|\,,$$

  so the claim follows from Lemma 30.6.

- The groups S_3 has three conjugacy classes and thus three irreducible complex representations.

We find that the character table of S_3 is given as follows:

S_3		triv	sgn	V
id	1	1	1	2
$(1,2)$	3	1	-1	0
$(1,2,3)$	2	1	1	-1

The third column can also be deduced from the first two columns by using the orthonormality relations of the columns: If a, b, c are the entries of the last column then we need that

$$\begin{cases} a & +3b & +2c & = & 0\,, \\ a & -3b & +2c & = & 0\,, \\ a^2 & +3b^2 & +2c^2 & = & |S_3| = 6\,. \end{cases}$$

It follows from the first two equations that $b = 0$ and that $a = -2c$. From the third equation it then follows that $6c^2 = 6$ and thus either $(a, b, c) = (-2, 0, 1)$ or $(a, b, c) = (2, 0, -1)$. We have that $a > 0$ because a is precisely the dimension of the missing irreducible representation and thus arrive at $(a, b, c) = (2, 0, -1)$.

Example 30.33 (Character table of S_4)**.** The partitions of the natural number 4 are $(4), (3, 1), (2, 2), (2, 1, 1), (1, 1, 1, 1)$, so S_4 has five irreducible representations. The trivial representation triv and sign representation sgn are two of them. We thus get the following character table for S_4:

S_4		triv	sgn	?	?	?
id	1	1	1	?	?	?
$(1,2)$	6	1	-1	?	?	?
$(1,2,3)$	8	1	1	?	?	?
$(1,2,3,4)$	6	1	-1	?	?	?
$(1,2)(3,4)$	3	1	1	?	?	?

The symmetric group S_4 acts on $\mathbb{C}^4$ via

$$\sigma.e_i = e_{\sigma(i)}$$

for all $i = 1, 2, 3, 4$ and it follows from Example 5.3 that

$$V = \{(x_1, x_2, x_3, x_4) \in \mathbb{C}^4 \mid x_1 + x_2 + x_3 + x_4 = 0\}$$

is an irreducible three-dimensional representation of S_3 with basis

$$b_1 \coloneqq e_1 - e_2\,, \quad b_2 \coloneqq e_2 - e_3\,, \quad b_3 \coloneqq e_3 - e_4\,.$$

With respect to the basis b_1, b_2, b_3 of V we have the following representing matrices:

$$\begin{array}{ccccc} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} & \begin{bmatrix} -1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} & \begin{bmatrix} 0 & -1 & 1 \\ 1 & -1 & 1 \\ 0 & 0 & 1 \end{bmatrix} & \begin{bmatrix} 0 & 0 & -1 \\ 1 & 0 & -1 \\ 0 & 1 & -1 \end{bmatrix} & \begin{bmatrix} -1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & -1 \end{bmatrix} \\ \text{id} & (1,2) & (1,2,3) & (1,2,3,4) & (1,2)(3,4) \end{array}$$

From this we can read off another column of the character table:

S_4		triv	sgn	V	?	?
id	1	1	1	3	?	?
$(1,2)$	6	1	-1	1	?	?
$(1,2,3)$	8	1	1	0	?	?
$(1,2,3,4)$	6	1	-1	-1	?	?
$(1,2)(3,4)$	3	1	1	-1	?	?

To find another irreducible representation we consider the three-dimensional representation $V \otimes \mathrm{sgn}$, whose character is given as follows:

S_4		$V \otimes \mathrm{sgn}$
id	1	3
$(1,2)$	6	-1
$(1,2,3)$	8	0
$(1,2,3,4)$	6	1
$(1,2)(3,4)$	3	-1

We have that

$$\langle V \otimes \mathrm{sgn}, V \otimes \mathrm{sgn} \rangle = \frac{1}{24}\left(1 \cdot 3^2 + 6 \cdot 1^2 + 8 \cdot 0^2 + 6 \cdot 1^2 + 3 \cdot 1^2\right) = 1$$

so $V \otimes \mathrm{sgn}$ is irreducible. We have thus found another column of the character table:

S_4		triv	sgn	V	$V \otimes \mathrm{sgn}$	?
id	1	1	1	3	3	?
$(1,2)$	6	1	-1	1	-1	?
$(1,2,3)$	8	1	1	0	0	?
$(1,2,3,4)$	6	1	-1	-1	1	?
$(1,2)(3,4)$	3	1	1	-1	-1	?

Let $a, b, c, d, e \in \mathbb{C}$ be the missing entries of the last column. With the orthonormality relations of the columns we find that

$$\left\{\begin{array}{cccccccl} a & +6b & +8c & +6d & +3e & = & 0\,, \\ a & -6b & +8c & -6d & +3e & = & 0\,, \\ 3a & +6b & & -6d & -3e & = & 0\,, \\ 3a & -6b & & +6d & -3e & = & 0\,, \\ a^2 & +6b^2 & +8c^2 & +6d^2 & +3e^2 & = & |S_4| = 24\,. \end{array}\right.$$

The entry a is the dimension of the missing irreducible representation W and it follows from

$$24 = |S_4| = 1^2 + 1^2 + 3^2 + 3^2 + a^2$$

that $a = 2$. We can therefore simplify the above equation system to

$$\left\{\begin{array}{ccccccr} 6b & +8c & +6d & +3e & = & -2\,, \\ -6b & +8c & -6d & +3e & = & -2\,, \\ 6b & & -6d & -3e & = & -6\,, \\ -6b & & +6d & -3e & = & -6\,, \\ 6b^2 & +8c^2 & +6d^2 & +3e^2 & = & 20\,, \end{array}\right.$$

which leads to the solution

$$(a, b, c, d, e) = (2, 0, -1, 0, 2)\,.$$

We have now found the complete character table:

S_4		triv	sgn	V	$V \otimes \mathrm{sgn}$	W
id	1	1	1	3	3	2
$(1,2)$	6	1	-1	1	-1	0
$(1,2,3)$	8	1	1	0	0	-1
$(1,2,3,4)$	6	1	-1	-1	1	0
$(1,2)(3,4)$	3	1	1	-1	-1	2

We can also construct the missing two-dimensional irreducible representation W explicitely: The group S_4 acts on $\{1,2,3,4\}$ in the natural way, and therefore also on the set

$$X = \{ \quad \{\{1,2\},\{3,4\}\}, \quad \{\{1,3\},\{2,4\}\}, \quad \{\{1,4\},\{2,3\}\} \quad \}$$

of partitions of $\{1,2,3,4\}$ into two-element subsets. By labeling these subsets as X_1, X_2, X_3 this action of S_4 on X corresponds to a group homomorphism $\varphi \colon S_4 \to S_3$. We have that

$$\begin{aligned} \varphi((1,2)) &= (2,3)\,, & \varphi((1,3)) &= (1,3)\,, & \varphi((1,4)) &= (1,2)\,, \\ \varphi((2,3)) &= (1,2)\,, & \varphi((2,4)) &= (1,3)\,, & \varphi((3,4)) &= (2,3)\,, \end{aligned}$$

which shows in particular that φ is surjective. We can therefore pull back the two-dimensional irreducible representation W of S_3 (see Example 30.32) to a two-dimensional irreducible representation of S_4 via

$$\sigma.w = \varphi(\sigma).w$$

for all $\sigma \in S_4$, $w \in W$. We have that

$$\begin{aligned} \varphi(\mathrm{id}) &= \mathrm{id} \\ \varphi((1,2)) &= (2,3)\,, \\ \varphi((1,2,3)) &= \varphi((1,2)(2,3)) = \varphi((1,2))\varphi((2,3)) = (2,3)(1,2) = (1,3,2)\,, \\ \varphi((1,2,3,4)) &= \varphi((1,2)(2,3)(3,4)) = \varphi((1,2))\varphi((2,3))\varphi((3,4)) \\ &= (2,3)(1,2)(2,3) = (1,3)\,, \\ \varphi((1,2)(3,4)) &= \varphi((1,2))\varphi((3,4)) = (2,3)(2,3) = \mathrm{id}\,, \end{aligned}$$

so by using the representing matrices from (30.1) we find that with respect to a suitable basis b_1, b_2 of W the action of S_4 on W is represented by the following matrices:

$$\begin{array}{ccccc} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix} & \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix} & \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} & \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\ \mathrm{id} & (1,2) & (1,2,3) & (1,2,3,4) & (1,2)(3,4) \end{array}$$

By reading off the traces of this matrices we get the last column of the character table as calculated above.

Example 30.34. Let $Q \coloneqq \{\pm 1, \pm i, \pm j, \pm k\} \subseteq \mathbb{H}^\times$ be the quaternion group. The five conjugacy classes of Q are given by $\{1\}, \{-1\}, \{i, -i\}, \{j, -j\}, \{k, -k\}$.

Let triv be the trivial irreducible representation of Q. It follows from

$$8 = |Q| = \sum_{[V] \in \operatorname{irr}(Q)} (\dim V)^2 = 1 + \sum_{\substack{[V] \in \operatorname{irr}(Q) \\ V \ncong \operatorname{triv}}} (\dim V)^2$$

that Q has up to isomorphism

- either eight one-dimensional irreducible representations, or
- four one-dimensional irreducible representations (including triv) and one two-dimensional irreducible representation.

The group Q is not abelian and has therefore by Lemma 30.11 a non-one-dimensional irreducible representation. We thus find that Q has up to isomorphism precisely four one-dimensional irreducible represenations as well as one two-dimensional irreducible representation.

To find the one-dimensional irreducible representations we use that $\mathrm{Z}(Q) = \{\pm 1\}$ is a normal subgroup of index 2 and that $Q/\mathrm{Z}(Q)$ is therefore a group of order 4, which is either isomorphic to $\mathbb{Z}/4$ or to $\mathbb{Z}/2 \times \mathbb{Z}/2$. For every $g \in Q$ we have that $g^2 = \pm 1 \in \mathrm{Z}(Q)$ so it follows that every nontrivial element of $Q/\mathrm{Z}(Q)$ has order 2, which shows that $Q/\mathrm{Z}(Q) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$. An explicit isomorphism is given by

$$Q/\mathrm{Z}(Q) \to \mathbb{Z}/2 \times \mathbb{Z}/2, \quad \begin{cases} \overline{1} \mapsto (\overline{0}, \overline{0}), \\ \overline{i} \mapsto (\overline{1}, \overline{0}), \\ \overline{j} \mapsto (\overline{0}, \overline{1}), \\ \overline{k} \mapsto (\overline{1}, \overline{1}). \end{cases}$$

We can use the resulting surjective groups homomorphism $Q \to \mathbb{Z}/2 \times \mathbb{Z}/2$ to pull back the four irreducible representations of $\mathbb{Z}/2 \times \mathbb{Z}/2$ to representations of Q, each of which is one-dimensional and again irreducible.

The resulting representations $V_{++}, V_{+-}, V_{-+}, V_{--}$ are one-dimensional, the action of $\pm i$ on $V_{\varepsilon_1 \varepsilon_2}$ is given by multiplication with ε_1, the action of $\pm j$ is given by multiplication with ε_2, and the action of $\pm k$ is given by multiplication with $\varepsilon_1 \varepsilon_2$. We therefore get the following entries for the character table of Q:

Q		V_{++}	V_{+-}	V_{-+}	V_{--}	?
1	1	1	1	1	1	?
-1	1	1	1	1	1	?
$\pm i$	2	1	1	-1	-1	?
$\pm j$	2	1	-1	1	-1	?
$\pm k$	2	1	-1	-1	1	?

The last column of the character table, corresponding to the missing two-dimensional irreducible representation W, can be calculated using the orthonormality relation of the columns: If a, b, c, d, e are the entries of the last column then

$$\left\{\begin{array}{llllllr} a & +b & +2c & +2d & +2e & = & 0\,, \\ a & +b & +2c & -2d & -2e & = & 0\,, \\ a & +b & -2c & +2d & -2e & = & 0\,, \\ a & +b & -2c & -2d & +2e & = & 0\,, \\ a^2 & +b^2 & +2c^2 & +2d^2 & +2e^2 & = & |Q| = 8\,. \end{array}\right.$$

We know that $a = \dim W = 2$ so we can simplify the above equation system to

$$\left\{\begin{array}{llllcr} b & +2c & +2d & +2e & = & -2\,, \\ b & +2c & -2d & -2e & = & -2\,, \\ b & -2c & +2d & -2e & = & -2\,, \\ b & -2c & -2d & +2e & = & -2\,, \\ b^2 & +2c^2 & +2d^2 & +2e^2 & = & 4\,. \end{array}\right.$$

Solving this equation system results in

$$(a, b, c, d, e) = (2, -2, 0, 0, 0)\,.$$

With this we have arrived at the following character table:

Q		V_{++}	V_{+-}	V_{-+}	V_{--}	W
1	1	1	1	1	1	2
-1	1	1	1	1	1	-2
$\pm i$	2	1	1	-1	-1	0
$\pm j$	2	1	-1	1	-1	0
$\pm k$	2	1	-1	-1	1	0

We can also explicity construct the missing two-dimensional irreducible representation W: The quaternion group acts on the quaternions $\mathbb{H}$ via

$$q.x = qx$$

for all $q \in Q$, $x \in \mathbb{H}$. Because $\mathbb{C} \subseteq \mathbb{H}$ is a subring we can regard $\mathbb{H}$ as a right[1] $\mathbb{C}$-vector space via

$$x \cdot \lambda = x\lambda$$

for all $\lambda \in \mathbb{C}$, $x \in \mathbb{H}$. This right $\mathbb{C}$-vector space structure corresponds to a left $\mathbb{C}^{\mathrm{op}}$-vector space structure, and thus left $\mathbb{C}$-vector space structure, given by

$$\lambda * x = x \cdot \lambda = x\lambda$$

[1] We can regard $\mathbb{H}$ as both a left and a right $\mathbb{C}$-vector space, but because $\mathbb{C}$ is not contained in $\mathrm{Z}(\mathbb{H}) = \mathbb{R}$ we have to distinguish between these two vector space structures. It is our goal to have Q act $\mathbb{C}$-linearly on $\mathbb{H}$, and for this we need Q and $\mathbb{C}$ to act from different sides on $\mathbb{H}$. We have choosen to let Q act from the left, so $\mathbb{C}$ acts from the right.

for all $\lambda \in \mathbb{C}$, $x \in \mathbb{H}$. The elements $1, j$ then form a $\mathbb{C}$-basis of $\mathbb{H}$ with

$$\begin{aligned} a + bi + cj + dk = a + bi + cj - dji &= 1 \cdot (a + bi) + j \cdot (c - di) \\ &= (a + bi) * 1 + (c - di) * j \end{aligned}$$

for all $a, b, c, d \in \mathbb{R}$. The above action of Q on $\mathbb{H}$ is then $\mathbb{C}$-linear with respect to this left $\mathbb{C}$-vector space structure because

$$q.(\lambda * x) = q.(x\lambda) = qx\lambda = (q.x)\lambda = \lambda * (q.x)$$

for all $q \in Q$, $\lambda \in \mathbb{C}$, $x \in \mathbb{H}$. We have thus constructed a two-dimensional complex representation $W = \mathbb{H}$ of Q. Note that every subrepresentation of W is already invariant under $\langle Q \rangle_{\mathbb{R}} = \mathbb{H}$ and thus a left-ideal of $\mathbb{H}$. Because $\mathbb{H}$ is a skew field the only nonzero subrepresentation is $\mathbb{H}$ itself. This shows that W is irreducible.

With respect to the $\mathbb{C}$-basis $1, j$ of W the action of Q on W is represented by the following matrices:

$$\begin{array}{cccc} \pm\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & \pm\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} & \pm\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} & \pm\begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix} \\ \pm 1 & \pm i & \pm j & \pm k \end{array}$$

By reading off the traces of this matrices we get the last column of the character table as previously calculated.

31. Schur–Weyl Duality

Conventions 31.1. In the following k denotes an infinite field, V denotes a finite-dimensional k-vector space and we fix a natural number $d \geq 1$.

31.2. The group $\mathrm{GL}(V)$ acts on V in the natural way and therefore acts on $V^{\otimes d}$ via

$$\varphi.(v_1 \otimes \cdots \otimes v_d) = (\varphi.v_1) \otimes \cdots \otimes (\varphi.v_d)$$

for all $\varphi \in \mathrm{GL}(V)$ and simple tensors $v_1 \otimes \cdots \otimes v_d \in V^{\otimes d}$. This turns $V^{\otimes d}$ into a representation of $\mathrm{GL}(V)$. The symmetric group S_d also acts on $V^{\otimes d}$ by permuting the tensor factors, i.e. via

$$\pi.(v_1 \otimes \cdots \otimes v_d) = v_{\pi^{-1}(1)} \otimes \cdots \otimes v_{\pi^{-1}(d)}$$

for all $\pi \in S_d$ and simple tensors $v_1 \otimes \cdots \otimes v_d \in V^{\otimes d}$.

These actions of $\mathrm{GL}(V)$ and S_d on $V^{\otimes d}$ commute and we will see in Theorem 31.4 that they do actually centralize each other.

Lemma 31.3. *Let V be a finite-dimensional k-vector space and let $X \subseteq V$ be Zariski-dense. Then the space of symmetric tensors $(V^{\otimes d})^{S_d}$ is generated as a k-vector space by the tensors $x \otimes \cdots \otimes x$ with $x \in X$.*

Proof. Let $e_1, \dots, e_n$ be a k-basis of V, let $S \coloneqq (V^{\otimes d})^{S_d}$ be the space of symmetric tensors and let

$$U \coloneqq \langle x \otimes \cdots \otimes x \,|\, x \in X \rangle_k \subseteq V^{\otimes d}.$$

For every partition $\lambda \in \mathrm{Par}(d)$ of length $\ell(\lambda) = n$ we set

$$e^\lambda = \underbrace{e_1 \otimes \cdots \otimes e_1}_{\lambda_1} \otimes \underbrace{e_2 \otimes \cdots \otimes e_2}_{\lambda_2} \otimes \cdots \otimes \underbrace{e_n \otimes \cdots \otimes e_n}_{\lambda_n}$$

as well as

$$s^\lambda = \sum \text{distinct permutations of } e^\lambda .$$

Note that every basis element $e_{i_1} \otimes \cdots \otimes e_{i_d}$ with $i_1, \dots, i_d = 1, \dots, n$ occurs in precisely one of the elements s^λ. It follows that the element s^λ with $\lambda \in \mathrm{Par}(d)$, $\ell(\lambda) = n$ form a basis of S.

We have that $U \subseteq S$ and to show the other inclusion it suffices to show that every k-linear map $f \colon S \to k$ which vanishes on U already vanishes on S. For this we note that for $v \in V$ with $v = \sum_{i=1}^n v_i e_i$ we have that

$$\begin{aligned} f(v \otimes \cdots \otimes v) &= f\left(\left(\sum_{i_1=1}^n v_i e_i\right) \otimes \cdots \otimes \left(\sum_{i_d=1}^n v_i e_i\right)\right) \\ &= f\left(\sum_{i_1,\dots,i_d=1}^n v_{i_1} \cdots v_{i_d} e_{i_1} \otimes \cdots \otimes e_{i_d}\right) \\ &= f\left(\sum_{\substack{\lambda \in \mathrm{Par}(d) \\ \ell(\lambda)=n}} v_1^{\lambda_1} \cdots v_n^{\lambda_n} s^\lambda\right) = \sum_{\substack{\lambda \in \mathrm{Par}(d) \\ \ell(\lambda)=n}} f(s^\lambda) v_1^{\lambda_1} \cdots v_n^{\lambda_n} . \end{aligned}$$

It follows for the polynomial $p \in k[X_1, \dots, X_n]$ with

$$p(X_1, \dots, X_n) \coloneqq \sum_{\substack{\lambda \in \mathrm{Par}(d) \\ \ell(\lambda)=n}} f(s^\lambda) X_1^{\lambda_1} \cdots X_n^{\lambda_n}$$

that

$$0 = f(x \otimes \cdots \otimes x) = p(x_1, \dots, x_n) .$$

for every element $x \in X$ with $x = \sum_{i=1}^n x_i e_i$. It follows from the Zariski density of X in V that

$$p(v_1, \dots, v_n) = 0$$

for all $v_1, \dots, v_n \in k$, and therefore that $p = 0$ because k is infinite. It follows that $f(s^\lambda) = 0$ for all $\lambda \in \mathrm{Par}(d)$ with $\ell(\lambda) = n$ and therefore that $f = 0$. □

Theorem 31.4. (Schur–Weyl duality) Let A be the image of the canonical homomorphism

$$k[\mathrm{GL}(V)] \to \mathrm{End}_k\left(V^{\otimes d}\right), \quad a \mapsto (x \mapsto ax)$$

and let B be the image of the canonical homomorphism

$$k[S_d] \to \operatorname{End}_k\left(V^{\otimes d}\right), \quad \sigma \mapsto (b \mapsto bx).$$

a) We have that $B' = A$.

b) If $\operatorname{char}(k) = 0$ or $\operatorname{char}(k) > d$ then $A' = B$.

Proof.

a) We have an isomorphism of k-vector spaces

$$\Phi\colon (\operatorname{End}_k(V))^{\otimes d} \to \operatorname{End}_k\left(V^{\otimes d}\right), \quad f_1 \otimes \cdots \otimes f_d \mapsto f_1 \otimes \cdots \otimes f_d\,.$$

Now both $\operatorname{End}_k(V)^{\otimes d}$ and $\operatorname{End}_k\left(V^{\otimes d}\right)$ are representations of S_d via

$$\pi.(f_1 \otimes \cdots \otimes f_d) = f_{\pi^{-1}(1)} \otimes \cdots \otimes f_{\pi^{-1}(d)}$$

for all $\pi \in S_d$ and simple tensors $f_1 \otimes \cdots \otimes f_d \in \operatorname{End}_k(V)^{\otimes d}$, and via

$$(\pi.f)(x) = \pi.f\left(\pi^{-1}.x\right)$$

for all $\pi \in S_d$, $f \in \operatorname{End}_k(V^{\otimes d})$ and $x \in V^{\otimes d}$.

The isomorphism Φ is G-equivarint and thus an isomorphism of representations because for every $\pi \in S_d$ and all simple tensors $f_1 \otimes \cdots \otimes f_d \in \operatorname{End}_k(V)^{\otimes d}$, $v_1 \otimes \cdots \otimes v_d \in V^{\otimes d}$ we have that

$$\begin{aligned}
&\Phi(\pi.(f_1 \otimes \cdots \otimes f_d))(v_1 \otimes \cdots \otimes v_d)\\
&= \Phi\left(f_{\pi^{-1}(1)} \otimes \cdots \otimes f_{\pi^{-1}(d)}\right)(v_1 \otimes \cdots \otimes v_d)\\
&= f_{\pi^{-1}(1)}(v_1) \otimes \cdots \otimes f_{\pi^{-1}(d)}(v_d)
\end{aligned}$$

and

$$\begin{aligned}
&(\pi.\Phi(f_1 \otimes \cdots \otimes f_d))(v_1 \otimes \cdots \otimes v_d)\\
&= \pi.\left(\Phi(f_1 \otimes \cdots \otimes f_d)\left(\pi^{-1}.(v_1 \otimes \cdots \otimes v_d)\right)\right)\\
&= \pi.\left(\Phi(f_1 \otimes \cdots \otimes f_d)\left(v_{\pi(1)} \otimes \cdots \otimes v_{\pi(d)}\right)\right)\\
&= \pi.\left(f_1(v_{\pi(1)}) \otimes \cdots \otimes f_d(v_{\pi(d)})\right)\\
&= f_{\pi^{-1}(1)}(v_1) \otimes \cdots \otimes f_{\pi^{-1}(d)}(v_d)\,.
\end{aligned}$$

It follows that Φ induces an isomorphism

$$\begin{aligned}
B' = \operatorname{End}_{S_d}(V^{\otimes d}) = \operatorname{End}_k\left(V^{\otimes d}\right)^{S_d} &\cong \left(\operatorname{End}_k(V)^{\otimes d}\right)^{S_d}\\
&= \text{symmetric tensors in } \operatorname{End}_k(V)^{\otimes d}\,.
\end{aligned}$$

The group algebra $k[\operatorname{GL}(V)]$ has the elements $\varphi \in \operatorname{GL}(V)$ as a basis, so A is generated by the elements $\varphi \otimes \cdots \otimes \varphi$ with $\varphi \in \operatorname{GL}(V)$ as a k-vector space. To show that $B' = A$ we thus need to show that B' is generated by the elements

$\varphi \otimes \cdots \otimes \varphi$ with $\varphi \in \mathrm{GL}(V)$ as a k-vector space. Under the above isomorphism this is equivalent to $(\mathrm{End}_k(V)^{\otimes d})^{S_d}$ being generated by the elements $\varphi \otimes \cdots \otimes \varphi$ with $\varphi \in \mathrm{GL}(V)$ as a k-vector space. This follows from Lemma 31.3 because $\mathrm{GL}_n(V) \subseteq \mathrm{End}_k(V)$ is Zariski dense.

b) The group algebra $k[S_d]$ is semisimple, so its quotient B is also semisimple by Corollary 23.7. It follows from $B' = A$ and the double centralizer theorem that $A' = B'' = B$. □

Corollary 31.5. If $\mathrm{char}(k) = 0$ then $V^{\otimes d}$ decomposes as

$$V^{\otimes d} \cong \bigoplus_{\lambda \in \Delta} V_\lambda \otimes_{D_\lambda} S_\lambda$$

where

- the summands $V_\lambda \otimes_{D_\lambda} S_\lambda$, $\lambda \in \Delta$ are pairwise non-isomorphic irreducible representations of $\mathrm{GL}(V) \times S_d$,
- V_λ, $\lambda \in \Delta$ are pairwise non-isomorphic irreducible representations of $\mathrm{GL}(V)$,
- S_λ, $\lambda \in \Delta$ are pairwise non-isomorphic irreducible representation of S_d, and
- D_λ is a division k-algebra with $D_i \cong \mathrm{End}_{S_d}(S_\lambda)$ and $D_i^{\mathrm{op}} \cong \mathrm{End}_{\mathrm{GL}(V)}(V_\lambda)$.

Proof. This follows from the Schur–Weyl duality and double centralizer theorem. □

Example 31.6. We consider the case $k = \mathbb{C}$, $V = \mathbb{C}^2$ and $d = 2$. Let e_1, e_2 be the standard basis of $\mathbb{C}^2$. For

$$\Lambda^2(\mathbb{C}) = \langle e_1 \otimes e_2 - e_2 \otimes e_1 \rangle_k \quad \text{and} \quad S^2(\mathbb{C}) = \langle e_1 \otimes e_1, e_1 \otimes e_2 + e_2 \otimes e_1, e_2 \otimes e_2 \rangle_k$$

we have that

$$V \otimes V = \Lambda^2(\mathbb{C}) \oplus S^2(\mathbb{C}) \cong \big(\Lambda^2(\mathbb{C}) \boxtimes \mathrm{sgn}\big) \oplus \big(S^2(\mathbb{C}) \boxtimes \mathrm{triv}\big)$$

with $\Lambda^2(\mathbb{C}), S^2(\mathbb{C})$ being irreducible representations of $\mathrm{GL}_2(\mathbb{C})$ and $\mathrm{triv}, \mathrm{sgn}$ being the irreducible representations of S_2.

31.7. The Schur–Weyl duality leads to the following questions:

- Which representations of S_d occur in $V^{\otimes d}$?
- Do all irreducible representations of S_d occur in $V^{\otimes d}$ for some $d \geq 1$?
- What is a good indexing set Δ?
- What are explicit descriptions for V_λ and S_λ?

These questions lead to the following:

Outlook: Representation Theory of S_n

31.8. Suppose that $\operatorname{char}(k) = 0$. Then the group algebra $k[S_d]$ is semisimple and we know from Example 30.19 that the number of irreducible representations of S_d coincides with the number of partitions of d. One of the main goals of the representation theory of S_d is the construction of an explicit bijection between irreducible representations of S_d and partitions of d.

Definition 31.9. Given a partition λ of d, a *standard Young tableau* (plural: tableaux) of *shape* λ if a filling of the Young diagram of λ with the numbers $1, \dots, d$ which is increasing in both rows and columns.

Example 31.10. The standard Young tabelaux for $d = 3$ are as follows:

$$\begin{array}{|c|c|c|}\hline 1&2&3\\\hline\end{array} \qquad \begin{array}{|c|c|}\hline 1&2\\\hline 3&\multicolumn{1}{c}{}\\\cline{1-1}\end{array} \qquad \begin{array}{|c|c|}\hline 1&3\\\hline 2&\multicolumn{1}{c}{}\\\cline{1-1}\end{array} \qquad \begin{array}{|c|}\hline 1\\\hline 2\\\hline 3\\\hline\end{array}$$

The standard Young tabelaux for $d = 4$ are the following:

$$\begin{array}{|c|c|c|c|}\hline 1&2&3&4\\\hline\end{array} \qquad \begin{array}{|c|c|c|}\hline 1&2&3\\\hline 4&\multicolumn{2}{c}{}\\\cline{1-1}\end{array} \qquad \begin{array}{|c|c|c|}\hline 1&2&4\\\hline 3&\multicolumn{2}{c}{}\\\cline{1-1}\end{array} \qquad \begin{array}{|c|c|c|}\hline 1&3&4\\\hline 2&\multicolumn{2}{c}{}\\\cline{1-1}\end{array}$$

$$\begin{array}{|c|c|}\hline 1&2\\\hline 3&4\\\hline\end{array} \qquad \begin{array}{|c|c|}\hline 1&3\\\hline 2&4\\\hline\end{array} \qquad \begin{array}{|c|c|}\hline 1&2\\\hline 3&\multicolumn{1}{c}{}\\\cline{1-1} 4&\multicolumn{1}{c}{}\\\cline{1-1}\end{array} \qquad \begin{array}{|c|c|}\hline 1&3\\\hline 2&\multicolumn{1}{c}{}\\\cline{1-1} 4&\multicolumn{1}{c}{}\\\cline{1-1}\end{array} \qquad \begin{array}{|c|c|}\hline 1&4\\\hline 2&\multicolumn{1}{c}{}\\\cline{1-1} 3&\multicolumn{1}{c}{}\\\cline{1-1}\end{array} \qquad \begin{array}{|c|}\hline 1\\\hline 2\\\hline 3\\\hline 4\\\hline\end{array}$$

Theorem 31.11. For every partition λ of d let S_λ be the free vector space on the set of standard Young tableaux of shape λ. Then every S_λ can be endowed with the structure of an S_d-representation such that

- every representation S_λ is irreducible, and
- every irreducible representation of S_d is isomorphis to precisely one S_λ.

Appendices

Linear Algebra

A1. Extension of Scalars

Conventions A1.1. During this appendix we fix a field extension L/k.

A1.2. Every L-vector space W can be regarded as a k-vector space in a straightforward way, and this process is known as the *restriction of scalars.* Less straightforward but often useful is the reverse process, the *extension of scalars*, which extends every k-vector space V to an L-vector spaces V_L.

In this section we give a short introduction to this process. We assume that the reader is familiar with the tensor product of vector spaces.

A1.1. Definition and Universal Property

A1.3. let V be a k-vector space. Then the k-vector space strucure of $L \otimes_k V$ extends to an L-vector space structure on $L \otimes_k V$ which is given by

$$\lambda \cdot (l \otimes v) = (\lambda l) \otimes v$$

for all $\lambda \in L$ and simple tensors $l \otimes v \in L \otimes_k V$ with $l \in L$, $v \in V$: To see that this multipliation is well-defined let $\lambda \in L$ and consider the map

$$m_\lambda \colon L \to L, \quad l \mapsto \lambda l \,,$$

which is L-linear and thus k-linear. Then the multiplication with λ on $L \otimes_k V$ is given by $m_\lambda \otimes \mathrm{id}_V$, and therefore well-defined. The various vector space axioms can be checked on simple tensors.

Definition A1.4. For a k-vector space V the L-vector space $V_L \coloneqq L \otimes_k V$ is the *extension of scalars* of V. The k-linear map $\mathrm{can}_V \colon V \to V_L$, $v \mapsto 1 \otimes v$ is the *canonical homomorphism.*

Example A1.5. For $V = k^n$ we have that $V_L = L \otimes_k k^n \cong L^n$, and the canonical homomorphism $\mathrm{can} \colon k^n \to (k^n)_L$ corresponds to the inclusion $k^n \hookrightarrow L^n$.

$$\begin{tikzcd}
(k^n)_L \arrow[r, "\sim"] & L^n \\
k^n \arrow[u, "\mathrm{can}"] \arrow[ur, hook] &
\end{tikzcd}$$

Recall A1.6. Recall from linear algebra that for k-vector spaces U, V and $u \in U$, $v \in V$ one has that $u \otimes v = 0$ if and only if $u = 0$ or $v = 0$:

If $u \neq 0$ and $v \neq 0$, then u can be extended to a k-basis $(u_i)_{i \in I}$ of U with $u = u_{i_0}$ for some $i_0 \in I$, and v can be extended to a k-basis $(v_j)_{j \in J}$ of V with $v = v_{j_0}$ for some $j_0 \in J$. Then $(u_i \otimes v_j)_{i \in I, j \in J}$ is a k-basis of $U \otimes_k V$, and it follows that the basis element $u_{i_0} \otimes v_{j_0}$ is nonzero.

Corollary A1.7. The canonical homomorphism $\mathrm{can}_V \colon V \to V_L$, $v \mapsto 1 \otimes v$ is injective for every k-vector space V.

A1.8. As a consequence of Corollary A1.7 we can regard V as a k-linear subspace of V_L by identifying $v \in V$ with $1 \otimes v \in V_L$. We will not do so during this section, but will at time in the main text.

A1.9. Let V be a k-vector space and let W be an L-vector space.

When $g \colon V_L \to W$ is an L-linear map, then g is also k-linear. It then follows that $g^\circ := g \circ \mathrm{can} \colon V \to W$ is a k-linear map:

$$\begin{tikzcd}
V_L \arrow[r, "g"] & W \\
V \arrow[u, "\mathrm{can}"] \arrow[ur, dashed, "g^\circ"'] &
\end{tikzcd}$$

On elements, g° is given by $g^\circ(v) = g(1 \otimes v)$ for every $v \in V$. One may think about g° as the restriction of g onto V.

Let on the other hand $f \colon V \to W$ be a k-linear map. Then the map

$$f' \colon L \times V \to W, \quad (l, v) \mapsto l \cdot f(v)$$

is k-bilinear and thus induces a k-linear map $\overline{f} \colon V_L \to W$, which is given on simple tensors by

$$\overline{f}(l \otimes v) = l \cdot f(v)$$

for all $l \in L$, $v \in V$. This map is already L-linear: For every $\lambda \in L$ and simple tensor $l \otimes v \in V_L$ with $l \in L$, $v \in V$ one has that

$$\overline{f}(\lambda \cdot (l \otimes v)) = \overline{f}((\lambda l) \otimes v) = (\lambda l) \cdot f(v) = \lambda \cdot (l \cdot f(v)) = \lambda \cdot \overline{f}(l \otimes v)\,.$$

It then follows from the k-linearity of $\overline{f}$ that $\overline{f}(\lambda \cdot x) = \lambda \cdot \overline{f}(x)$ for all $\lambda \in L$, $x \in V_L$ because every $x \in V_L$ is a sum of simple tensors. The constructed L-linear map $\overline{f} \colon V_L \to W$ satisfies

$$\overline{f}(\mathrm{can}_V(v)) = \overline{f}(1 \otimes v) = 1 \cdot f(v) = f(v)$$

for all $v \in V$, and therefore makes the following diagram commute:

$$\begin{tikzcd}
V_L \arrow[r, dashed, "\overline{f}"] & W \\
V \arrow[u, "\mathrm{can}"] \arrow[ur, "f"'] &
\end{tikzcd}$$

One may think about $\overline{f}$ as the L-linear extension of f onto V_L.

If $f\colon V \to W$ is a k-linear map then for the corresponding L-linear map $\overline{f}\colon V_L \to W$ the induced k-linear map $(\overline{f})^\circ\colon V \to W$ is given by

$$(\overline{f})^\circ(v) = \overline{f}(1 \otimes v) = 1 \cdot f(v) = f(v)$$

for all $v \in V$, which shows that $(\overline{f})^\circ = f$.

If $g\colon V_L \to W$ is an L-linear map and $g^\circ\colon V \to W$ is the corresponding k-linear map, then for the induced L-linear map $\overline{g^\circ}\colon V_L \to k$ we have that

$$\overline{g^\circ}(l \otimes v) = l \cdot g^\circ(v) = l \cdot g(1 \otimes v) = g(l \cdot (1 \otimes v)) = g(l \otimes v)$$

for every simple tensor $l \otimes v \in V_L$ with $l \in L$, $v \in V$. It follows from the linearity of both $\overline{g^\circ}$ and g that already $\overline{g^\circ}(x) = g(x)$ for every $x \in V_L$, and thus $\overline{g^\circ} = g$.

This shows that the two constructions $(-)^\circ$ and $\overline{(-)}$ are inverse to each other. Altogether we have found the *universal property of the extension of scalars*:

Theorem A1.10 (Universal property of the extension of scalars)**.** Let V be a k-vector space and let W be an L-vector space. Then the map

$$\begin{aligned} \Phi_{V,W}\colon \operatorname{Hom}_L(V_L, W) &\to \operatorname{Hom}_k(V, W)\,, \\ f &\mapsto g^\circ = g \circ \operatorname{can}_V\,, \\ \overline{g} &\mapsfrom g \end{aligned}$$

is a well-defined bijection.

Remark A1.11. One can think about this universal property in different ways:

- The universal property states that every k-linear map $V \to W$ extends uniquely to an L-linear map $V_L \to W$ along can_V. To construct an L-linear map $V_L \to W$ it therefore sufficies to construct the corresponding k-linear map $V \to W$.
- The L-vector space V_L together with the inclusion $\operatorname{can}_V\colon V \to V_L$ is the most general way to extend the k-vector space V to an L-vector space:

  Whenever W is another L-vector space and $f\colon V \to W$ is a k-linear map, then we may think of f as an embedding of V into W, except that f needs not be injective. Then f factors trough V_L by extending to an L-linear map $\overline{f}\colon V_L \to W$ which me may think about as an embedding of V_L into W, except that $\overline{f}$ also does not need to be injective.

  (Note that $\overline{f}$ does not need to be injective even if f is injective: Consider $k = \mathbb{R}$, $L = \mathbb{C}$, $V = \mathbb{R}^2$ and $W = \mathbb{C}$. Then the map $f\colon \mathbb{R}^2 \to \mathbb{C}$, $(x, y) \mapsto x + iy$ is an isomorphism of $\mathbb{R}$-vector spaces, but the induced L-linear map $\overline{f}\colon (\mathbb{R}^2)_{\mathbb{C}} \to \mathbb{C}$ cannot be injective because $(\mathbb{R}^2)_{\mathbb{C}} \cong \mathbb{C}^2$ by Example A1.5. Indeed, the map $\overline{f}$ corresponds to the map $\mathbb{C}^2 \to \mathbb{C}$, $(x, y) \mapsto x + iy$.)

Remark A1.12. As usual with universal properties, the L-vector space V_L together with the canonical homomorphism $\operatorname{can}_V\colon V \to V_L$ is uniquely determined by it up to unique isomorphism: If V' is another L-vector space and $\iota\colon V \to V'$ is a k-linear map such that

$$\mathrm{Hom}_L(V', W) \to \mathrm{Hom}_k(V, W)\,, \quad f \mapsto f \circ \iota$$

is bijective for every L-vector space W, then there exists a unique L-linear map

$$\varphi\colon V_L \to V'$$

such that the diagram

$$\begin{tikzcd} & V \arrow[dl, "\mathrm{can}_V"'] \arrow[dr, "\iota"] & \\ V_L \arrow[rr, "\varphi"] & & V' \end{tikzcd}$$

commutes, and φ is an isomorphism of L-vector spaces.

Remark A1.13. The bijections $\Phi_{V,W}$ from Theorem A1.10 are actually isomorphisms of k-vector spaces, which are "natural" in V and W in the sense of category theory. (To make this naturality precise one needs to expand $(-)_L$ to a functor, which we will do in the next subsection.) This gives a rise to an adjunction, see Remark A1.24.

Lemma A1.14. Let V be a k-vector space. If a family $(v_i)_{i\in I}$ of vectors $v_i \in V$ is a k-basis of V, then $(1 \otimes v_i)_{i\in I}$ is an L-basis of V_L.

Proof. We have that $V = \bigoplus_{i\in I} \langle v_i \rangle_k$ and therefore

$$V_L = L \otimes_k V = L \otimes_k \left(\bigoplus_{i\in I} \langle v_i \rangle_k \right) = \bigoplus_{i\in I} (L \otimes_k \langle v_i \rangle_k) = \bigoplus_{i\in I} \langle 1 \otimes v_i \rangle_L \ ,$$

which proves the claim. □

Remark A1.15. Recall from linear algebra that $B \subseteq V$ is a k-basis of V if and only if for every k-vector space W the restriction

$$\mathrm{Hom}_k(V, W) \to \mathrm{Maps}(B, W), \quad f \mapsto f|_B$$

is a bijection. This can be used to given an alternative proof of Lemma A1.14:

Let $\{v_i\}_{i\in I}$ be a k-basis of V. The canonical homomorphism $\mathrm{can}_V\colon V \to V_L$ is injective, and thus induces a bijection

$$c\colon \{v_i\}_{i\in I} \to \{1 \otimes v_i\}_{i\in I}, \quad v_i \mapsto 1 \otimes v_i = \mathrm{can}_V(v_i)\,.$$

For every L-vector space W we therefore get a commutative diagram

$$\begin{tikzcd} \mathrm{Hom}_L(V_L, W) \arrow[r, "\mathrm{can}_V^*"] \arrow[d, "\text{restriction}"'] & \mathrm{Hom}_k(V, W) \arrow[d, "\text{restriction}"] \\ \mathrm{Maps}\left(\{1 \otimes v_i\}_{i\in I}, W\right) \arrow[r, "c^*"] & \mathrm{Maps}\left(\{v_i\}_{i\in I}, W\right) \end{tikzcd}$$

where the map

$$\mathrm{can}_V^*\colon \mathrm{Hom}_L(V_L, W) \to \mathrm{Hom}_k(V, W), \quad h \mapsto h \circ \mathrm{can}_V$$

is bijective by Theorem A1.10, and the map

$$c_*\colon \mathrm{Maps}\left(\{1 \otimes v_i\}_{i\in I}, W\right) \to \mathrm{Maps}\left(\{v_i\}_{i\in I}, W\right), \quad h \mapsto h \circ c$$

is bijective because c is a bijection.

It follows that the restriction on the left is a bijection if and only if the restriction on the right is a bijection, i.e. that $\{v_i\}_{i\in I}$ is a k-basis of V if and only if $\{1 \otimes v_i\}_{i\in I}$ is an L-basis of V_L.

A1.16. So far we have constructed for every k-vector space V a new L-vector space V_L which contains V as a k-linear subspace (via $\mathrm{can}_V\colon V \hookrightarrow V_L$) and is universal with this property.

In praxis we often want to realize the extension of scalars V_L as an already know L-vector space W which contains V as a k-linear subspace $V \subseteq W$, just how we can realize $(k^n)_L$ as L^n as seen in Example A1.5.

A general criterion for this is given by the following corollary of Lemma A1.14.

Corollary A1.17. Let W be an L-vector space, and let $V \subseteq W$ a k-linear subspace. Suppose that $B \subseteq V$ is both a k-basis of V and an L-basis of W. Then the unique L-linear map $\varphi\colon V_L \to W$ given on simple tensors by

$$\varphi(l \otimes v) = lv$$

for all $l \in L$, $v \in V$ is an isomorphism.

Proof. The desired map φ is the unique L-linear extension of the k-linear inclusion $V \hookrightarrow W$, which exists by the universal property of the extension of scalars:

$$\begin{tikzcd}
V_L \arrow[r, dashed, "\varphi"] & W \\
V \arrow[u, "\mathrm{can}_V"] \arrow[ur, hook] &
\end{tikzcd}$$

Then φ maps the L-basis $(1 \otimes b)_{b\in B}$ of V_L bijectively onto the L-basis B of W, and is therefore an isomorphism. □

Example A1.18.

a) We have that $k^n \subseteq L^n$ is a k-linear subspace, and the standard basis $e_1, \dots, e_n$ is both a k-basis of k^n and an L-basis of L^n. It follows that there exists an isomorphism of L-vector spaces $(k^n)_L \to L^n$ which maps $1 \otimes e_i \in (k^n)_L$ to $e_i \in L^n$ for every $i = 1, \dots, n$. (We have already seen this in Example A1.5.)

b) We have that $K[X] \subseteq L[X]$ is a k-linear subspace, and the monomials X^n, $n \geq 0$ form both a k-basis of $K[X]$ and an L-basis of L^n. It follows that there exists an isomorphism of L-vector spaces $k[X]_L \to L[X]$ which maps $1 \otimes X^n \in k[X]_L$ to $X^n \in L[X]$ for every $n \geq 0$.

c) We find in the same way that there exists an isomorphism of L-vector spaces $k[X_1, \dots, X_n]_L \to L[X_1, \dots, X_n]$ which maps $1 \otimes X^{\alpha_1} \cdots X^{\alpha_n} \in k[X_1, \dots, X_n]_L$ to $X_1^{\alpha_1} \cdots X_n^{\alpha_n} \in L[X_1, \dots, X_n]$ for every multiindex $\boldsymbol{\alpha} \in \mathbb{N}^n$.

d) We have that $\mathrm{M}_n(k) \subseteq \mathrm{M}_n(L)$ is a k-linear subspace, and the matrices E_{ij}, $1 \leq i, j \leq n$ are both a k-basis of $\mathrm{M}_n(k)$ and an L-basis of $\mathrm{M}_n(L)$. It follows that there exists an isomorphism of L-vector spaces $\mathrm{M}_n(k)_L \to \mathrm{M}_n(L)$ which maps $1 \otimes E_{ij} \in \mathrm{M}_n(k)_L$ to $E_{ij} \in \mathrm{M}_n(L)$ for all $1 \leq i, j \leq n$.

e) Let G be a group. Then $k[G] \subseteq L[G]$ is a k-linear subspace, and the group G is both a k-basis of $k[G]$ and an L-basis of $L[G]$. It follows that there exists an isomorphism of L-vector spaces $k[G]_L \to L[G]$ which maps $1 \otimes g \in k[G]$ to $g \in L[G]$ for every $g \in G$.

Recall A1.19. Let W, V be k-vector spaces and let $(w_j)_{j \in J}$ be a k-basis of W. Then every $x \in W \otimes_k V$ can be written as $x = \sum_{j \in J} w_j \otimes v_j$ for unique elements $v_j \in V$ (with $v_j = 0$ for all but finitely many $j \in J$): We have that $W = \bigoplus_{j \in J} \langle w_j \rangle_k$ and therefore

$$W \otimes_k V = \left(\bigoplus_{j \in J} \langle w_j \rangle_k \right) \otimes_k V = \bigoplus_{j \in J} (\langle w_j \rangle_k \otimes_k V) = \bigoplus_{j \in J} (w_j \otimes V) \cong \bigoplus_{j \in J} V \,.$$

Note that for the uniqueness of the decomposition $x = \sum_{j \in J} w_j \otimes v_j$ it sufficies that $(w_j)_{j \in J}$ in linearly independent, because we can then set $W = \langle w_j \mid j \in J \rangle_k$ and use the above result. (Of course, if $(w_j)_{j \in J}$ is not a basis of W then such a decomposition may not exist.)

Corollary A1.20. Let V be a k-vector space and $\{U_i\}_{i \in I}$ a collection of k-vector subspaces $U_i \subseteq V$. Then

$$L \otimes_k \left(\bigcap_{i \in I} U_i \right) = \bigcap_{i \in I} (L \otimes_k U_i) \,.$$

First proof. For every $j \in I$ we have that $\bigcap_{i \in I} U_i \subseteq U_j$, therefore

$$L \otimes_k \left(\bigcap_{i \in I} U_i \right) \subseteq L \otimes_k U_j \,,$$

and thus altogether

$$L \otimes_k \left(\bigcap_{i \in I} U_i \right) \subseteq \bigcap_{j \in I} (L \otimes_k U_j) \,.$$

For the other inclusion let $x \in \bigcap_{i \in I}(L \otimes U_i)$, and let $(b_j)_{j \in J}$ be a k-basis of L. By using that $x \in L \otimes_k V$ we may write

$$x = \sum_{j \in J} b_j \otimes v_j$$

for unique elements $v_j \in V$. For every $i \in I$ it similarly follows from $x \in L \otimes_k U_i$ that

$$x = \sum_{j \in J} b_j \otimes u^i_j$$

for unique elements $u^i_j \in U_i$. It follows for every $j \in J$ from the uniqueness of these decompositions that $v_j = u^i_j \in U_i$ for every $i \in I$, and therefore that $v_j \in \bigcap_{i \in I} U_i$. It thus follows that

$$x = \sum_{j \in J} b_j \otimes v_j \in L \otimes_k \left(\bigcap_{i \in I} U_i \right).$$

This proves the other inclusion. □

Second proof. Let $(b_j)_{j \in J}$ be a k-basis of L. Then

$$L \otimes_k V = \bigoplus_{j \in J} k b_j \otimes V = \bigoplus_{j \in J} b_j \otimes V \cong V^{\oplus J}.$$

Under this isomorphism, a subspace of $L \otimes_k V$ that is of the form $L \otimes_k U$ for some linear subspace $U \subseteq V$ becomes identified with the linear subspace $U^{\oplus J} \subseteq V^{\oplus J}$. It follows that $L \otimes_k U_i$ becomes for every $i \in I$ identified with $U_i^{\oplus J}$, and hence that $\bigcap_{i \in I} L \otimes_k U_i$ becomes identified with $\bigcap_{i \in I} U_i^{\oplus J}$. But

$$\bigcap_{i \in I} U_i^{\oplus J} = \left(\bigcap_{i \in I} U_i \right)^{\oplus J},$$

and the subspace on the right-hand side is the one identified with $L \otimes_k (\bigcap_{i \in I} U_i)$. □

A1.2. Functoriality

A1.21. For every k-linear map $f \colon V \to W$ between k-vector spaces V, W the induced k-linear map

$$f_L \coloneqq \mathrm{id}_L \otimes f \colon V_L \to W_L$$

is already L-linear: For all $\lambda \in L$ and simple tensors $l \otimes v \in V_L$ with $l \in L$, $v \in V$ we have that

$$f_L(\lambda \cdot (l \otimes v)) = f_L((\lambda l) \otimes v) = (\lambda l) \otimes f(v) = \lambda \cdot (l \otimes f(v)) = \lambda f_L(l \otimes v),$$

and thus $f_L(\lambda \cdot x) = \lambda f_L(x)$ for every $x \in V_L$ because every tensor is a sum of simple tensors.

For every k-vector space V we have that

$$(\mathrm{id}_V)_L = \mathrm{id}_L \otimes \mathrm{id}_V = \mathrm{id}_{V \otimes_k L} = \mathrm{id}_{V_L} \,,$$

and for all composable k-linear maps $f\colon U \to V$, $g\colon V \to W$ we have that

$$g_L \circ f_L = (\mathrm{id}_L \otimes g) \circ (\mathrm{id}_L \otimes f) = (\mathrm{id}_L \circ \mathrm{id}_L) \otimes (g \circ f) = \mathrm{id}_L \otimes (g \circ f) = (g \circ f)_L \,.$$

This shows that $(-)_L$ defines a functor

$$(-)_L \colon k\text{-}\mathbf{Vect} \to L\text{-}\mathbf{Vect} \,.$$

Lemma A1.22. Let V and V' be k-vector spaces. Then the diagram

$$\begin{tikzcd}
V_L \arrow[r, "f_L"] & V'_L \\
V \arrow[u, "\mathrm{can}_V"] \arrow[r, "f"] & V' \arrow[u, "\mathrm{can}_{V'}"']
\end{tikzcd}$$

commutes for every k-linear map $f\colon V \to V'$.

Proof. For every $v \in V$ one has that

$$f_L(\mathrm{can}_V(v)) = f_L(1 \otimes v) = 1 \otimes f(v) = \mathrm{can}_{V'}(f(v)) \,. \qquad \square$$

Remark A1.23. One can also construct the action of $(-)_L$ on k-linear maps in a more abstract way:

If $f\colon V \to W$ is a k-linear map between k-vector spaces V, W then the k-linear map $\mathrm{can}_W \circ f\colon V \to W_L$ induces a unique L-linear map $f_L\colon V_L \to W_L$ which make the diagram

$$\begin{tikzcd}
V_L \arrow[r, dashed, "f_L"] & W_L \\
V \arrow[u, "\mathrm{can}_V"] \arrow[r, "f"] & W \arrow[u, "\mathrm{can}_W"']
\end{tikzcd}$$

commutes, and Lemma A1.22 shows that this abstract definition of f_L coincides with the previous definition. That $(-)_L$ is compatible with identities and composition can also be seen using diagrams:

It follows for every k-vector space V from the commutativity of the diagram

$$\begin{tikzcd}
V_L \arrow[r, "\mathrm{id}_{V_L}"] & V_L \\
V \arrow[u, "\mathrm{can}_V"] \arrow[r, "\mathrm{id}_V"] & V \arrow[u, "\mathrm{can}_V"']
\end{tikzcd}$$

that id_{V_L} satisfies the defining property of $(\mathrm{id}_V)_L$, so it follows that $(\mathrm{id}_V)_L = \mathrm{id}_{V_L}$.

For all composable k-linear maps $f\colon U \to V$, $g\colon V \to W$ it follows from the commutativity of the diagram

$$\begin{tikzcd}
U_L \arrow[r, "f_L"] \arrow[rr, bend left, "g_L \circ f_L"] & V_L \arrow[r, "g_L"] & W_L \\
U \arrow[u, "\mathrm{can}_U"'] \arrow[r, "f"] \arrow[rr, bend right, "g \circ f"'] & V \arrow[u, "\mathrm{can}_V"'] \arrow[r, "g"] & W \arrow[u, "\mathrm{can}_W"']
\end{tikzcd}$$

that $g_L \circ f_L$ satisfies the defining property of $(g \circ f)_L$, so it follows that $(g \circ f)_L = g_L \circ f_L$.

Remark A1.24. We also have the restriction of scalars

$$R\colon L\text{-}\mathbf{Vect} \to k\text{-}\mathbf{Vect}$$

which sends every L-vector space to its underlying k-vector space and every L-linear map to the corresponding k-linear map.

From the universal property of the extension of scalars we know that for every k-vector space V and L-vector space W we have a bijection

$$\begin{aligned}\Phi_{V,W}\colon \operatorname{Hom}_L(E(V), W) &\to \operatorname{Hom}_k(V, R(W)), \\ g &\mapsto R(g) \circ \mathrm{can}_V \ .\end{aligned}$$

These bijections $\Phi_{V,W}$ result in an adjunction $\Phi\colon (-)_L \dashv R$:

It only remains to show that the bijections $\Phi_{V,W}$ are natural in V and W, i.e. that for every k-linear map $f\colon V \to V'$ between k-vector spaces V, V' and every L-linear map $g\colon W \to W'$ between L-vector spaces W, W' the diagram

$$\begin{tikzcd}
\operatorname{Hom}_L(V'_L, W) \arrow[r, "g \circ (-) \circ f_L"] \arrow[d, "R(-)\circ \mathrm{can}_{V'} = \Phi_{V',W}"'] & \operatorname{Hom}_L(V_L, W') \arrow[d, "\Phi_{V,W'} = R(-) \circ \mathrm{can}_V"] \\
\operatorname{Hom}_k(V', R(W)) \arrow[r, "R(g) \circ (-) \circ f"] & \operatorname{Hom}_k(V, R(W'))
\end{tikzcd}$$

commutes. This holds because

$$R(g \circ (-) \circ f_L) \circ \mathrm{can}_V = R(g) \circ R(-) \circ R(f_L) \circ \mathrm{can}_V = R(g) \circ R(-) \circ \mathrm{can}_{V'} \circ f \,,$$

where we use the equality $R(f_L) \circ \mathrm{can}_V = \mathrm{can}_{V'} \circ f$ from Lemma A1.22.

Remark A1.25. If $f\colon V \to W$ is a k-linear map between finite-dimensional k-vector spaces V, W and $B \subseteq V$, $C \subseteq W$ are k-basis, then with respect to the basis

$$B_L \coloneqq 1 \otimes B = \{1 \otimes b \mid b \in B\}$$

of V_L and the basis $C_L \coloneqq 1 \otimes C$ of W_L we have the equality of representing matrices

$$[f]^B_C = [f_L]^{B_L}_{C_L} \,.$$

We will not need this.

A1.3. Extension of Scalars for Algebras

A1.26. For k-algebras A and B their tensor product $A \otimes_k B$ can again be endowed with the structure of a k-algebra, with the multiplication being given on simple tensors by

$$(a_1 \otimes b_1) \cdot (a_2 \otimes b_2) = (a_1 a_2) \otimes (b_1 b_2).$$

for all $a_1, a_2 \in A$, $b_1, b_2 \in B$. If both A, B are unital then $A \otimes_k B$ is again unital with $1_{A \otimes B} = 1_A \otimes 1_B$.

To see that this multiplication is well-defined note that the map

$$\begin{aligned} A \times B \times A \times B &\to A \otimes_k B\,, \\ (a_1, b_1, a_2, b_2) &\mapsto (a_1 a_2) \otimes (b_1 b_2) \end{aligned}$$

is well-defined and k-multilinear, and thus induces a well-defined k-linear map

$$\begin{aligned} A \otimes_k B \otimes_k A \otimes_k B &\to A \otimes_k B\,, \\ a_1 \otimes b_1 \otimes a_2 \otimes b_2 &\mapsto (a_1 a_2) \otimes (b_1 b_2)\,, \end{aligned}$$

which in turn corresponds to a k-bilinear map

$$\begin{aligned} (A \otimes_k B) \times (A \otimes_k B) &\to A \otimes_k B\,, \\ (a_1 \otimes b_1, a_2 \otimes b_2) &\mapsto (a_1 a_2) \otimes (b_1 b_2)\,. \end{aligned}$$

The various algebra axioms can now be checked on simple tensors.

A1.27. Let A be a k-algebra. By considering L as a k-algebra it now follows that $A_L = L \otimes_k A$ carries the structure of a k-algebra, with the multiplication being given on simple tensors by

$$(l_1 \otimes a_1) \cdot (l_2 \otimes a_2) = (l_1 l_2) \otimes (a_1 a_2)$$

for all $l_1, l_2 \in L$, $a_1, a_2 \in A$. The k-bilinear map

$$\begin{aligned} (L \otimes_k A) \times (L \otimes_k A) &\to L \otimes_k A\,, \\ (l_1 \otimes a_1, l_2 \otimes a_2) &\mapsto (l_1 l_2) \otimes (a_1 a_2) \end{aligned}$$

is already L-bilinear, so the L-vector space structure of A_L makes the k-algebra A_L into an L-algebra.

Remark A1.28. Let A be a k-algebra.

a) If A is unital then so is A_L with $1_{A_L} = 1 \otimes 1_A$.

b) The canonical homomorphism $\mathrm{can}_A \colon A \to A_L$ is already a homomorphism of k-algebras.

Lemma A1.29. If $f \colon A \to B$ is a homomorphism of k-algebras, then the induced L-linear map $f_L \colon A_L \to B_L$ is a homomorphism of L-algebras.

Proof. The map f_L is multiplicative on simple tensors because

$$\begin{aligned} f_L((l_1 \otimes a_1)(l_2 \otimes a_2)) &= f_L((l_1 l_2) \otimes (a_1 a_2)) = (l_1 l_2) \otimes f(a_1 a_2) \\ = (l_1 l_2) \otimes (f(a_1) f(a_2)) &= (l_1 \otimes f(a_1))(l_2 \otimes f(a_2)) = f_L(l_1 \otimes a_1) f_L(l_2 \otimes a_2) \end{aligned}$$

for all $l_1, l_2 \in L$, $a_1, a_2 \in A$. It follows that f_L is multiplicative because these simple tensors generate $L \otimes_k A_1$ as a vector space i. □

Remark A1.30. With this we have seen that the extension of scalars defines a functor $(-)_L \colon k\text{-}\mathbf{Alg} \to L\text{-}\mathbf{Alg}$.

Lemma A1.31. Let A be a k-algebra, B an L-algebra and $f \colon A \to B$ a homomorphism of k-algebras. Then the corresponding L-linear map $\overline{f} \colon A_L \to B$ is a homomorphism of L-algebras.

Proof. The map $\overline{f}$ is multiplicative on simple tensors because

$$\begin{aligned} \overline{f}((l_1 \otimes a_1)(l_2 \otimes a_2)) &= \overline{f}((l_1 l_2) \otimes (a_1 a_2)) = l_1 l_2 f(a_1 a_2) \\ &= l_1 l_2 f(a_1) f(a_2) = l_1 f(a_1) l_2 f(a_2) = \overline{f}(l_1 \otimes a_1) \overline{f}(l_2 \otimes a_2) \end{aligned}$$

for all $l_1, l_2 \in L$, $a_1, a_2 \in A$. It follows that $\overline{f}$ is multiplicative because the simple tensors generate A_L as a vector space. □

Remark A1.32. It follows from Lemma A1.31 that for a k-algebra A and an L-algebra B the bijection

$$\Phi_{A,B} \colon \operatorname{Hom}_L(A_L, B) \to \operatorname{Hom}_k(A, B), \quad f \mapsto f \circ \operatorname{can}_A$$

restricts to a bijection

$$\Psi_{A,B} \colon \operatorname{Hom}_{L\text{-}\mathbf{Alg}}(A_L, B) \to \operatorname{Hom}_{k\text{-}\mathbf{Alg}}(A, B) \,.$$

This can also be formulated by giving a variation of Theorem A1.10 for algebras.

It follows that the functor $(-)_L \colon k\text{-}\mathbf{Alg} \to L\text{-}\mathbf{Alg}$ is left adjoint to the forgetful functor $R \colon L\text{-}\mathbf{Alg} \to k\text{-}\mathbf{Alg}$.

A1.33. We have seen in Corollary A1.17 that it is possible to realize the extension of scalars of a k-vector V as a given L-vector space W with $V \subseteq W$ under suitable conditions. This also generalizes to algebras:

Corollary A1.34. Let B be an L-algebra and $A \subseteq B$ a k-subalgebra. Suppose that $X \subseteq A$ is both a k-basis of A and an L-basis of B. Then the isomorphism of L-vector spaces $\varphi \colon A_L \to B$ from Corollary A1.17, which is given on simple tensors by

$$\varphi(l \otimes a) = la$$

for all $l \in L$, $a \in A$, is an isomorphism of L-algebras.

Proof. The inclusion $A \hookrightarrow B$ is a homomorphism of k-algebras, so it follows from Lemma A1.31 that the induced L-linear map $A_L \to B$, which is precisely the isomorphism φ, is a homomorphism of L-algebras. □

Example A1.35. The isomorphisms of L-vector spaces

$$k[X_1, \dots, X_n]_L \to L[X_1, \dots, X_n]\,, \quad \mathrm{M}_n(k)_L \to \mathrm{M}_n(L)\,, \quad k[G]_L \to L[G]$$

from Example A1.18 are all isomorphisms of L-algebras.

Lemma A1.36. Let A be a k-algebra and let $I \trianglelefteq A$ be a left-ideal (resp. right-ideal, resp. both sided ideal). Then I_L is a left-ideal (resp. right-ideal, resp. both sided ideal) in A_L.

Proof. It follows from I being a k-linear subspace of A that I_L is an L-linear subspace of A_L. For all simple tensors $l \otimes a \in A_L$, $l' \otimes x \in I_L$ with $l, l' \in L$, $a \in A$, $x \in I$ we have that

$$(l \otimes a) \cdot (l' \otimes x) = (ll') \otimes (ax) \in L \otimes_k I = I_L\,.$$

It follows that $A_L I_L \subseteq I_L$ because every tensor is a linear combination of simple tensors. This shows that I_L is a left ideal in A_L. The case of I being a right ideal can be treated in the same way, and the case of I being a two-sided ideal follows from the previous two cases. □

Lemma A1.37. Let A be a k-algebra and let $I \trianglelefteq A$ be an ideal generated by elements $(b_j)_{j \in J}$. Then the ideal $I_L \trianglelefteq A_L$ is generated by the elements $(1 \otimes b_j)_{j \in J}$.

Proof. Let I_0 be the ideal in A_L generated by the elements $(1 \otimes b_j)_{j \in J}$. We have that $I_0 \subseteq I_L$ because I_L is an ideal with $1 \otimes b_j \in I_L$ for every $j \in J$. To show that $I_L \subseteq I_0$ we consider the preimage

$$I' \coloneqq \{a \in A \mid 1 \otimes a \in I_0\} = \mathrm{can}_A^{-1}(I_0)\,.$$

This is an ideal in A because can_A is a homomorphism of k-algebras. We have that $b_j \in I'$ for every $j \in J$, and thus $I \subseteq I'$. It follows that $1 \otimes a \in I_0$ for all $a \in I$, and it further follows that $I_L \subseteq I_0$ because these simple tensors generate I_L as an L-vector space. □

Warning A1.38. The ideal $(X^2 + 1)_{\mathbb{R}[X]} \subseteq \mathbb{R}[X]$ is a prime ideal, but the ideal $(X^2 + 1)_{\mathbb{C}[X]} \subseteq \mathbb{C}[X]$ is not. This shows that for a prime (resp. maxmial) ideal $P \trianglelefteq A$ the ideal $P_L \trianglelefteq A_L$ is not necessarily prime (resp. maximal).

Ring Theory and Module Theory

A2. Noetherian and Artinian Modules and Rings

A2.1. Noetherian and Artinian Modules

Conventions A2.1. We denote by R, S a rings (unitary, but not necessarily commutative). By *R-modules* we mean left R-modules.

Lemma A2.2. For an R-module M the following conditions are equivalent:

a) Every submodule $N \subseteq M$ is finitely generated.

b) The module M satisfies the *ascending chain condition*: Every ascending sequence

$$N_1 \leq N_2 \leq N_3 \leq N_4 \leq \cdots$$

of submodules $N_i \subseteq M$ stabilizes.

c) Every non-empty collection $\mathcal{S}$ of submodules of M has a maximal element, i.e. there exists some $N_0 \in \mathcal{S}$ such that there exists no $N \in \mathcal{S}$ with $N \gneq N_0$.

Proof.

a) $\implies$ b): The union $N := \bigcup_{i \geq 1} N_i$ is a submodule of M and therefore finitely generated. Let $n_1, \dots, n_s \in N$ be a finite generating set. Then there exists some $j \geq 1$ with $n_i \in N_j$ for all $i = 1, \dots, s$. It follows that $N = \langle n_1, \dots, n_s \rangle \subseteq N_j \subseteq N$ and therefore $N = N_j$. It follows that for every $i \geq j$ that $N_j \leq N_j \leq N = N_j$ and therefore $N_i = N_j$. This shows that the sequence stabilizes.

b) $\implies$ c): Suppose that there exists a non-empty collection $\mathcal{S}$ of submodules of M which has no maximal element. By starting with any $N_1 \in \mathcal{S}$ there then exists for every $i \geq 1$ some $N_{i+1} \in \mathcal{S}$ with $N_i \subsetneq N_{i+1}$. Then the ascending sequence

$$N_1 \lneq N_2 \lneq N_3 \lneq N_4 \lneq \cdots$$

of submodules of M does not stabilize.

c) $\implies$ a): Let $N \leq M$ be submodule and let

$$\mathcal{S} = \{N' \leq N \,|\, N' \text{ is a finitely generated submodule}\}.$$

The collection $\mathcal{S}$ is non-empty because $0 \in \mathcal{S}$. It follows that N contains a maximal element N'. If $N \neq N'$ then $N' \lneq N$ so there exists some $n \in N$ with $n \notin N'$. Then $N'' := N' + \langle n \rangle$ is a finitely generated submodule of N with $N' \lneq N''$, contradicting the maximality of N. □

Definition A2.3. An R-module M is *noetherian* if it satisfies one (and thus all) of the conditions from Lemma A2.2.

Lemma A2.4. For an R-module M the following conditions are equivalent:

a) The module M satisfies the *descending chain condition*: Every descending sequence

$$N_1 \geq N_2 \geq N_3 \geq \cdots$$

of submodules of N stabilizes.

b) Every non-empty collection $\mathcal{S}$ of submodules of M has a minimal element, i.e. there exists some $N_0 \in \mathcal{S}$ such that there exist no $N \in \mathcal{S}$ with $N \gneq N_0$.

Proof.

a) $\implies$ b) Suppose that there exists a non-empty collection $\mathcal{S}$ of submodules of M which has no minimal element. Then by starting with any $N_0 \in \mathcal{S}$ there exists for every $i \geq 0$ some $N_{i+1} \in \mathcal{S}$ with $N_i \lneq N_{i+1}$. Then

$$N_1 \lneq N_2 \lneq N_3 \lneq \cdots$$

is a decreasing sequence which does not stabilize.

b) $\implies$ a) The collection of submodules $\mathcal{S} = \{N_i \,|\, i \geq 0\}$ is non-emtpy and therefore has a minimal element, i.e. there exists some $j \geq 0$ with $N_i \geq N_j$ for every $i \geq j$. It then follows that $N_i = N_j$ for all $i \geq j$, which shows that the sequence stabilizes. □

Definition A2.5. An R-module M is *artinian* if it satisfies one (and thus all) of the conditions from Lemma A2.4.

Lemma A2.6. Let M be an R-module with submodule $N \leq M$ and let $\pi\colon M \to M/N$ be the canonical projection. If $P_1, P_2 \leq M$ are submodules with $P_1 \leq P_2$ such that $P_1 \cap N = P_2 \cap N$ and $\pi(P_1) = \pi(P_2)$ then $P_1 = P_2$.

First proof. For $p_2 \in P_2$ it follows from $\pi(P_2) = \pi(P_1)$ that there exists some $p_1 \in P_1$ with $\pi(p_1) = \pi(p_2)$, and thus some $n \in N$ with $p_2 - p_1 = n$. It then follows that $n = p_2 - p_1 \in P_2 - P_1 = P_2$ and therefore that $n \in N \cap P_2 = N \cap P_1$. We thus have that $n \in P_1$ and therefore that $p_2 = p_1 + n \in P_1$. □

Second proof. The following commutative diagram has exact rows:

$$\begin{tikzcd}
0 \arrow[r] & N \cap P_1 \arrow[r] \arrow[d, equal] & P_1 \arrow[r, "\pi"] \arrow[d, hook] & \pi(P_1) \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & N \cap P_2 \arrow[r] & P_2 \arrow[r, "\pi"] & \pi(P_2) \arrow[r] & 0
\end{tikzcd}$$

It follows from the five lemma that the inclusion $P_1 \hookrightarrow P_2$ is an isomorphism. □

Proposition A2.7. If

$$0 \to N \xrightarrow{f} M \xrightarrow{g} P \to 0 \tag{A2.1}$$

is a short exact sequence of R modules then M is noetherian (resp. artinian) if and only if both N and P are noetherian (resp. artinian).

Proof. We only show the noetherian part of the statement, the artinian part can be shown in the same way.

Suppose that M is noetherian. Then every increasing sequence of submodules of N is also an increasing sequence of submodules of M and thus stabilizes. This shows that N is noetherian. To show that P is noetherian let $\pi\colon M \to P$ denote the canonical projection and let

$$P_1 \leq P_2 \leq P_3 \leq \cdots$$

be an increasing sequence of submodules $P_i \leq P$. Then the modules $\pi^{-1}(P_i)$ form an increasing sequence of submodules of M, which stabilizes. It then follows from $P_i = \pi(\pi^{-1}(P_i))$ that the original sequence also stabilizes.

Suppose that both N, P are noetherian and let

$$M_1 \leq M_2 \leq M_3 \leq \cdots$$

be an increasing sequence of submodules $M_i \leq M$. It then follows that the modules $\pi(M_i)$ form an increasing sequence of submodules of P and that the modules $M_i \cap N$ form increasing sequece of submodules of N. Both of this sequence stabilize, so there exists some $j \geq 0$ with $N \cap M_i = N \cap M_j$ and $\pi(M_i) = \pi(M_j)$ for all $i \geq j$. It then follows from Lemma A2.6 that $M_i = M_j$ for all $i \geq j$. □

Corollary A2.8. For all noetherian (resp. artinian) R-modules M, N their direct sum $M \oplus N$ is again noetherian (resp. artinian).

Proof. Apply Corollary A2.7 to the short exact sequence

$$0 \to M \xrightarrow{i} M \oplus N \xrightarrow{p} N \to 0$$

given by $i(m) = (m, 0)$ and $p(m, n) = n$. □

A2.9. For noetherian modules an alternative proof of Proposition A2.7 can be given as follows:

Lemma A2.10. Let

$$0 \to N \to M \to P \to 0$$

be a short exact sequence of R-modules.

a) If M is finitely generated then P is also finitely generated.

b) If both N and P are finitely generated then M is finitely generated.

Proof. We may assume w.l.o.g. that N is a submodule of M and that $P = M/N$.

a) If M is generated by $m_1, \dots, m_s$ then M/N is generated by $\overline{m_1}, \dots, \overline{m_s}$.

b) If N is generated by $m_1, \dots, m_s$ and M/N is generated by $\overline{m_{s+1}}, \dots, \overline{m_t}$ then M is generated by $m_1, \dots, m_t$: Let $m \in M$. Then there exist $r_{s+1}, \dots, r_t \in R$ with

$$\overline{m} = r_{s+1}\overline{m_{s+1}} + \cdots + r_t\overline{m_t} = \overline{r_{s+1}m_{s+1} + \cdots + r_t m_t}\,.$$

It follows that $m - (r_{s+1}m_{s+1} + \cdots + r_t m_t) \in N$, so there exist $r_1, \dots, r_s \in R$ with

$$m - (r_{s+1}m_{s+1} + \cdots + r_t m_t) = r_1 m_1 + \cdots + r_s m_s\,.$$

We therefore have that $m = r_1 m_1 + \cdots + r_t m_t$. □

Alternative proof of Proposition A2.7. Suppose that the module M is noetherian. We may assume w.l.o.g. than N is a submodule of M and that $P = M/N$. Every submodule of N is then also a submodule of M and therefore finitely generated. This shows that N is notherian. Every submodule $P' \leq P = M/N$ is of the form $P' = M'/N$ for some submodule $M' \leq M$. The module M' is then finitely generated and it follows from Lemma A2.10 that the module $M'/N = P'$ is also finitely generated. This shows that P is noetherian.

Suppose that the modules N, P are noetherian and let $M' \leq M$ be a submodule. Then $N' \coloneqq f^{-1}(M')$ and $P' \coloneqq g(M')$ are submodules of N', resp. P' and the short extact sequence (A2.1) restrict to a short exact sequence

$$0 \to N' \to M' \to P' \to 0\,.$$

The modules N', P' are finitely generated because N, P are notherian, so it follows from Lemma A2.10 that M' is finitely generated. This shows that M is noetherian. □

A2.2. Noetherian and Artinian Rings

Definition A2.11. A ring R is *noetherian* (resp. *artinian*) if it is noetherian (resp. *artinian*) as an R-module.

Lemma A2.12. If R is noetherian (resp. artinian) then every finitely generated R-module is noetherian (resp. artinian).

Proof. It follows from Corollary A2.8 that $R^{\oplus n}$ is noetherian for every $n \geq 0$. An R-module is finitely-generated if and only if it is isomorphic to $R^{\oplus n}/N$ for some $n \geq 0$ and submodule $N \subseteq R^{\oplus n}$, so the lemma follows from Corollary A2.7. □

Example A2.13.

a) Every field and skew field is both noetherian and artinian.

b) Every principal ideal ring is noetherin, but not necessarily artinian: In $\mathbb{Z}$ the decreasing sequence of ideals

$$(1) \gneq (2) \gneq (4) \gneq \cdots \gneq (2^i) \gneq (2^{i+1}) \gneq \cdots$$

does not stabilize.

c) The following example is taken (with slight modifications) from [AM15, Chapter 6]: Let p be prime and consider the $\mathbb{Z}$-module $M := \mathbb{Z}[1/p]/\mathbb{Z}$, i.e. the $\mathbb{Z}$-submodule of $\mathbb{Q}/\mathbb{Z}$ given by all residue classes

$$M = \left\{ \left[\frac{a}{p^n} \right] \,\middle|\, a \in \mathbb{Z}, n \geq 0 \right\}.$$

Then M is artinian but not noetherian:

We have in $\mathbb{Q}$ the increasing sequence of submodules

$$\mathbb{Z} \lneq \frac{\mathbb{Z}}{p} \lneq \frac{\mathbb{Z}}{p^2} \lneq \cdots \lneq \frac{\mathbb{Z}}{p^i} \lneq \cdots$$

which does not stabilize; it follows that

$$0 \lneq \left(\frac{\mathbb{Z}}{p} \middle/ \mathbb{Z} \right) \lneq \left(\frac{\mathbb{Z}}{p} \middle/ \mathbb{Z} \right) \lneq \cdots \lneq \left(\frac{\mathbb{Z}}{p^i} \middle/ \mathbb{Z} \right) \lneq \cdots$$

is an increasing sequence of submodules of M which does not stabilize. This shows that M is not noetherian.

To see that M in artinian let $m \in M$ with $m = [a/p^i]$ for some $a \in \mathbb{Z}$, $i \geq 0$. If $a = 0$ then $m = 0$. Otherwise we may write $a = p^j b$ with b being coprime to p. Then $[a/p^i] = [p^{j-i} b] = 0$ if $j \geq i$ and $[a/p_i] = [b/p^{i-j}]$ if $j \leq i$. In the second case there exist coefficients $x, y \in \mathbb{Z}$ with $1 = xb + yp^i$ from which it then follows that

$$x \left[\frac{b}{p^{i-j}} \right] = \left[\frac{xb}{p^{i-j}} \right] = \left[\frac{xb + yp^i}{p^{i-j}} \right] = \left[\frac{1}{p^{i-j}} \right].$$

This shows that every cyclic submodule of M is either M itself or of the form

$$M_i := \left\langle \left[\frac{1}{p^i} \right] \right\rangle = \left\{ \left[\frac{a}{p^i} \right] \,\middle|\, a \in \mathbb{Z} \right\} = \left\{ \left[\frac{a}{p^i} \right] \,\middle|\, a = 0, \dots, p^i - 1 \right\}$$

for some $i \geq 0$.

Note that $M_i \leq M_{i+1}$ for all $i \geq 0$ and that $M = \bigcup_{i \geq 0} M_i$. Because every submodule of M is a sum of cyclic submodules it thus further follows the only proper submodules of M are the M_i for $i \geq 0$.

For every descreasing sequence

$$N_1 \geq N_2 \geq N_3 \geq \cdots$$

of submodules $N_i \leq M$ there are now two possible cases to consider: If $N_i = M$ for every $i \geq 0$ then the sequence is already constant. Otherwise there exists some $i \geq 0$ for which N_i is a proper submodule. Then $N_i = M_j$ for some $j \geq 0$ and it follows from the finiteness of M_j that the sequence stabilizes.

Altogether this shows that M is artinian.

d) If $R_1, \dots, R_n$ are rings then $R_1 \times \cdots \times R_n$ is noetherian (resp. artinian) if and only if $R_1, \dots, R_n$ are noetherian (resp. artinian) because every ideal in $R_1 \times \cdots \times R_n$ is of the form $I_1 \times \cdots \times I_n$ for some ideals $I_j \trianglelefteq R_j$.

e) The ring

$$R = \begin{bmatrix} \mathbb{Q} & \mathbb{Q} \\ & \mathbb{Z} \end{bmatrix} = \left\{ \begin{bmatrix} x & y \\ & n \end{bmatrix} \,\middle|\, x, y \in \mathbb{Q}, n \in \mathbb{Z} \right\}$$

is left noetherian but not right noetherian.

To see that R is left noetherian note that

$$I = \begin{bmatrix} \mathbb{Q} & 0 \\ & 0 \end{bmatrix}$$

is a left ideal in R. For every $x \in \mathbb{Q}$ with $x \neq 0$ we have that $\mathbb{Q}x = \mathbb{Q}$, so it follows for every $x \in I$ with $x \neq 0$ that $Rx = I$. It follows that the only subideals of I are 0 and I itself, from which it follows that I is noetherian. By Corollary A2.7 it thus sufficies to show that the R-module

$$R/I \cong \begin{bmatrix} 0 & \mathbb{Q} \\ & \mathbb{Z} \end{bmatrix} =: M$$

is noetherian. Note that

$$N := \begin{bmatrix} 0 & \mathbb{Q} \\ & 0 \end{bmatrix}$$

is a submodule of M, which is noetherian by the same argumentation as for I. By Corollary A2.7 it thus sufficies to show that M/N is noetherian. We have that $M/N \cong \mathbb{Z}$ as abelian groups, so every submodule of M/N is already cyclically generated as an abelian group. This shows that M/N is noetherian.

The ring R is not right noetherian because

$$J_n := \begin{bmatrix} 0 & \mathbb{Z}[1/2^n] \\ & 0 \end{bmatrix}$$

is a right ideal in R for every $n \geq 1$ such that the sequence

$$J_1 \subsetneq J_2 \subsetneq J_3 \subsetneq \cdots$$

does not stabilize.

Remark A2.14. The attentive reader will have noticed that we did not give an example for a ring which is artinian but not noetherian. Such examples are hard to construct because they don't exist: The theorem of Hopkins–Levitzki assures that every artinian ring is already noetherian. A proof of this can be found in [Lam91, Theorem 4.15]

We have seen in Example A2.13, part b) that the converse does not hold, i.e. that noetherian rings are not necessarily artinian. We have also seen in part c) that the analogous statement for modules does not hold, i.e. that not every artinian module needs to be noetherian.

Remark A2.15. Part e) of Example A2.13 can be generalized as follows: If R, S are rings and M is an R-S-bimodule then it follows that

$$A = \begin{bmatrix} R & M \\ & S \end{bmatrix}$$

is a ring via naive matrix addition and multiplication. It can then be shown that A is left (resp. right) noetherian if and only if R, S are both left (resp. right) noetherian and M is noetherian as a left R-module (resp. right S-module). (See [Lam91, Theorem 1.22].)

In our previous example we have the situation that $\mathbb{Q}$ is noetherian as a left $\mathbb{Q}$-module but not noetherian as a right $\mathbb{Z}$-module (as shown in part c) of Example A2.13), which then implies that the constructed ring is left noetherian but not right noetherian.

A2.3. Hilbert's Basis Theorem

A2.16. One of the fundamental theorems about noetherian rings is Hilbert's basis theorem. It is so important that we give two proofs.

Theorem A2.17 (Hilbert's basis theorem)**.** If R is a noetherian ring, then the polynomial ring $R[X]$ is also noetherian.

First proof: For every degree $d \geq 0$ let

$$I_d := \left\{ a \in R \,\middle|\, \text{there exists some polynomial } \sum_{i=0}^{d} a_i X^i \in I \text{ mit } a_d = a \right\}.$$

Then I_d is an ideal in R for every $d \geq 0$, because it is the image of the map $R[X]_{\leq d} \to R$, $\sum_{i=0}^{d} a_i X^i \to a_d$ which is a homomorphism of R-modules.

For $a \in I_d$ there exists a polynomial $f \in I$ of degree $\deg(f) \leq d$ whose d-th coefficient is a. Then $Xf \in I$ is a polynomial of degree $\deg(Xf) \leq d+1$ whose $(d+1)$-th coefficient is a. This shows that $I_d \subseteq I_{d+1}$, so that

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

is an increasing sequence of ideals $I_d \trianglelefteq R$.

This sequence stabilizes because R is noetherian, so there exists some $D \geq 0$ with $I_d = I_D$ for all $d \geq D$. The ideals $I_0, \dots, I_D$ are finitely generated because R is noetherian. For every $d = 0, \dots, D$ let $a_{d,1}, \dots, a_{d,n(d)} \in I_d$ with $I_d = (a_{d,1}, \dots, a_{d,n(d)})$ and $a_{d,j} \neq 0$ for all $j = 1, \dots, n(d)$. For every $d = 0, \dots, D$ let $f_{d,1}, \dots, f_{d,n(d)} \in I$ be polynomials of degree $\deg(f_{d,j}) = d$ with leading coefficient $a_{d,j}$.

We show for $J := (f_{d,j} \,|\, d = 0, \dots, D, j = 1, \dots, n(d))$ that $I = J$, which shows that I is finitely generated. That $J \subseteq I$ follows from $f_{d,j} \in I$.

To show the other inclusion let $f \in I$. We show that $f \in J$ by induction over the degree $d := \deg(f)$. If $d = -\infty$ then $f = 0$ and thus $f \in J$. For $d \geq 1$ let a_d be the leading coefficient of f. We construct a polynomial $g \in J$ with the same leading coefficient and degree as f by distinguishing between two cases:

- Suppose that $d \leq D$. Then $a_d \in I_d$ and it follows that there exist $r_1, \dots, r_{n(d)} \in R$ with $a_d = r_1 a_{d,1} + \dots + r_{n(d)} a_{d,n(d)}$. We then set $g \coloneqq r_1 f_{d,1} + \dots + r_{n(d)} f_{d,n(d)}$.
- Suppose that $d \geq D$. Then $a_d \in I_d = I_D$ so there exist $r_1, \dots, r_{n(D)} \in R$ with $a_d = r_1 a_{D,1} + \dots + r_D a_{D,n(D)}$. We then set $g \coloneqq (r_1 f_{D,1} + \dots + r_D f_{D,n(D)}) X^{d-D}$.

It follows that $\deg(f-g) \leq d-1$ and therefore that $f - g \in J$ by the induction hypothesis. It follows that $f = (f-g) + g \in J$. □

Second proof: Suppose that there exist an ideal $I \trianglelefteq R[X]$ which is not finitely generated. Starting with $f_0 \coloneqq 0$ there exists for every $n \geq 0$ some polynomial $f_{n+1} \in I$ with $f_{n+1} \notin (f_0, \dots, f_n)$ of minimal degree. Then $\deg(f_n) \leq \deg(f_{n+1})$ for all $n \geq 0$.

For every $n \geq 0$ let $a_n \in R$ be the leading coefficient of f_n. Then

$$0 = (a_0) \subseteq (a_0, a_1) \subseteq (a_0, a_1, a_2) \subseteq \cdots$$

is an increasing sequence of ideals in R and thus stabilizes. It follows that there exists some $m \geq 0$ with $a_{m+1} \in (a_0, \dots, a_m)$ and therefore $a_{m+1} = r_0 a_0 + \dots + r_m a_m$ for suitable $r_0, \dots, r_m \in R$. The polynomial

$$g \coloneqq \sum_{n=0}^{m} r_n f_n X^{\deg(f_{m+1}) - \deg(f_n)} \in (f_0, \dots, f_n)$$

has the same degree and leading coefficient as f_{m+1} so that $\deg(f_{m+1} - g) < \deg(f_{m+1})$. But it follows from $f_{m+1} \notin (f_0, \dots, f_m)$ and $g \in (f_0, \dots, f_m)$ that

$$f_{m+1} - g \notin (f_0, \dots, f_m)\,,$$

which contradicts the degree-minimality of f_{n+1}. □

Remark A2.18. The main idea in both proofs of Hilbert's basis theorem is to consider ideals in the original ring R which are generated by leading coefficients of polynomials in $I \trianglelefteq R[X]$. This idea leads to the theory of *Gröbner bases*, which are a powerful tool in (computational) commutativ algebra. The author can recommend [DF04, Section 9.6] for a short introduction to Gröbner bases.

Example A2.19. If k is a field then $k[X_1, \dots, X_n]$ is noetherian for every $n \geq 0$.

Example A2.20. If k is a field then the polynom ring $R \coloneqq k[X_1, X_2, X_3, \dots]$ in countable many variables is not noetherian because the ideal $I \coloneqq (X_1, X_2, X_3, \dots)$ is not finitely generated: Supose that the ideal I were generated by $f_1, \dots, f_n \in I$. In each of the polynomials f_i only finitely many variables occur, so there exists some $m \geq 1$ with $f_1, \dots, f_n \in (X_1, \dots, X_m)$ (note that the polynomials f_i have no constant coefficient because $f_i \in I$). Then $I = (X_1, \dots, X_m)$ and it would follows that

$$\begin{aligned} R \cong k[X_{m+1}, X_{m+2}, X_{m+3}, \dots] &\cong k[X_1, X_2, X_3, \dots]/(X_1, \dots, X_m) \\ &= k[X_1, X_2, X_3, \dots]/(X_1, X_2, X_3, \dots) \cong k\,, \end{aligned}$$

but R is not a field.

Lemma A2.21. If R is noetherian and $I \trianglelefteq R$ is a two-sided ideal then the ring R/I is again noetherian.

Proof. The ring R is noetherian as an R-module so R/I is also noetherian as an R-module. The R/I-submodules of R/I are precisely the R-submodules of R/I, so it follows that R/I is also noetherian as an R/I-module. □

Corollary A2.22. If R is a noetherian commutative ring then every finitely generated R-algebra is again noetherian.

Proof. If A is a finitely generated R-algebra then $A \cong R[X_1, \ldots, X_n]/I$ as R-algebras for some $n \geq 0$ and some ideal $I \trianglelefteq R[X_1, \ldots, X_n]$. The R-algebra $R[X_1, \ldots, X_n]$ is noetherian by Hilbert's basis theorem and it follows that $R[X_1, \ldots, X_n]/I$ is noetherian by Lemma A2.21. □

A3. Zariski's Lemma

Lemma A3.1. Let $A \subseteq B \subseteq C$ be commutative rings such that C is finitely generated as an A-algebra. If A is noetherian and C is finitely generated as a B-module then B is also finitely generated as an A-algebra.

Proof. We will construct a ring B_0 with $A \subseteq B_0 \subseteq B$ such that B_0 is finitely generated as an A-algebra, say $B_0 = A[b'_1, \ldots, b'_s]$ for suitable $b'_i \in B_0$, and C is finitely generated as an B_0-module. It then follows from Corollary A2.22 that B_0 is noetherian because A is noetherian, and that C is noetherian as a B_0-module by Lemma A2.12. Then the B_0-submodule $B \subseteq C$ is also finitely generated as an B_0-module, say $B = B_0 b_1 + \cdots + B_0 b_t$ for suitable $b_1, \ldots, b_t \in B$. It then follows that B is finitely generated as an A-algebra because

$$\begin{aligned} B &= B_0 b_1 + \cdots + B_0 b_t \\ &= A[b'_1, \ldots, b'_s] b_1 + \cdots + A[b'_1, \ldots, b'_s] b_t \\ &\subseteq A[b'_1, \ldots, b'_s, b_1, \ldots, b_t] \subseteq B\,. \end{aligned}$$

To construct B_0 we use that

$$C = A[x_1, \ldots, x_n] = By_1 + \cdots + By_m$$

for suitable $x_i, y_j \in C$. It then follows that there exist coefficients $b_{ij} \in B$ with

$$x_i = \sum_{j=1}^{m} b_{ij} y_j$$

for every $i = 1, \ldots, n$, as well as coefficients $b_{ijk} \in B$ with

$$y_i y_j = \sum_{k=1}^{m} b_{ijk} y_k$$

for all $i, j = 1, \dots, m$. Let B_0 be the A-subalgebra of B generated by all b_{ij}, b_{ijk}.

Then B_0 is finitely generated as an A-algebra by construction and we need to show that C is finitely generated as a B_0-module. We have that

$$C = A[x_1, \dots, x_n] \subseteq B_0[y_1, \dots, y_m]$$

because $A \subseteq B_0$ and $x_i = \sum_{j=1}^m b_{ij} y_i \in B_0[y_1, \dots, y_m]$ for every $i = 1, \dots, n$. It further follows from $A \subseteq B_0$ and

$$y_i y_j = \sum_{k=1}^m b_{ijk} y_k \in B_0 y_1 + \cdots + B_0 y_m$$

for all $i, j = 1, \dots, m$ that $B_0 + B_0 y_1 + \cdots + B_0 y_m$ is an A-subalgebra of B which contains $y_1, \dots, y_m$, so that

$$B_0[y_1, \dots, y_m] \subseteq B_0 + B_0 y_1 + \cdots + B_0 y_m \,.$$

Together this shows that

$$C \subseteq B_0 + B_0 y_1 + \cdots + B_0 y_m \subseteq C$$

and thus $C = B_0 + B_0 y_1 + \cdots + B_0 y_m$. □

Lemma A3.2. Let R be a unique factorizaton domain which contains infinitely many non-associated primes and let K be the field of fractions of R. Then K is not finitely generated as an R-algebra.

Proof. Let $f_1, \dots, f_n \in K$ with $f_i = g_i/h_i$ where $g_i, h_i \in R$ with $h_i \neq 0$. We have that

$$\begin{aligned} R[f_1, \dots, f_n] = R\left[\frac{g_1}{h_1}, \dots, \frac{g_n}{h_n}\right] &= R\left[\frac{g_1 h_2 \cdots h_n}{h_1 \cdots h_n}, \dots, \frac{h_1 \cdots h_{n-1} g_n}{h_1 \cdots h_n}\right] \\ &\subseteq R\left[\frac{1}{h_1 \cdots h_n}\right] \end{aligned}$$

and it follows that every element $f \in R[f_1, \dots, f_n]$ is of the form

$$f = \frac{g}{(h_1 \cdots h_n)^m}$$

for some $g \in R$, $m \geq 0$. There exists some $h \in R$ which is prime and does not divide any h_i because R contains infinitely many non-associated primes. For all $g \in R$, $m \geq 0$ it follows that $gh \neq (h_1 \cdots h_n)^m$ and therefore that

$$\frac{g}{(h_1 \cdots h_n)^m} \neq \frac{1}{h} \,.$$

This shows that $1/h \notin R[f_1, \dots f_n]$ and thus $R[f_1, \dots, f_n] \subsetneq K$. □

Remark A3.3. The converse of Lemma A3.2 also holds: If R is a unique factorization domain which contains only finitely non-associated primes $p_1, \dots, p_n \in R$ then $K = R[p_1^{-1}, \dots, p_n^{-1}]$ is finitely generated as an R-algebra.

Example A3.4. If k is a field and $n \geq 1$ then $k(X_1, \dots, X_n)$ is not finitely generated as a $k[X_1, \dots, X_n]$-algebra by Lemma A3.2 because $k[X_1, \dots, X_n]$ contains infinitely many non-associated primes. Then $k(X_1, \dots, X_n)$ is also not finitely generated as a k-algebra.

Corollary A3.5 (Zariski's lemma)**.** Let L/k be a field extension. If L is finitely generated as a k-algebra then the field extension L/k is already finite.

Proof. We have that $L = k[x_1, \dots, x_n]$ for some suitable elements $x_1, \dots, x_n \in L$. The set $\{x_1, \dots, x_n\}$ contains a maximal subset which is algebraically independent over k. We may assume w.l.o.g. that there exists some $0 \leq r \leq n$ such that $x_1, \dots, x_r$ are algebraically independent over L while $x_1, \dots, x_r, x_k$ are algebraically dependent for every $r < k \leq n$.

It follows for $F \coloneqq k(x_1, \dots, x_r)$ that $x_{r+1}, \dots, x_n$ are algebraic over F. The field extension L/F is therefore finite because $L = F(x_{r+1}, \dots, x_n)$ is generated by finitely many algebraic elements.

We can now apply Lemma A3.1 to $k \subseteq F \subseteq L$ to conclude that F is finitely generated as a k-algebra. We have that $F \cong k(X_1, \dots, X_r)$ as k-algebras because $x_1, \dots, x_r$ are algebraically independent so it follows that $k(X_1, \dots, X_r)$ is finitely generated as a k-algebra. By Example A3.4 this can only happen for $r = 0$.

This shows that $F = k$ and that L/F is finite. □

Remark A3.6. Another proof of Zariski's Lemma which uses the concept of integral dependece can be found in [AM15, Corollary 5.24].

A4. The Opposite Ring

Conventions A4.1. In the following R, S denote rings.

Definition A4.2. The *opposite ring* R^{op} has the same underlying additive group as R and the multiplication $*$ is given by

$$a * b \coloneqq b \cdot a = ba$$

for all $a, b \in R^{\mathrm{op}}$, where $\cdot$ denotes the multiplication of R.

Notation A4.3. If we regard an element $a \in R$ as an element of R^{op} then we often write a^{op} instead of a. For all $a, b \in R$ the multiplication of R can the be expressed as

$$a^{\mathrm{op}}\, b^{\mathrm{op}} = ba\,.$$

Note that the multiplication on the left hand side is the one of R^{op} whereas the on the right hand side is the one of R. We will try to avoid expressions of the form $a^{\mathrm{op}}b$ with $a, b \in R$ for which it is not clear which multiplication is to be used.

Lemma A4.4.

a) We have that $(R^{\mathrm{op}})^{\mathrm{op}} = R$.

b) The ring R is commutative if and only if $R = R^{\mathrm{op}}$.

c) If D is a skew field then D^{op} is also a skew field.

d) For every family of rings $(R_i)_{i\in I}$ we have that $(\prod_{i\in I} R_i)^{\mathrm{op}} = \prod_{i\in I} R_i^{\mathrm{op}}$. □

Definition A4.5. A map $f\colon R \to S$ is an *antihomomorphism of rings* if f is additive with

$$f(ab) = f(b)f(a)$$

for all $a, b \in R$. If f is additionally bijective then f is an *antiisomorphism of rings*.

Example A4.6.

a) The map $R \to R^{\mathrm{op}}$, $a \mapsto a^{\mathrm{op}}$ is an antiisomorphism.

b) If $f\colon R \to S$ and $g\colon S \to T$ are antihomomorphisms then $g \circ f$ is a homomorphism. If one of the maps f, g is an antihomomorphism and the other is a homomorphism then the composition $g \circ f$ is an antihomomorphism.

c) If $f\colon R \to S$ is an antiisomorphism then $f^{-1}\colon S \to R$ is again an antiisomorphism.

Lemma A4.7. For any map $f\colon R \to S$ the following conditions are equivalent:

a) The map f is a homomorphism $R \to S$.

b) The map f is an antihomomorphism $R \to S^{\mathrm{op}}$.

c) The map f is an antihomomorphism $R^{\mathrm{op}} \to S$.

d) The map f is a homomorphism $R^{\mathrm{op}} \to S^{\mathrm{op}}$. □

Lemma A4.8. The map

$$\mathrm{M}_n(R)^{\mathrm{op}} \to \mathrm{M}_n(R^{\mathrm{op}}), \quad A^{\mathrm{op}} = ((A_{ij})_{ij})^{\mathrm{op}} \mapsto (A_{ji}^{\mathrm{op}})_{ij} = A^T$$

is an isomorphism of rings.

Proof. The map $\mathrm{M}_n(R) \to \mathrm{M}_n(R^{\mathrm{op}})$, $A \mapsto A^T$ is an antiisomorphism of rings and thus results in an isomorphism of rings $\mathrm{M}_n(R)^{\mathrm{op}} \to \mathrm{M}_n(R^{\mathrm{op}})$, $A^{\mathrm{op}} \mapsto A^T$. □

Remark A4.9. If I is any index set then we similarly get an isomorphism

$$\mathrm{M}_I^{\mathrm{cf}}(R)^{\mathrm{op}} \to \mathrm{M}_I^{\mathrm{rf}}(R^{\mathrm{op}}), \quad A^{\mathrm{op}} = ((A_{ij})_{ij})^{\mathrm{op}} \mapsto (A_{ji}^{\mathrm{op}})_{ij} = A^T\,,$$

where $\mathrm{M}_I^{\mathrm{cf}}(R)$ and $\mathrm{M}_I^{\mathrm{rf}}(R^{\mathrm{op}})$ denote the rings of column finite, resp. row finite $(I \times I)$-matrices with coefficients in R, resp. R^{op} (see Definition A7.22 and Lemma A7.23).

Lemma A4.10. The map

$$\Phi\colon R^{\mathrm{op}} \to \mathrm{End}_R(R), \quad a^{\mathrm{op}} \mapsto (x \mapsto xa)$$

is an isomorphism of rings with inverse given by $\varphi \mapsto \varphi(1)^{\mathrm{op}}$.

Proof. The additivity of $\Phi(a^{\mathrm{op}})$ for every $a \in R$ follows from the distributivity of R, and for every $a \in R$ we have that

$$\Phi(a^{\mathrm{op}})(rx) = rxa = r\Phi(a^{\mathrm{op}}(x)$$

for all $r \in R$, $x \in R$. Together this shows that $\Phi(a^{\mathrm{op}})$ is R-linear for every $a \in R$, which shows that Φ is well-defined.

The additivity of Φ also follows from the distributivity of R, and we have that $\Phi(1_{R^{\mathrm{op}}}) = \Phi(1_R^{\mathrm{op}}) = \mathrm{id}_R$. We have that

$$\begin{aligned}\Phi(a^{\mathrm{op}}b^{\mathrm{op}})(x) = \Phi((ba)^{\mathrm{op}})(x) = xba &= \Phi(a^{\mathrm{op}})(xb) \\ &= \Phi(a^{\mathrm{op}})(\Phi(b^{\mathrm{op}})(x)) = (\Phi(a^{\mathrm{op}}) \circ \Phi(b^{\mathrm{op}}))(x)\end{aligned}$$

for all $a, b \in R$, $x \in R$, which shows that Φ is multiplicative.

For every $a \in R$ we have that $\Phi(a^{\mathrm{op}})(1) = a$, which shows that Φ is injective. For every $\varphi \in \mathrm{End}_R(R)$ we have for $a \coloneqq \varphi(1)$ that

$$\varphi(x) = \varphi(x \cdot 1) = x \cdot \varphi(1) = xa = \Phi(a^{\mathrm{op}})(x)$$

and thus $\Phi(a^{\mathrm{op}}) = \varphi$. This shows that Φ is surjective. □

Proposition A4.11.

a) Let M be an abelian group. Then a multiplication

$$R \times M \to M, \quad (r, m) \mapsto r \cdot m$$

is a left R-module structure on M if and only if the multiplication

$$M \times R^{\mathrm{op}} \to M, \quad (m, r^{\mathrm{op}}) \mapsto m * r^{\mathrm{op}} \coloneqq r \cdot m$$

is a right R^{op}-module structure on M.

This shows that left modules over R are “the same” as right modules over R^{op}.

b) If M, N are two left R-modules then a map $f\colon M \to N$ is a homomorphism of left R-modules if and only if it is a homomorphism of right R^{op}-modules. □

Remark A4.12. The above proposition shows that the category R-**Mod** of left R-modules is isomorphic to the category **Mod**-R^{op} of right R^{op}-modules.

Example A4.13 (Duality for finite-dimensional modules over k-algebras)**.** Let k be a field and let A be a k-algebra.

For every left A-module M its the dual space M^* carries the structure of a right A-module via

$$(\varphi \cdot a)(m) = \varphi(am)$$

for all $a \in A$, $\varphi \in M^*$, $m \in M$, which then corresponds to a left A^{op}-module structure on M^* given by

$$(a^{\mathrm{op}} * \varphi)(m) = (\varphi \cdot a)(m) = \varphi(am)$$

for all $a \in A$, $\varphi \in M^*$, $m \in M$. If $f\colon M \to N$ is a homomorphis of left A-modules then $f^*\colon N^* \to M^*$ is a homomorphism of right A-modules and therefore a homomorphism of left A^{op}-modules. Together this shows that dualizing results in a contravariant functor

$$(-)^*\colon A\text{-}\mathbf{Mod} \to A^{\mathrm{op}}\text{-}\mathbf{Mod}\,.$$

It similarly follows that for every right A-module M its dual M^* carries the structure of a left A-module via

$$(a \cdot \varphi)(m) = \varphi(ma)$$

for all $a \in A$, $\varphi \in M^*$, $m \in M$, which then corresponds to a right A^{op}-module structure on M^* given by

$$(\varphi * a^{\mathrm{op}})(m) = (a \cdot \varphi)(m) = \varphi(ma)$$

for all $a \in A$, $\varphi \in A$, $m \in M$. As above we find that the dual of a homomorphism of right A-modules is an homomorphism of left A-modules and therefore a homomorphism of right A^{op}-modules.

If M is a left A-module then it follows that M^{**} carries the structure of a left A-module via

$$(a \cdot \beta)(\varphi) = \beta(\varphi \cdot a)$$

for all $a \in A$, $\beta \in (M^*)^*$, $\varphi \in M^*$. The canonical homomorphism

$$\eta_M\colon M \to M^{**}, \quad m \mapsto (\varphi \mapsto \varphi(m))$$

is then a homomorphism of left A-modules because

$$(a \cdot \eta_M(m))(\varphi) = \eta_M(m)(\varphi \cdot a) = (\varphi \cdot a)(m) = \varphi(am) = \eta_M(am)(\varphi)$$

for all $a \in A$, $m \in M$, $\varphi \in M^*$.

The analogous results for right A-modules also hold by similar arguments.

Let A-$\mathbf{Mod_{fd}}$ be the category of finite-dimensional left A-modules and let similary A^{op}-$\mathbf{Mod_{fd}}$ be the category of finite-dimensional A^{op}-modules. It follows from the above discussion that dualizing defines a duality of categories

$$(-)^*\colon A\text{-}\mathbf{Mod_{fd}} \to A^{\mathrm{op}}\text{-}\mathbf{Mod_{fd}}$$

with inverse being again given by dualizing $(-)^*$. So whenever we have a theorem which holds for finite-dimensional modules over an arbitrary k-algebras (or at least for a class of k-algebras which is closed under $(-)^{\mathrm{op}}$) we then get a dual theorem for free. This applies to the following two classes of k-algebras:

a) If G is a group then $k[G]^{\mathrm{op}} = k[G^{\mathrm{op}}] \cong k[G]$ because the antiisomorphism of groups $G \to G$, $g \mapsto g^{-1}$ induces an isomorphism of groups $G^{\mathrm{op}} \to G$, $g^{\mathrm{op}} \mapsto g^{-1}$, which then induces an isomorphism of k-algebras $k[G^{\mathrm{op}}] \to k[G]$. It follows that the category $k[G]$-$\mathbf{Mod}_{\mathbf{fd}}$, which is isomorphic to the category of finite dimensional k-representations of G over k, has an autoduality given by $(-)^*$: If V is a (finite-dimensional) representation of G, then V^* is just the dual representation as defined in Example 2.6.

b) If Q is a quiver then $k[Q]^{\mathrm{op}} \cong k[Q^{\mathrm{op}}]$ and it follows that the cateories of finite dimensional representations of Q and Q^{op} over k are dual to each other via $(-)^*$. This is prominently used in the representation theory of quivers.

A5. Recognizing Direct Sums and Direct Products

Conventions A5.1. In the following R denotes a ring.

A5.2. We give explain under what conditions an R-moudule M can be decomposed into a finite direct sum $M = M_1 \oplus \cdots \oplus M_n$ of submodules $M_1, \dots, M_n \leq M$, and under what conditions the ring R can be decomposed into a finite product $R \cong R_1 \times \cdots \times R_n$ of suitable rings $R_1, \dots, R_n$.

A5.1. Decomposition of Modules

Definition A5.3.

a) An element $e \in R$ is *idempotent* if $e^2 = e$.

b) If X is any set then a map $e \colon X \to X$ is *idempotent* if $e^2 = e$.

Remark A5.4. Note that for an R-module M and an element $e \in \operatorname{End}_R(M)$ both notions of idempotence coincide.

Lemma A5.5. If X is any set then a map $e \colon X \to X$ is idempotent if and only if $e(y) = y$ for every $y \in \operatorname{im}(e)$. □

Definition A5.6. Two elements $r_1, r_2 \in R$ are *orthogonal* if $r_1 r_2 = r_2 r_1 = 0$.

Definition A5.7. A collection of elements $r_1, \dots, r_n \in R$ is *complete* if $1 = r_1 + \cdots + r_n$.

Theorem A5.8. Let M be an R-module.

a) Let $M = M_1 \oplus \cdots \oplus M_n$ be a decomposition into submodules $M_1, \dots, M_n \leq M$. For every $i = 1, \dots, n$ let $e_i \colon M \to M$ be the projection onto the summand M_i alongside this decomposition, i.e. the map e_i is given by

$$e_i(m_1 + \cdots + m_n) = m_i$$

for all $m_1 \in M_1, \dots, m_n \in M_n$. Then $(e_1, \dots, e_n)$ is a complete family of pairwise orthogonal idempotents in $\operatorname{End}_R(M)$.

b) Let on the other hand $(e_1, \dots, e_n)$ be a complete family of pairwise orthogonal idempotents in $\operatorname{End}_R(M)$ and let $M_i \coloneqq \operatorname{im}(e_i)$ for every $i = 1, \dots, n$.

   1) We have that $e_i|_{M_i} = \mathrm{id}_{M_i}$ for every $i = 1, \dots, n$ and $e_j|_{M_i} = 0$ for all $i \neq j$.

   2) We have that $M = M_1 \oplus \cdots \oplus M_n$.

c) The above two constructions result in mutually inverse bijections

$$\left\{ \begin{array}{c} \text{complete families of pairwise} \\ \text{orthogonal idempotents} \\ (e_1, \dots, e_n) \text{ in } \operatorname{End}_R(M) \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{families } (M_1, \dots, M_n) \text{ of} \\ \text{submodules } M_i \leq M \text{ with} \\ M = M_1 \oplus \cdots \oplus M_n \end{array} \right\}.$$

Proof.

a) Every element $m \in M$ can be written as $m = m_1 + \cdots + m_n$ for some elements $m_1 \in M_1, \dots, m_n \in M_n$ and it follows that

$$\mathrm{id}_M(m) = m = m_1 + \cdots + m_n = e_1(m) + \cdots + e_n(m) = (e_1 + \cdots + e_n)(m)$$

which shows that $\mathrm{id}_M = e_1 + \cdots + e_n$. We also have that

$$e_i^2(m) = e_i(m_i) = m_i = e_i(m)$$

for every $i = 1, \dots, n$ which shows that the e_i are idempotent, and we have that

$$e_i(e_j(m)) = e_i(m_j) = 0$$

for all $i \neq j$ which shows that the collection $e_1, \dots, e_n$ is pairwise orthogonal.

b) 1) For every $m_i \in M_i$ there exists $m \in M$ with $m_i = e_i(m)$ and it follows that

$$e_i(m_i) = e_i(e_i(m)) = e_i(m) = m_i$$

and that

$$e_j(m_i) = e_j(e_i(m)) = 0\,.$$

   2) For every $m \in M$ we have that

$$m = \mathrm{id}_M(m) = (e_1 + \cdots + e_n)(m) = e_1(m) + \cdots + e_n(m) \in M + \cdots + M_n\,,$$

   which shows that $M = M_1 + \cdots + M_n$. If $m \in M$ then for every decomposition $m = m_1 + \cdots + m_n$ with $m_1 \in M_1, \dots, m_n \in M_n$ we have that

$$e_i(m) = e_i(m_1 + \cdots + m_n) = e_i(m_1) + \cdots + e_i(m_n) = m_i\,.$$

   This shows that this decomposition $m = m_1 + \cdots + m_n$ is unique, which in turn shows the directness of the sum $M = M_1 + \cdots + M_n$.

c) Let $(e_1, \dots, e_n)$ be a complete family of pairwise orthogonal idempotents, let $M = M_1 \oplus \cdots \oplus M_n$ be the associated decomposition and let $(e'_1, \dots, e'_n)$ be the resulting complete family of pairwise orthogonal idempotents. We then have for all $i = 1, \dots, n$ that

$$e_i|_{M_i} = \mathrm{id}_{M_i} = e'_i|_{M_i}$$

and for all $i \neq j$ that

$$e_i|_{M_j} = 0 = e'_i|_{M_j} \,,$$

which together shows that $e_i = e'_i$ for all $i = 1, \dots, n$.

Let $M = M_1 \oplus \cdots \oplus M_n$ be a decomposition into submodule $M_i \leq M$, let $(e_1, \dots, e_n)$ be the associated complete family of pairwise orthogonal idempotents and let $M = M'_1 \oplus \cdots \oplus M'_n$ be the resulting decomposition. It then follows for every $i = 1, \dots, n$ from $e_i|_{M_i} = \mathrm{id}_{M_i}$ and $e_i|_{M_j} = 0$ for $j \neq i$ that $M_i = \mathrm{im}(e_i) = M'_i$ and therefore that $M_i = M'_i$. □

Corollary A5.9.

a) The map

$$\left\{ \begin{array}{c} \text{complete families of pairwise} \\ \text{orthogonal idempotents} \\ (e_1, \dots, e_n) \text{ in } R \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{families } (I_1, \dots, I_n) \text{ of} \\ \text{left ideals } I_I \leq M \text{ with} \\ R = I_1 \oplus \cdots \oplus I_n \end{array} \right\},$$
$$(e_1, \dots, e_n) \longmapsto (Re_1, \dots, Re_n)$$

is a well-defined bijection.

Let $(I_1, \dots, I_n)$ be a family of left ideals $I_i \leq R$ with $R = I_1 \oplus \cdots \oplus I_n$ and let $(e_1, \dots, e_n)$ be the corresponding complete family of pairwise orthogonal idempotents.

b) The projection onto the summand I_i alongside the decomposition $R = I_1 \oplus \cdots \oplus I_n$ is given by right multiplication with the idempotent e_i.

c) The idempotents $e_1, \dots, e_n$ are the unique elements $e_i \in I_i$ with $1 = e_1 + \cdots + e_n$.

Proof. Part a) and part b) follow from Theorem A5.8 by using the isomorphism $\mathrm{End}_R(R) \cong R^{\mathrm{op}}$ from Lemma A4.10. Part c) follows from part b) by applying the projection onto I_i to the element $1 \in R$. □

Remark A5.10. The analogous result of Corollary A5.9 for right ideal also holds and can be proven in the same way. Note that the left ideals Re_i have to be replaced by the right ideals $e_i R$, and the right multiplication with e_i has to be replaced by the left multiplication with e_i.

Corollary A5.11. If M is an R-module, then the map

$$\{\text{idempotents } e \in \mathrm{End}_R(M)\} \longrightarrow \left\{ \begin{array}{c} \text{pairs } (N, P) \text{ of submodules} \\ N, P \leq M \text{ with } M = N \oplus P \end{array} \right\},$$
$$e \longmapsto (\mathrm{im}(e), \ker(e))$$

is a well-defined bijection. For a pair (N, P) of submodules $N, P \leq M$ with $M = N \oplus P$ the corresponding idempotent $e \in \mathrm{End}_R(M)$ is given by the projection onto N alongside this decomposition.

Proof. This follows from Theorem A5.8 by using the bijection

$$\left\{ \begin{matrix} \text{idempotents} \\ e \in \mathrm{End}_R(M) \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} \text{complete families of pairwise} \\ \text{orthogonal idempotents} \\ (e_1, e_2) \text{ in } \mathrm{End}_R(M) \end{matrix} \quad , \right\}$$

$$\begin{aligned} e &\longmapsto (e, 1 - e)\,, \\ e_1 &\longleftarrow\!\shortmid (e_1, e_2) \end{aligned}$$

and observing that $\mathrm{im}(e_2) = \ker(e_1)$. □

Corollary A5.12. If M is an R-module then for any submodule $N \leq M$ the following conditions are equivalent:

a) The submodule N is a direct summand of M.

b) There exists an idempotent R-module endomorphism $e \colon M \to M$ with $\mathrm{im}\, e = N$.

c) There exists an idempotent R-module endomorphism $e' \colon M \to M$ with $\ker e' = N$.

d) There exists an idempotent R-module endomorphism $e \colon M \to M$ with $\mathrm{im}\, e \leq N$ and $e(n) = n$ for every $n \in N$.

The above endomorphisms e, e' are then related by $e' = 1 - e$. □

A5.2. Decomposition of Rings

Lemma A5.13. Let $R_1, \dots, R_n$ be rings and for every $i = 1, \dots, n$ let

$$I_i \coloneqq 0 \times \cdots \times 0 \times R_i \times 0 \times \cdots \times 0$$

with R_i in the i-th position. Then $I_1, \dots, I_n$ are two-sided ideals in $R_1 \times \cdots \times R_n$ with $R_1 \times \cdots \times R_n = I_1 \oplus \cdots \oplus I_n$. □

A5.14. We will now discuss under what conditions a ring R can be decomposed as $R \cong R_1 \times \cdots \times R_n$ for rings $R_1, \dots, R_n$. We have already seen that $R_1, \dots, R_n$ must appear as two-sided ideals in R.

Definition A5.15. An element $z \in R$ is *central* if $rz = zr$ for every $r \in R$.

Proposition A5.16. Let R be a ring and let $I_1, \dots, I_n \trianglelefteq R$ be two-sided ideals with $R = I_1 \oplus \cdots \oplus I_n$. For every $i = 1, \dots, n$ let $e_i \in I_i$ be the unique elements such that $1 = e_1 + \cdots + e_n$.

a) For all $i \neq j$ we have that $I_i I_j = 0$.

b) Every summand I_i is a ring with the addition and multiplication inherited from R, and $1_{I_i} = e_i$ for every $i = 1, \dots, n$.

c) The map
$$I_1 \times \cdots \times I_n \to R, \quad (x_1, \dots, x_n) \mapsto x_1 + \cdots + x_n$$
is an isomorphism of rings.

d) If $1_R = e_1 + \cdots + e_n$ is the unique decomposition of 1_R with $e_j \in I_j$ for every $j = 1, \dots, n$ then $e_1, \dots, e_n$ is a complete collection of pairwise orthogonal central idempotents of R.

Proof.

a) We have that $I_i I_j \subseteq I_i \cap I_j = 0$.

b) The addition and multiplication of R restrict to I_i it only remains to show that $1_{I_i} = e_i$. We have for $x, y \in R$ with $x = \sum_{i=1}^n x_i$ and $y = \sum_{i=1}^n y_i$ where $x_i, y_i \in I_i$ that $x_i y_j \in I_i I_j = 0$ for all $i \neq j$, and it follows that
$$xy = \sum_{i,j=1}^n x_i y_j = \sum_{i=1}^n x_i \,. \tag{A5.1}$$
It follows for every $x \in I_i$ that
$$x = 1 \cdot x = \sum_{j=1}^n e_j x = e_i x$$
which shows that $1_{I_i} = x$.

c) The map is bijective and additive becaues $R = I_1 \oplus \cdots \oplus I_n$ and Equation (A5.1) shows that the map is also multiplicative.

d) It follows from Equation (A5.1) that $e_i e_j = 0$ for $i \neq j$, and for every $i = 1, \dots n$ we have that $e_i^2 = 1_{I_i}^2 = 1_{I_i} = e_i$. □

Definition A5.17. In the situation of Proposition A5.16 we call R the *internal direct product* of $I_1, \dots, I_n$ and write $R = I_1 \times \cdots \times I_n$.

Theorem A5.18.

a) The map
$$\left\{ \begin{array}{c} \text{complete families of pairwise} \\ \text{orthogonal central idempotents} \\ (e_1, \dots, e_n) \text{ in } R \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{families } (I_1, \dots, I_n) \text{ of} \\ \text{two-sided ideals } I_j \trianglelefteq R \\ \text{with } R = I_1 \oplus \cdots \oplus I_n \end{array} \right\},$$
$$\begin{aligned} (e_1, \dots, e_n) \longmapsto & (Re_1, \dots, Re_n) \\ = & (e_1 R, \dots, e_n R) \\ = & (Re_1 R, \dots, Re_n R) \end{aligned}$$
is a well-defined bijection.

Let $(I_1, \dots, I_n)$ be a family of two-sided ideals $I_i \leq R$ with $R = I_1 \oplus \cdots \oplus I_n$ and let $(e_1, \dots, e_n)$ be the corresponding complete family of pairwise orthogonal central idempotents.

b) The projection onto the summand I_i alongside the decomposition $R = I_1 \oplus \cdots \oplus I_n$ is given by multiplication with the idempotent e_i.

c) The idempotents $e_1, \dots, e_n$ are the unique elements $e_i \in I_i$ with $1 = e_1 + \cdots + e_n$.

Proof. It sufficies to show that the bijection from Corollary A5.9 restricts to the desired bijection: We have to show for every family $(I_1, \dots, I_n)$ of left ideals $I_i \trianglelefteq R$ with $R = I_1 \oplus \cdots \oplus I_n$ and corresponding complete family $(e_1, \dots, e_n)$ of pairwise orthogonal idempotents $e_1, \dots, e_n \in R$ that the ideals $I_1, \dots, I_n$ are two-sided if and only if the idempotents $e_1, \dots, e_n$ are central.

If e_i is central then $I_i = Re_i = e_i R$ is two-sided. If on the other hand $I_1, \dots, I_n$ are two-sided then it follows for every $x \in R$ that

$$xe_i = \text{projection of } x \text{ onto } I_i = e_i x$$

where the first equality follows from part b) of Corollary A5.9 and the second equality follows similarly from the version of Corollary A5.9 for right-ideals. □

A6. Modules over Products of Rings

Conventions A6.1. In the following R_1, R_2 denote two rings. We denote by e_1, e_2 the central idemponent elements $e_1 = (1, 0)$, $e_2 = (0, 1)$ of $R_1 \times R_2$.

A6.2. In this subsection we give a brief explanition how modules over $R_1 \times R_2$ can be understood componentswise.

A6.1. Modules over Products

Lemma A6.3. Let M_i be an R_i-module for $i = 1, 2$. Then $M_1 \oplus M_2$ carries the structure of an $(R_1 \times R_2)$-module via

$$(r_1, r_2) \cdot (m_1, m_2) = (r_1 m_1, r_2 m_2)$$

for all $(r_1, r_2) \in R_1 \times R_2$, $(m_1, m_2) \in M_1 \oplus M_2$. □

Definition A6.4. For an R_1-module M_1 and an R_2-module M_2 we denote the resulting $(R_1 \times R_2)$-module described in Lemma A6.3 by $M_1 \boxplus M_2$.

Remark A6.5. If $(R_i)_{i \in I}$ is any family of rings and M_i is an R_i-module for every $i \in I$ then we can endow both $\bigoplus_{i \in I} M_i$ and $\prod_{i \in I} M_i$ with the structure of an $\prod_{i \in I} R_i$-module as above.

Lemma A6.6. Let M be an $(R_1 \times R_2)$-module and let $M_i \coloneqq e_i M$ for $i = 1, 2$.

a) We have that $e_i m_i = m_i$ for $i = 1, 2$ and $m_i \in M_i$ as well as $e_i M_j = 0$ for $i \neq j$.

b) The abelian group pM_1 carries the structure of an R_1-module via

$$r_1 \cdot m_1 \coloneqq (r_1, 0) m_1$$

for all $r_1 \in R_1$, $m_1 \in M_1$, and M_2 carries the structure of an R_2-module via

$$r_2 \cdot m_2 \coloneqq (0, r_1) m_2$$

for all $r_2 \in R_2$, $m_2 \in M_2$.

Proof.

a) For every $m_i \in M_i$ there exists some $m \in M$ with $m_i = e_i m$ and it follows that

$$e_i m_i = e_i^2 m = e_i m = m_i$$

as well as

$$e_j m_i = e_j e_i m = 0$$

for $i \neq j$ because $e_j e_i = 0$.

b) We have that

$$R_1 M_1 = (R_1 \times 0) M_1 = e_1 (R_1 \times R_2) M_1 \subseteq e_1 (R_1 \times R_2) M \subseteq e_1 M = M_1 \,,$$

which shows that the action of R_1 on M_1 is well-defined. We also have that

$$1_{R_1} \cdot m_1 = (1, 0) m_1 = e_1 m_1 = m_1$$

for every $m_1 \in M$ by part a). The other R_1-module axioms can be shown by direct calculation.

That M_2 is a well-defined R_2-module can be shown in the same way. □

Definition A6.7. For an $(R_1 \times R_2)$-module M we denote for $i = 1, 2$ the resulting R_i-module as described in Lemma A6.6 by $[M]_i$.

Theorem A6.8.

a) Let M be an $(R_1 \times R_2)$-module. Then the map

$$\alpha_M \colon M \to [M]_1 \boxplus [M]_2 \quad m \mapsto (e_1 m, e_2 m)$$

is an isomorphism of $(R_1 \times R_2)$-modules, whose inverse is given by

$$(m_1, m_2) \mapsto m_1 + m_2 \,.$$

b) Let M_i be an R_i-module for $i = 1, 2$. Then

$$[M_1 \boxplus M_2]_1 = \{(m_1, 0) \mid m_1 \in M_1\}$$

and

$$[M_1 \boxplus M_2]_2 = \{(0, m_2) \mid m_2 \in M_2\} .$$

The map

$$\beta_{1,M_1} \colon M_1 \to [M_1 \boxplus M_2]_1, \quad m_1 \mapsto (m_1, 0)$$

is an isomorphism of R_1-modules and the map

$$\beta_{2,M_2} \colon M_2 \to [M_1 \boxplus M_2]_2, \quad m_2 \mapsto (0, m_2)$$

is an isomorphism of R_2-modules.

Proof.

a) We have for all $(r_1, r_2) \in R_1 \times R_2$ and $m \in M$ that

$$\begin{aligned} \alpha_M((r_1, r_2)m) &= (e_1(r_1, r_2)m, e_2(r_1, r_2)m) = ((r_1, 0)e_1m, (r_2, 0)e_2m) \\ &= (r_1e_1m, r_2e_2m) = (r_1, r_2) \cdot (e_1m, e_2m) = (r_1, r_2) \cdot \alpha_M(m) \end{aligned}$$

which shows that α_M is a homomorphism of $(R_1 \times R_2)$-modules. We now show that α_M and the map

$$\tilde{\alpha}_M \colon [M]_1 \boxplus [M]_2 \to M, \quad (m_1, m_2) \mapsto m_1 + m_2$$

are mutually inverse: We have for every $m \in M$ that

$$\begin{aligned} \tilde{\alpha}_M(\alpha_M(m)) &= \tilde{\alpha}_M((e_1m, e_2m)) = e_1m + e_2m \\ &= (e_1 + e_2)m = (1, 1)m = 1_{R_1 \times R_2}m = m \end{aligned}$$

and we have for all $(m_1, m_2) \in [M]_1 \boxplus [M]_2$ that

$$\begin{aligned} \alpha_M(\tilde{\alpha}_M((m_1, m_2))) &= \alpha_M(m_1 + m_2) = (e_1(m_1 + m_2), e_2(m_1 + m_2)) \\ &= (\underbrace{e_1m_1}_{=m_1} + \underbrace{e_1m_2}_{=0}, \underbrace{e_2m_1}_{=0} + \underbrace{e_2m_2}_{=m_2}) = (m_1, m_2) . \end{aligned}$$

b) We have that

$$[M_1 \boxplus M_2]_1 = e_1(M_1 \boxplus M_2) = \{e_1(m_1, m_2) \mid m_i \in M_i\} = \{(m_1, 0) \mid m_1 \in M_1\} .$$

We have for all $r_1 \in R_1$ and $m_1 \in M_1$ that

$$r_1 \cdot \beta_{1,M_1}(m_1) = r_1 \cdot (m_1, 0) = (r_1, 0) \cdot (m_1, 0) = (r_1m_1, 0) = \beta_{1,M_1}(r_1m_1)$$

which shows that the bijection β_{1,M_1} is a homomorphism of R_1-modules. It can similarly be shown that β_{2,M_2} is a well-defined isomorphism of R_2-modules. □

Corollary A6.9. Every $(R_1 \times R_2)$-module is up to isomorphism of the form $M_1 \boxplus M_2$ for R_i-modules M_i. □

Remark A6.10. Corollary A6.9 does not hold for an infinite products of rings: Let $(R_i)_{i \in I}$ be a family of rings with $R_i \neq 0$ for infinitely many $i \in I$. Then $\bigoplus_{i \in I} R_i$ is a proper ideal of $\prod_{i \in I} R_i$ and the quotient

$$M := \prod_{i \in I} R_i \Big/ \bigoplus_{i \in I} R_i$$

is an $\prod_{i \in I} R_i$-module which is nonzero but is annihilated by every factor R_i.

Lemma A6.11. For all R_i-modules M_i with $i = 1, 2$ the diagram

$$\begin{tikzcd}
M_1 \boxplus M_2 \arrow[rr, equal] \arrow[dr, "\alpha_{M_1 \boxplus M_2}"'] & & M_1 \boxplus M_2 \arrow[dl, "\beta_{1,M_1} \boxplus \beta_{2,M_2}"] \\
& {[M_1 \boxplus M_2]_1 \boxplus [M_1 \boxplus M_2]_2} &
\end{tikzcd}$$

commutes.

Proof. For every element $(m_1, m_2) \in M_1 \boxplus M_2$ we have that

$$\alpha_{M_1 \boxplus M_2}((m_1, m_2)) = (e_1(m_1, m_2), e_2(m_1, m_2)) = ((m_1, 0), (0, m_2))$$

and

$$(\beta_{1,M_1} \boxplus \beta_{2,M_2})(m_1, m_2) = (\beta_{1,M_1}(m_1), \beta_{2,M_2}(m_2)) = ((m_1, 0), (0, m_2))$$

as claimed. □

A6.2. Homomorphisms of Modules over Products

Lemma A6.12. Let $f_i \colon M_i \to N_i$ be a homomorphism of R_i-modules for $i = 1, 2$. Then the map

$$M_1 \boxplus M_2 \to N_1 \boxplus N_2, \quad (m_1, m_2) \mapsto (f_1(m_1), f_2(m_2))$$

is a homomorphism of $(R_1 \times R_2)$-modules. □

Definition A6.13. In the situation of Lemma A6.12 we denote the induced homomorphism of $(R_1 \times R_2)$-modules by $f_1 \boxplus f_2$.

Lemma A6.14. Let M_i, N_i, P_i be R_i modules for $i = 1, 2$.

a) We have that $\mathrm{id}_{M_1} \boxplus \mathrm{id}_{M_2} = \mathrm{id}_{M_1 \boxplus M_2}$.

b) If $f_i \colon M_i \to N_i$, $g_i \colon N_i \to P_i$ ar homomorphisms of R_i-modules for $i = 1, 2$ then

$$(g_1 \boxplus g_2) \circ (f_1 \boxplus f_2) = (g_1 \circ f_1) \boxplus (g_2 \circ f_2).$$

c) We have that
$$(f_1 \boxplus f_2) + (g_1 \boxplus g_2) = (f_1 + g_1) \boxplus (f_2 + g_2) .$$
for all R_i-module homomorphisms $f_i, g_i \colon M_i \to N_i$. □

Remark A6.15. Altogether we have shows that $(-) \boxplus (-)$ defines a (bi)functor
$$(R_1\text{-}\mathbf{Mod}) \times (R_2\text{-}\mathbf{Mod}) \to (R_1 \times R_2)\text{-}\mathbf{Mod} .$$

Lemma A6.16. Let $f \colon M \to N$ be a homomorphism of $(R_1 \times R_2)$-modules. Then f restricts for $i = 1, 2$ to a homomorphism of R_i-modules
$$[M]_i \to [N]_i , \quad m_i \mapsto f(m_i) .$$

Proof. We have that
$$f([M]_i) = f(e_i M) = e_i f(M) \subseteq e_i N = [N]_i ,$$
which shows that f restrict to a map $f_i \colon [M]_i \colon [N]_i$. We have for all $r_i \in R_i$ and $m_i \in [M]_i$ that
$$f(r_i \cdot m_i) = f((r_i, 0) m_i) = (r_i, 0) f(m_i) = r_i \cdot f(m_i) ,$$
which shows that f_i is a homomorphism of R_i-modules. □

Definition A6.17. In the situation of Lemma A6.16 we denote for $i = 1, 2$ the induced homomorphisms of R_i-modules by $[f]_i$.

Lemma A6.18. Let M, N, P be $(R_1 \times R_2)$-modules.

a) We have for $i = 1, 2$ that $[\mathrm{id}_M]_i = \mathrm{id}_{[M]_i}$.

b) If $f \colon M \to N$ and $g \colon N \to P$ are homomorphisms of $(R_1 \times R_2)$-modules then for $i = 1, 2$ we have that
$$[g \circ f]_i = [g]_i \circ [f]_i .$$

c) We have that
$$[f + g]_i = [f]_i + [g]_i$$
for all $i = 1, 2$ and $(R_1 \times R_2)$-module homomorphisms $f, g \colon M \to N$. □

Remark A6.19. Altogether we have for $i = 1, 2$ constructed a functor
$$[-]_i \colon (R_1 \times R_2)\text{-}\mathbf{Mod} \to R_i\text{-}\mathbf{Mod} .$$
Together these result in a functor
$$([-]_1, [-]_2) \colon (R_1 \times R_2)\text{-}\mathbf{Mod} \to (R_1\text{-}\mathbf{Mod}) \times (R_2\text{-}\mathbf{Mod}) .$$

Theorem A6.20. The isomorphisms from Theorem A6.8 are compatible with homomorphisms in the following sense:

a) If $f\colon M \to N$ is a homomorphisms of $(R_1 \times R_2)$-modules then the diagram

$$\begin{tikzcd}
M \arrow[r, "f"] \arrow[d, "\alpha_M"'] & N \arrow[d, "\alpha_N"] \\
{[M]_1 \boxplus [M]_2} \arrow[r, "{[f]_1 \boxplus [f]_2}"] & {[N]_1 \boxplus [N]_2}
\end{tikzcd}$$

commutes.

b) If $f_i\colon M_i \to N_i$ is a homomorphisms of R_i-modules for $i = 1, 2$ then the diagram

$$\begin{tikzcd}
M_i \arrow[r, "f_i"] \arrow[d, "\beta_{i,M_i}"'] & N_i \arrow[d, "\beta_{i,N_i}"] \\
{[M_1 \boxplus M_2]_i} \arrow[r, "{[f_1 \boxplus f_2]_i}"] & {[N_1 \boxplus N_2]_i}
\end{tikzcd}$$

commmutes for $i = 1, 2$.

Proof.

a) We have for every $m \in M$ that

$$\begin{aligned}
([f]_1 \boxplus [f]_2)(\alpha_M(m)) &= ([f]_1 \boxplus [f]_2)((e_1 m, e_2 m)) \\
&= (f(e_1 m), f(e_2 m)) = (e_1 f(m), e_2 f(m)) = \alpha_N(f(m)) \,.
\end{aligned}$$

b) We have for every $m_1 \in M_1$ that

$$[f_1 \boxplus f_2]_1(\beta_{1,M_1}(m_1)) = [f_1 \boxplus f_2]_1((m_1, 0)) = (f_1(m_1), 0) = \beta_{1,N_1}(f_1(m_1)) \,,$$

which shows that the diagram commutes for $i = 1$. It can be shown in the same way that it commutes for $i = 2$. □

Remark A6.21. This shows that the functors constructed in Remark A6.15 and Remark A6.19 (together with α and β) form an equivalence of categories

$$(R_1 \times R_2)\text{-}\mathbf{Mod} \simeq (R_1\text{-}\mathbf{Mod}) \times (R_2\text{-}\mathbf{Mod}) \,.$$

Corollary A6.22. Let M_i, N_i be R_i-modules for $i = 1, 2$.

a) Every $(R_1 \times R_2)$-module homomorphism $f\colon M_1 \boxplus M_2 \to N_1 \boxplus N_2$ is of the form $f = f_1 \boxplus f_2$ for unique R_i-module homomorphisms $f_i\colon M_i \to N_i$.

b) The map

$$\begin{aligned}
\operatorname{End}_{R_1}(M_1) \times \operatorname{End}_{R_2}(M_2) &\longrightarrow \operatorname{End}_{R_1 \times R_2}(M_1 \boxplus M_2), \\
(f_1, f_2) &\longmapsto f_1 \boxplus f_2 \,.
\end{aligned}$$

is a well-defined isomorphism of rings.

Proof.

a) The uniqueness of f_1, f_2 follows from part b) of Theorem A6.20. To show the existence we define $f_i \colon M_i \to N_i$ by

$$f_i \coloneqq M_i \xrightarrow{\beta_{i,M_i}} [M_1 \boxplus M_2]_i \xrightarrow{[f]_i} [N_1 \boxplus N_2]_i \xrightarrow{\beta_{i,N_i}^{-1}} N_i \,.$$

In the diagram

$$\begin{tikzcd}
M_1 \boxplus M_2 \arrow[r, "f"] \arrow[d, "\alpha_{M_1 \boxplus M_2}"'] \arrow[dd, equal, bend right=60] & N_1 \boxplus N_2 \arrow[d, "\alpha_{N_1 \boxplus N_2}"] \arrow[dd, equal, bend left=60] \\
{[M_1 \boxplus M_2]_1 \boxplus [M_1 \boxplus M_2]_2} \arrow[r, "{[f]_1 \boxplus [f]_2}"] \arrow[d, "\beta_{1,M_1}^{-1} \boxplus \beta_{2,M_2}^{-1}"'] & {[N_1 \boxplus N_2]_1 \boxplus [N_1 \boxplus N_2]_2} \arrow[d, "\beta_{1,N_1}^{-1} \boxplus \beta_{2,N_2}^{-1}"] \\
M_1 \boxplus M_2 \arrow[r, "f_1 \boxplus f_2"] & N_1 \boxplus N_2
\end{tikzcd}$$

the upper square commutes by part a) of Theorem A6.20, the lower square commutes in each coordinate by definition of f_1, f_2 and therefore altogether commutes by Lemma A6.14, and the triangles on the left and right commute by Lemma A6.11. It follows that the above diagram commutes and therefore that $f = f_1 \boxplus f_2$.

b) The bijectivity follows from part A6.22 and the additivity and multiplicativity follows from Lemma A6.14. □

Corollary A6.23. Let M_i, N_i be R_i-modules for $i = 1, 2$. Then $M_1 \boxplus M_2 \cong N_1 \boxplus N_2$ as $(R_1 \times R_2)$-modules if and only if $M_i \cong N_i$ as R_i-modules for $i = 1, 2$.

Proof. It follows from Corollary A6.22 and Corollary A6.14 that there exists $(R_1 \times R_2)$-homomorphisms $f \colon M_1 \boxplus M_2 \to N_1 \boxplus N_2$ and $g \colon N_1 \boxplus N_2 \to M_1 \boxplus M_2$ with $f \circ g = \mathrm{id}$ and $g \circ f = 0$ if and only if for both $i = 1, 2$ there exists R_i-homomorphisms $f_i \colon M_i \to N_i$ and $g_i \colon N_i \to M_i$ with $f_i \circ g_i = \mathrm{id}$ and $g_i \circ f_i = \mathrm{id}$. □

Corollary A6.24. The map

$$\begin{gathered}
\left\{ \begin{array}{c} \text{iso. classes of} \\ R_1\text{-modules} \end{array} \right\} \times \left\{ \begin{array}{c} \text{iso. classes of} \\ R_2\text{-modules} \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{iso. classes of} \\ (R_1 \times R_2)\text{-modules} \end{array} \right\} , \\
([M_1], [M_2]) \longmapsto [M_1 \boxplus M_2] \,,
\end{gathered}$$

is a well-defined bijection.

Proof. The surjectivity follows from Corollary A6.9 and the injectivity follows from Corollary A6.23. □

A6.3. Submodules over Products

Proposition A6.25. Let M_i be an R_i-module for $i = 1, 2$.

a) If $N_i \le M_i$ is an R_i-submodule for $i = 1, 2$ then $N_1 \boxplus N_2$ is an $(R_1 \times R_2)$-submodule of $M_1 \boxplus M_2$.

b) Every $(R_1 \times R_2)$-submodule of $M_1 \boxplus M_2$ is of the form $N_1 \boxplus N_2$ for unique R_i submodules $N_i \le M_i$.

We thus have a bijection

$$\left\{ (N_1, N_2) \,\middle|\, \begin{matrix} R_i\text{-submodules} \\ N_i \le M_i \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} (R_1 \times R_2)\text{-submodules} \\ \text{of } M_1 \boxplus M_2 \end{matrix} \right\}$$
$$(N_1, N_2) \longmapsto N_1 \boxplus N_2 \,.$$

Proof.

b) If $N_1 \boxplus N_2 = N_1' \boxplus N_2'$ for R_i-modlues N_i, N_i' then $N_i = N_i'$ which shows the claimed uniqueness. To show the existence of N_1, N_2 we observe that $[N]_i \le [M_1 \boxplus M_2]_i$ is again a submodule and set

$$N_i := \beta_{i,M_i}^{-1}([N]_i) \le M_i \,.$$

If $\iota \colon N \to M_1 \boxplus M_2$ denotes the inclusion the diagram

$$\begin{tikzcd}
M_1 \boxplus M_2 \arrow[r, "\alpha_{M_1 \boxplus M_2}"] \arrow[rr, equal, bend left] & {[M_1 \boxplus M_2]_1 \boxplus [M_1 \boxplus M_2]_2} \arrow[r, "\beta_{1,M_1}^{-1} \boxplus \beta_{2,M_2}^{-1}"] & M_1 \boxplus M_2 \\
N \arrow[u, hook, "\iota"] \arrow[r, "\alpha_N"] & {[N]_1 \boxplus [N]_2} \arrow[u, hook, "{[\iota]_1 \boxplus [\iota]_2}"] \arrow[r, "\beta_{1,M_1}^{-1} \boxplus \beta_{2,M_2}^{-1}"] & N_1 \boxplus N_2 \arrow[u, hook]
\end{tikzcd}$$

commutes. It follows that $N = N_1 \boxplus N_2$ because all horizontial maps are isomorphisms. □

Corollary A6.26. Every left ideal in $R_1 \times R_2$ is of the form $J_1 \times J_2$ for unique left ideals $J_i \trianglelefteq R_i$ for $i = 1, 2$.

Proof. This follows from Propositon A6.25 because $R_1 \times R_2 = R_1 \boxplus R_2$ as $(R_1 \times R_2)$-modules. □

Remark A6.27. The analogous result for right ideals also holds and can be shown in the same way. The analogous result for two-sided ideals also holds and follows as a combination of the other two results.

Lemma A6.28.

a) Let $(M_i^j)_{j\in J}$ be a family of R_i-modules for $i=1,2$. Then

$$\left(\bigoplus_{j\in J} M_1^j\right) \boxplus \left(\bigoplus_{j\in J} M_2^j\right) = \bigoplus_{j\in J}(M_1^j \boxplus M_2^j)\,.$$

b) For $i=1,2$ let M_i be an R_i-module and let $(N_i^j)_{j\in J}$ a family of submodules $N_i^j \le M_i$. Then $M_1 \boxplus M_2 = \bigoplus_{j\in J}(N_1^j \boxplus N_2^j)$ if and only if both $M_i = \bigoplus_{j\in J} N_i^j$ for both $i=1,2$. □

Corollary A6.29. Let M_i be an R_i-module and let $N_i \le M_i$ an R_i-submodule for $i=1,2$. Then the submodule $N_1 \boxplus N_2 \le M_1 \boxplus M_2$ is a direct summand if and only if both $N_1 \le M_1$ and $N_2 \le M_2$ are direct summands. □

Remark A6.30. All the results of this section can be generalized to finite products of rings $R_1 \times \cdots \times R_n$. This can be done directly or by induction over n. Instead of using rings $R_1,\dots,R_n$, we could also use a ground field k and consider k-algebras $A_1,\dots,A_n$.

A7. Homomorphims between Direct Sums

Conventions A7.1. In the following R denotes a ring

A7.1. For Finite Direct Sums

Conventions A7.2. In the following $M, M_1, \dots, M_t, N, N_1, \dots, N_s$ denote R-modules. We abbreviate $\mathrm{Hom}_R =: \mathrm{Hom}$.

A7.3. In this section we will explain how R-module homomorphisms between finite direct sums can be represented by matrices. We keep our treatment elementary and will not (explicitely) use the categorical notions of coproducts, products or biproducts. We encourage the reader who is familiar with these notions to generalize the contents of this subsection to additive categorie

A7.4. Let

$$\pi_i \colon N_1 \oplus \cdots \oplus N_s \to N_i$$

denotes the projection onto the i-th summand for $i=1,\dots,s$, and let

$$\iota_j \colon M_j \to M_1 \oplus \cdots \oplus M_t$$

denote the inclusion of the j-th summand for every $j=1,\dots t$.

Definition A7.5. For every homomorphism of R-modules

$$f\colon M_1 \oplus \cdots \oplus M_t \to N_1 \oplus \cdots \oplus N_s$$

its (ij)-*th component* is given by

$$[f]_{ij} \coloneqq \pi_i \circ f \circ \iota_j$$

for all $i = 1, \dots, s$, $j = 1, \dots, t$, and we set

$$[f] \coloneqq \begin{bmatrix} [f]_{11} & \cdots & [f]_{1t} \\ \vdots & \ddots & \vdots \\ [f]_{s1} & \cdots & [f]_{st} \end{bmatrix} \in \begin{bmatrix} \operatorname{Hom}(M_1, N_1) & \cdots & \operatorname{Hom}(M_t, N_1) \\ \vdots & \ddots & \vdots \\ \operatorname{Hom}(M_1, N_s) & \cdots & \operatorname{Hom}(M_t, N_s) \end{bmatrix}.$$

Theorem A7.6. The map

$$\begin{aligned} \operatorname{Hom}(M_1 \oplus \cdots \oplus M_t, N_1 \oplus \cdots \oplus N_s) &\longrightarrow \begin{bmatrix} \operatorname{Hom}(M_1, N_1) & \cdots & \operatorname{Hom}(M_t, N_1) \\ \vdots & \ddots & \vdots \\ \operatorname{Hom}(M_1, N_s) & \cdots & \operatorname{Hom}(M_t, N_s) \end{bmatrix}, \\ f &\longmapsto [f] \end{aligned}$$

is an isomorphism of abelian groups. If R is a k-algebra then it is an isomorphism of k-vector spaces.

Proof. A homomorphisn $f \colon M_1 \oplus \cdots \oplus M_t \to N_1 \oplus \cdots \oplus N_s$ is uniquely determined by the collection of its restrictions $f \circ \iota_j \colon M_j \to N_1 \oplus \cdots \oplus N_s$, which is turns it uniquely determined by the collections of its components $\pi_i \circ f \circ \iota_j \colon M_j \to N_i$. This shows that $[\,\cdot\,]$ is injective.

For all $i = 1, \dots, s$, $j = 1, \dots, t$ we have that

$$[f+g]_{ij} = \pi_i \circ (f+g) \circ \iota_j = (\pi_i \circ f \circ \iota_j) + (\pi_i \circ g \circ \iota_j) = [f]_{ij} + [g]_{ij}\,,$$

which shows that $[\,\cdot\,]_{ij}$ is additive. It follows that $[\,\cdot\,]$ additive. If R is a k-algebra then the component map $[\,\cdot\,]_{ij} = \pi_i \circ (\,\cdot\,) \circ \iota_j$ are k-linear for all i, j, and it follows that $[\,\cdot\,]$ is k-linear.

To show that $[\,\cdot\,]$ is surjective let $\pi'_j \colon M_1 \oplus \cdots \oplus M_t \to M_j$ be the projection onto the j-th summand for every $j = 1, \dots, t$, and let $\iota_i \colon N_i \to N_1 \oplus \cdots \oplus N_s$ be the inclusion of the i-th summand. For a collection

$$(f_{ij})_{i=1,\dots,s}^{j=1,\dots,t}$$

of homomorphisms $f_{ij} \colon M_j \to N_i$ we then have the homomorphism $f \colon M \to N$ given by

$$f = \sum_{\substack{j'=1,\dots,t \\ i'=1,\dots,s}} (\iota_{i'} \circ f_{i'j'} \circ \pi'_{j'})\,,$$

whose (ij)-th component is given by

$$\begin{aligned}
[f]_{ij} = \pi_i \circ f \circ \iota_j = \pi_i \circ \left(\sum_{\substack{j'=1,\dots,t \\ i'=1,\dots,s}} (\iota_{i'} \circ f_{i'j'} \circ \pi'_{j'}) \right) \circ \iota_j \\
= \sum_{\substack{j'=1,\dots,t \\ i'=1,\dots,s}} \left(\pi_i \circ \iota_{i'} \circ f_{i'j'} \circ \pi'_{j'} \circ \iota_j \right) \\
= \sum_{\substack{j'=1,\dots,t \\ i'=1,\dots,s}} \left((\delta_{i,i'} \operatorname{id}) \circ f_{i'j'} \circ (\delta_{j,j'} \operatorname{id}) \right) = f_{ij} \,.
\end{aligned}$$

This shows that $[\,\cdot\,]$ is surjective. □

A7.7. As a consequence of Theorem A7.6 we can represent every homomorphism between finite direct sums of R-modules as a matrix. We want to highlight the following special cases:

Corollary A7.8. The maps

$$\begin{aligned}
\operatorname{Hom}(M, N_1 \oplus \dots \oplus N_s) &\longrightarrow \operatorname{Hom}(M, N_1) \times \dots \times \operatorname{Hom}(M, N_s), \\
f &\longmapsto (\pi_1 \circ f, \dots, \pi_s \circ f)
\end{aligned}$$

and

$$\begin{aligned}
\operatorname{Hom}(M_1 \oplus \dots \oplus M_t, N) &\longrightarrow \operatorname{Hom}(M_1, N) \times \dots \times \operatorname{Hom}(M_t, N), \\
f &\longmapsto (f \circ \iota_1, \dots, f \circ \iota_t)
\end{aligned}$$

are isomorphism of abelian groups. If R is a k-algebra then these are isomorphisms of k-vector spaces. □

Remark A7.9. The second isomorphism of Corollary A7.8 holds for arbitrary direct sums, while the first isomorphism holds for arbitrary *products*: For all families $(M_j)_{j \in J}$ and $(N_i)_{i \in I}$ of R-modules the maps

$$\operatorname{Hom}\left(M, \prod_{i \in I} N_i \right) \longrightarrow \prod_{i \in I} \operatorname{Hom}(M, N_i), \quad f \longmapsto (\pi_i \circ f)_{i \in I}$$

and

$$\operatorname{Hom}\left(\bigoplus_{j \in J} M_j, N \right) \longrightarrow \prod_{j \in J} \operatorname{Hom}(M_j, N), \quad f \longmapsto (f \circ \iota_j)_{j \in J}$$

are isomorphism of abelian groups. If R is a k-algebra, then these are isomorphisms of k-vector spaces.

A7.10. We may write the elements of $M_1 \oplus \cdots \oplus M_t$ as column vectors

$$\begin{bmatrix} m_1 \\ \vdots \\ m_t \end{bmatrix}$$

with $m_j \in M_j$ for every $j = 1, \dots, t$. The elements of $N_1 \oplus \cdots \oplus N_s$ can be represented as column vectors in the same way. For every R-module homomorphism $f \colon M \to N$ with matrix representation

$$f = \begin{bmatrix} f_{11} & \cdots & f_{1t} \\ \vdots & \ddots & \vdots \\ f_{s1} & \cdots & f_{st} \end{bmatrix}$$

we then have that

$$\begin{aligned} f(m) = \begin{bmatrix} \pi_1(f(m)) \\ \vdots \\ \pi_s(f(m)) \end{bmatrix} &= \begin{bmatrix} \pi_1(f(\iota_1(m_1) + \cdots + \iota_t(m_t))) \\ \vdots \\ \pi_s(f(\iota_1(m_1) + \cdots + \iota_t(m_t))) \end{bmatrix} \\ &= \begin{bmatrix} \pi_1(f(\iota_1(m_1))) + \cdots + \pi_1(f(\iota_t(m_t))) \\ \vdots \\ \pi_s(f(\iota_1(m_1))) + \cdots + \pi_s(f(\iota_t(m_t))) \end{bmatrix} \\ &= \begin{bmatrix} f_{11}(m_1) + \cdots + f_{1t}(m_t) \\ \vdots \\ f_{s1}(m_1) + \cdots + f_{st}(m_t) \end{bmatrix} = \begin{bmatrix} f_{11} & \cdots & f_{1t} \\ \vdots & \ddots & \vdots \\ f_{s1} & \cdots & f_{st} \end{bmatrix} \begin{bmatrix} m_1 \\ \vdots \\ m_t \end{bmatrix}, \end{aligned}$$

where the matrix-vector product in the last expression is taken in the naive sense.

This shows that when representing a homomorphism by a matrix we can represent application of this homomorphism by matrix-vector multiplication.

Example A7.11. Let k be a field and let V, W be finite-dimensional k-vector spaces. A choice of a basis $b_1, \dots, b_t$ of V is then the same as an isomorphism $\varphi \colon V \to k^t$, and a choice of a basis $c_1, \dots, c_s$ of W is the same as an isomorphism $\psi \colon W \to k^s$. We also have that $k \xrightarrow{\sim} \operatorname{Hom}(k, k)$ where for $\lambda \in k$ the linear map $k \to k$ is given by $x \mapsto \lambda x$. Altogether this results in an isomorphism

$$\begin{aligned} \operatorname{Hom}(V, W) \xrightarrow{\sim} \operatorname{Hom}(k^s, k^t) \longrightarrow \begin{bmatrix} \operatorname{Hom}(k,k) & \cdots & \operatorname{Hom}(k,k) \\ \vdots & \ddots & \vdots \\ \operatorname{Hom}(k,k) & \cdots & \operatorname{Hom}(k,k) \end{bmatrix} &\xrightarrow{\sim} \begin{bmatrix} k & \cdots & k \\ \vdots & \ddots & \vdots \\ k & \cdots & k \end{bmatrix} \\ &= \mathrm{M}(t \times s, k) \end{aligned}$$

which associates to $f \in \operatorname{Hom}(V, W)$ its representing matrix with respect to the bases $b_1, \dots, b_t$ and $c_1, \dots, c_s$ in the usual way.

Proposition A7.12. Let

$$M_1 \oplus \cdots \oplus M_t \xrightarrow{f} N_1 \oplus \cdots \oplus N_s \xrightarrow{g} P_1 \oplus \cdots \oplus P_r$$

be R-module homomorphisms. Then

$$[g \circ f] = [g] \cdot [f]$$

where the matrix multiplication on the right hand side is taken in the naive sense.

Proof. We denote the various projections and inclusions by

$$\begin{aligned} M_j &\xrightarrow{\iota_j} M_1 \oplus \cdots \oplus M_t \,, \\ N_i &\xrightarrow{\iota'_i} N_1 \oplus \cdots \oplus N_s \xrightarrow{\pi'_i} N_i \,, \\ & P_1 \oplus \cdots \oplus P_r \xrightarrow{\pi''_k} P_r \,. \end{aligned}$$

For all $k = 1, \dots, r$, $j = 1, \dots, t$ we then have that

$$\begin{aligned} (g \circ f)_{kj} &= \pi_k \circ g \circ f \circ \iota_j = \pi_k \circ g \circ \mathrm{id}_N \circ f \circ \iota_j = \pi_k \circ g \circ \left(\sum_{i=1}^{s} \iota'_i \circ \pi'_i \right) \circ f \circ \iota_j \\ &= \sum_{i=1}^{s} (\pi_k \circ g \circ \iota'_i \circ \pi'_i \circ f \circ \iota_j) = \sum_{i=1}^{s} (g_{ki} \circ f_{ij}) \,, \end{aligned}$$

which is precisely the (kj)-th entry of $[g] \cdot [f]$. □

Corollary A7.13. The map

$$\begin{aligned} \mathrm{End}_R(M_1 \oplus \cdots \oplus M_t) &\longrightarrow \begin{bmatrix} \mathrm{Hom}(M_1, M_1) & \cdots & \mathrm{Hom}(M_t, M_1) \\ \vdots & \ddots & \vdots \\ \mathrm{Hom}(M_1, M_t) & \cdots & \mathrm{Hom}(M_t, M_t) \end{bmatrix} \\ f &\longmapsto [f] \end{aligned}$$

is an isomorphism of rings. If R is a k-algebra then this is an isomorphism of k-algebras. □

Example A7.14. We determine the automorphisms of the $\mathbb{Z}$-module $\mathbb{Z} \oplus (\mathbb{Z}/3)$: If $f \colon \mathbb{Z} \oplus (\mathbb{Z}/3) \to \mathbb{Z} \oplus (\mathbb{Z}/3)$ is an endomorphism then

$$f = \begin{bmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{bmatrix}$$

for homomorphisms

$$\begin{aligned} f_{11} &\colon \mathbb{Z} \to \mathbb{Z} \,, & f_{12} &\colon \mathbb{Z}/3 \to \mathbb{Z} \,, \\ f_{21} &\colon \mathbb{Z} \to \mathbb{Z}/3 \,, & f_{22} &\colon \mathbb{Z}/3 \to \mathbb{Z}/3 \,. \end{aligned}$$

There exists no nonzero homomorphism $\mathbb{Z}/3 \to \mathbb{Z}$ so we have that

$$f = \begin{bmatrix} f_{11} & 0 \\ f_{21} & f_{22} \end{bmatrix}.$$

For $f, g \colon \mathbb{Z} \oplus (\mathbb{Z}/3) \to \mathbb{Z} \oplus (\mathbb{Z}/3)$ we have that

$$fg = \begin{bmatrix} f_{11} & 0 \\ f_{21} & f_{22} \end{bmatrix} \begin{bmatrix} g_{11} & 0 \\ g_{21} & g_{22} \end{bmatrix} = \begin{bmatrix} f_{11}g_{11} & 0 \\ f_{21}g_{11} + f_{22}g_{21} & f_{22}g_{22} \end{bmatrix}.$$

It follows that f is an automorphism (with inverse g) if and only if both f_{11}, f_{22} are automorphisms (with inverses g_{11}, g_{22}). There exist two automorphisms $\mathbb{Z} \to \mathbb{Z}$, two automorphisms $\mathbb{Z}/3 \to \mathbb{Z}/3$, and three homomorphisms $\mathbb{Z} \to \mathbb{Z}/3$. It follows that $\mathbb{Z} \oplus (\mathbb{Z}/3)$ has

$$2 \cdot 2 \cdot 3 = 12$$

automorphisms, as described above.

Corollary A7.15.

a) For every $n \geq 0$ the map

$$\begin{aligned} \operatorname{End}(M^{\oplus n}) &\longrightarrow \begin{bmatrix} \operatorname{End}(M) & \cdots & \operatorname{End}(M) \\ \vdots & \ddots & \vdots \\ \operatorname{End}(M) & \cdots & \operatorname{End}(M) \end{bmatrix} = \mathrm{M}_n(\operatorname{End}(M)) \\ f &\longmapsto [f] \end{aligned}$$

is an isomorphism of rings. If R is a k-algebra then it is an isomorphism of k-algebras.

b) Suppose more generally that for all $i \neq j$ there exists no nonzero R-module homomorphism $M_i \to M_j$. Then for all $n_1, \dots, n_t \geq 0$ the map

$$\begin{aligned} \operatorname{End}(M_1^{\oplus n_1} \oplus \cdots \oplus M_t^{\oplus n_t}) &\longrightarrow \begin{bmatrix} \mathrm{M}_{n_1}(\operatorname{End}(M_1)) & & \\ & \ddots & \\ & & \mathrm{M}_{n_t}(\operatorname{End}(M_t)) \end{bmatrix} \\ f &\longmapsto [f] \end{aligned}$$

is a well-defined isomorphism of rings. If R is a k-algebra then it is an isomorphism of k-algebras. □

A7.2. Generalizations to Infinite Direct Sums

Conventions A7.16. In the following $(M_i)_{i \in I}$ and $(N_i)_{i \in I}$ denote two-families of R-modules and M denotes an R-module.

Proposition A7.17.

a) The following conditions are equivalent:

   1) Every homomorphism of R-modules $f\colon \bigoplus_{i\in I} M_i \to \bigoplus_{i\in I} N_i$ restricts for every $i \in I$ to a homomorphism $f_i\colon M_i \to N_i$.

   2) For all $i, j \in I$ with $i \neq j$ it holds that $\operatorname{Hom}_R(M_i, N_j) = 0$.

b) If one (and thus both) of the above two conditions are satisfied, then the map

$$\operatorname{Hom}_R\left(\bigoplus_{i\in I} M_i, \bigoplus_{i\in I} N_i\right) \to \prod_{i\in I} \operatorname{Hom}_R(M_i, N_i), \quad f \mapsto (f_i)_{i\in I}$$

is an isomorphism of abelian groups. If R is a k-algebra then it is an isomorphism of k-vector spaces. □

Corollary A7.18.

a) The following conditions are equivalent:

   1) Every endomorphism of R-modules $f\colon \bigoplus_{i\in I} M_i \to \bigoplus_{i\in I} M_i$ restricts for every $i \in I$ to an endomorphism $f_i\colon M_i \to M_i$.

   2) For all $i, j \in I$ with $i \neq j$ it holds that $\operatorname{Hom}_R(M_i, M_j) = 0$.

b) If one (and thus both) of the above two conditions are satisfied, then the map

$$\operatorname{End}_R\left(\bigoplus_{i\in I} M_i\right) \to \prod_{i\in I} \operatorname{End}_R(M_i), \quad f \mapsto (f_i)_{i\in I}$$

is an isomorphism of rings. If R is a k-algebra then it is an isomorphism of k-algebras. □

Corollary A7.19. If $\operatorname{Hom}_R(M_i, M_j) = 0$ for all $i \neq j$ then for all index sets J_i, $i \in I$ the map

$$\operatorname{End}\left(\bigoplus_{i\in I} M_i^{\oplus J_i}\right) \to \prod_{i\in I} \operatorname{End}(M_i^{\oplus J_i}), \quad f \mapsto \left(f\big|_{M_i^{\oplus J_i}}\right)_{i\in I}$$

is a well-defined isomorphism of rings. If R is a k-algebra, then it is an isomorphism of k-algebras. □

A7.20. For every $i \in I$ let $\iota_i\colon M_i \to \bigoplus_{i'\in I} M_{i'}$ be the inclusion of the i-th summand, and for every $i \in I$ let $\pi_i\colon \bigoplus_{i'\in I} N_{i'} \to N_i$ be the projection onto the i-th summand.

Lemma A7.21. For every R-module homomorphism $f\colon M \to \bigoplus_{i\in I} N_i$ let $f_i \coloneqq \pi_i \circ f$ be the i-th component of f. If M is finitely generated, then the map

$$\operatorname{Hom}_R\left(M, \bigoplus_{i\in I} N_i\right) \to \bigoplus_{i\in I} \operatorname{Hom}_R(M, N_i), \quad f \mapsto (f_i)_{i\in I}$$

is a well-defined isomorphism of abelian groups. If R is a k-algebra then it is an isomorphism of k-vector spaces.

Proof. We denote the given map by Φ. It sufficies to show that Φ is well-defined because its inverse is then given by the map Ψ with

$$\Psi((f_i)_{i\in I})(m) = (f_i(m))_{i\in I}$$

for all $(f_i)_{i\in I} \in \bigoplus_{i\in I} \operatorname{Hom}(M, M_i)$ and $m \in M$.

Let $x_1, \dots, x_n \in M$ be a finite generating set. The set

$$I'_j \coloneqq \{i' \in I \mid f_{i'}(x_j) \neq 0\}$$

is finite for every $j = 1, \dots, n$ and it follows that $I' \coloneqq \bigcup_{j=1}^n I'_j$ is finite. For every $i \in I$ with $i \notin I'$ we have that $f_i(x_j) = 0$ for every $j = 1, \dots, n$ and therefore $f_i(m) = 0$ for every $m \in M$. This shows that $f_i = 0$ for every $i \in I$ with $i \notin I'$. □

Definition A7.22. Let I, J be index sets.

- Let $(X_{ij})_{i\in I, j\in J}$ be a family of sets. The space of all $(I \times J)$-matrices whose (ij)-th entry is contained in X_{ij} is denoted by

$$\mathrm{M}(X_{ij} \mid i \in I, j \in J) = \{(A_{ij})_{i\in I,j\in J} \mid A_{ij} \in X_{ij} \text{ for all } i \in I,\, j \in J\}\,.$$

- Let $(C_{ij})_{i\in I,j\in J}$ be a family of abelian groups. A matrix $A \in \mathrm{M}(C_{ij} \mid i \in I, j \in J)$ is *column finite* if for every column index $j \in J$ there exist only finitely many $i \in I$ with $A_{ij} \neq 0$. The space of all such matrices is denoted by

$$\mathrm{M}^{\mathrm{cf}}(C_{ij} \mid i \in I, j \in J) \coloneqq \{A \in \mathrm{M}(C_{ij} \mid i \in I, j \in J) \mid A \text{ is column finite}\}\,.$$

- If C is an abelian group then we abbreviate

$$\begin{aligned} \mathrm{M}(I \times J, C) &\coloneqq \mathrm{M}(C \mid i \in I, j \in J)\,, \\ \mathrm{M}^{\mathrm{cf}}(I \times J, C) &\coloneqq \mathrm{M}^{\mathrm{cf}}(C \mid i \in I, j \in J)\,, \\ \mathrm{M}_I(C) &\coloneqq \mathrm{M}(I \times I, C)\,, \\ \mathrm{M}_I^{\mathrm{cf}}(C) &\coloneqq \mathrm{M}^{\mathrm{cf}}(I \times I, C)\,. \end{aligned}$$

The notion of a *row finite* $(I \times J)$-matrix is defined similarly, and instead of $^{\mathrm{cf}}$ the supscript $^{\mathrm{rf}}$ is used.

Lemma A7.23. Let I, J be index sets

a) If $(C_{ij})_{i\in I,j\in J}$ is a family of abelian groups then $\mathrm{M}(C_{ij} \mid i \in I, j \in J)$ is an abelian group via entrywise addition of matrices, and $\mathrm{M}^{\mathrm{cf}}(C_{ij} \mid i \in I, j \in J)$ is a subgroup of $\mathrm{M}(C_{ij} \mid i \in I, j \in J)$.

b) If $(V_{ij})_{i\in I,j\in J}$ is a family of k-vector spaces then $\mathrm{M}(V_{ij} \mid i \in I, j \in J)$ is a k-vector space via entrywise addition of matrices, and $\mathrm{M}^{\mathrm{cf}}(C_{ij} \mid i \in I, j \in J)$ is a k-linear subspace of $\mathrm{M}(C_{ij} \mid i \in I, j \in J)$.

c) If R is a ring then the column finite square matrices $\mathrm{M}_I^{\mathrm{cf}}(R)$ become a ring when endowed with entrywise addition and the usual matrix multiplication, i.e.

$$(A \cdot B)_{ik} = \sum_{j \in I} A_{ij} B_{jk}$$

for all $A, B \in \mathrm{M}_I^{\mathrm{cf}}(R)$ and all $i, k \in I$. If R is a k-algebra then this makes $\mathrm{M}_I^{\mathrm{cf}}(R)$ into a k-algebra.

The analogous results for row finite matrices also hold. □

Corollary A7.24. For every homomorphis of R-modules $f \colon \bigoplus_{i \in I} M_i \to \bigoplus_{i \in I} N_i$ let

$$f_{ij} \coloneqq \pi_i \circ f \circ \iota_j \colon M_j \to N_i$$

be its (ij)-th component for all $i, j \in I$. If M_i is finitely generated for every $i \in I$, then the map

$$\mathrm{Hom}_R \left(\bigoplus_{i \in I} M_i, \bigoplus_{i \in I} N_i \right) \to \mathrm{M}^{\mathrm{cf}} \left(\mathrm{Hom}_R(M_i, N_j) \,|\, i, j \in I \right), \quad f \mapsto (f_{ij})_{i \in I, j \in J}$$

is a well-defined isomorphism of abelian groups. If R is a k-algebra then it is an isomorphism of k-vector spaces. □

Corollary A7.25. For every endomorphism of R-modules $f \colon M^{\oplus I} \to M^{\oplus I}$ let

$$f_{ij} \coloneqq \pi_i \circ f \circ \iota_j \colon M \to M$$

be its (ij)-th component for all $i, j \in I$. If M is finitely generated then the map

$$\mathrm{End}_R \left(M^{\oplus I} \right) \to \mathrm{M}_I^{\mathrm{cf}}(\mathrm{End}_R(M)) \quad f \mapsto (f_{ij})_{i \in I, j \in J}$$

is an isomorphism of rings. If R is a k-algebra then it is an isomorphism of k-algebras. □

A8. The Jordan–Hölder Theorem

Conventions A8.1. We denote by R a ring (with unit, not necessarily commutative) and by M an R-module.

Definition A8.2. A *filtration* of M is an increasing sequence

$$0 = M_0 \lneq M_1 \lneq M_2 \lneq M_3 \lneq \cdots \lneq M_n = M$$

of submodules $M_i \leq M$. The number n is the *length* of this filtration, and the quotients M_i / M_{i-1} with $i = 1, \dots, n$ are its *factors*.

Definition A8.3. A filtration $(M'_j)_{j=0}^m$ is an *refinement* of a filtration $(M_i)_{i=0}^n$ if $(M_i)_{i=0}^n$ is a subsequence of $(M'_j)_{j=0}^m$.

Definition A8.4. Two filtrations $(M_i)_{i=0}^n$ and $(M'_j)_{j=0}^m$ are equivalent if they have the same factors up to permutation and isomorphism, i.e. if $n = m$ and there exists a bijection $\pi\colon \{1, \dots, n\} \to \{1, \dots, m\}$ such that

$$M'_{\pi(i)}/M'_{\pi(i)-1} \cong M_i/M_{i-1}$$

for all $i = 1, \dots, n$.

Remark A8.5. Two filtrations $(M_i)_{i=0}^n$ and $(M'_j)_{j=0}^m$ are equivalent if and only if the familes $(M_i/M_{i-1})_{i=1}^n$ and $(M'_j/M_{j-1})_{j=1}^m$ are the same up to reordering and isomorphism.

A8.1. Schreiers Theorem

Lemma A8.6. Let $P \leq N \leq M$ be submodules. Then

$$(P + C) \cap N = P + (C \cap N)$$

for every submodule $C \leq N$.

Proof. For $n \in (P + C) \cap N$ we have that $n \in N$ and there exist $p \in P$, $c \in C$ with $n = p + c$. It then follows from $n - c = p \in P \leq N$ that also $c = n - p \in N$. We therefore have that $c \in C \cap N$ and thus $n = p + c \in P + (C \cap N)$.

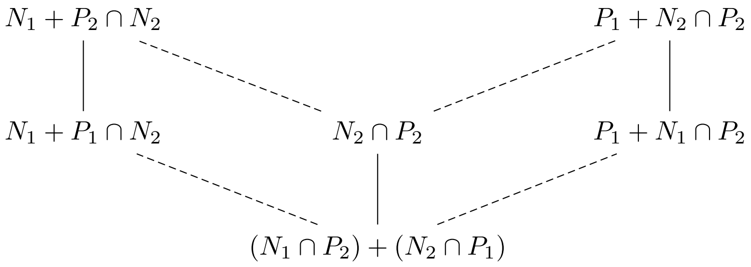
It follows from $P \leq P + C$ and $P \leq N$ that $P \leq (P + C) \cap N$, and it similarly follows from $C \cap N \leq C \leq P + C$ and $C \cap N \leq N$ that $C \cap N \leq N$. Together this shows that $P + (C \cap N) \leq (P + C) \cap N$. □

Remark A8.7. Lemma A8.6 shows that the lattice of submodules of M is *modular*.

Lemma A8.8 (Butterfly lemma)**.** Let M be an R-module and let $N_1 \leq N_2 \leq M$ and $P_1 \leq P_2 \leq M$ be submodules. Then

$$\begin{aligned} &(N_1 + P_2 \cap N_2)/(N_1 + P_1 \cap N_2) \\ &\cong (N_2 \cap P_2)/((N_1 \cap P_2) + (N_2 \cap P_1)) \\ &\cong (P_1 + N_2 \cap P_2)/(P_1 + N_1 \cap P_2)\,. \end{aligned}$$

A8.9. The understand the name “butterfly lemma” we can consider the Hasse diagramm of the various modules involved:



The two parallelograms form the wings of a butterfly. The butterfly lemma states that the quotients associated to the three vertical edges are isomorphic.

This image also explains how to prove the butterfly lemma: Recall that the third isomorphism theory states that for all submodule $N, P \leq M$ we have that

$$(N+P)/P \cong N/(N \cap P)\,,$$

i.e. that in the Hasse diagram

$$\begin{tikzcd}
 & N+P \arrow[dl, dash, dashed] \arrow[dr, dash] & \\
N \arrow[dr, dash] & & P \arrow[dl, dash, dashed] \\
 & N \cap P &
\end{tikzcd}$$

the quotients associated to any two parallel egdes are isomorphic.

Proof of the butterfly lemma. By the second isomorphism theorem it sufficies to show that

a) $(N_1 + P_1 \cap N_2) + (N_2 \cap P_2) = N_1 + P_2 \cap N_2$,

b) $(N_1 + P_1 \cap N_2) \cap (N_2 \cap P_2) = (N_1 \cap P_2) + (N_2 \cap P_1)$,

c) $(N_2 \cap P_2) + (P_1 + N_1 \cap P_2) = P_1 + N_2 \cap P_2$,

d) $(N_2 \cap P_2) \cap (P_1 + N_1 \cap P_2) = (N_1 \cap P_2) + (N_2 \cap P_2)$.

It sufficies to show a) and b) because then c) and d) follows by switching the roles of the N_i and P_i. The equality a) holds because

$$\begin{aligned}
&(N_1 + P_1 \cap N_2) + (N_2 \cap P_2) \\
&= N_1 + (P_1 \cap N_2) + (N_2 \cap P_2) \\
&= N_1 + (P_2 \cap N_2) \\
&= N_1 + P_2 \cap N_2\,,
\end{aligned}$$

and the equality b) holds because

$$\begin{aligned}
&(N_1 + P_1 \cap N_2) \cap (N_2 \cap P_2) \\
&= ((N_2 \cap P_1) + N_1) \cap (N_2 \cap P_2) \\
&= (N_2 \cap P_1) + (N_1 \cap (N_2 \cap P_2)) \\
&= (N_2 \cap P_1) + (N_1 \cap P_2)\,,
\end{aligned}$$

where we use for the second equality that $N_2 \cap P_1 \leq N_2 \cap P_2$ to apply Lemma A8.6. □

Theorem A8.10 (Schreier)**.** Any two filtration of M have equivalent refinements.

Proof. Let

$$0 = M_0 \lneq M_1 \lneq M_2 \lneq M_3 \lneq \cdots \lneq M_n = M \tag{A8.1}$$

and

$$0 = M'_0 \lneq M'_1 \lneq M'_2 \lneq M'_3 \lneq \cdots \lneq M'_m = M \tag{A8.2}$$

be two filtrations of M. We refine the filtration (A8.1) to an increasing sequence of submodules

$$\begin{aligned} 0 = {} & M_0 + M'_0 \cap M_1 \leq M_0 + M'_1 \cap M_1 \leq \cdots \leq M_0 + M'_m \cap M_1 \quad (= M_1) \\ = {} & M_1 + M'_0 \cap M_2 \leq M_1 + M'_1 \cap M_2 \leq \cdots \leq M_1 + M'_m \cap M_2 \quad (= M_2) \\ & \vdots \\ = {} & M_{n-1} + M'_0 \cap M_n \leq M_{n-1} + M'_1 \cap M_n \leq \cdots \leq M_{n-1} + M'_m \cap M_n \; (= M_n) = M \,, \end{aligned} \tag{A8.3}$$

and we can similarly refine the filtration (A8.2) to an increasing sequence of submodules

$$\begin{aligned} 0 = {} & M'_0 + M_0 \cap M'_1 \leq M'_0 + M_1 \cap M'_1 \leq \cdots \leq M'_0 + M_n \cap M'_1 \quad (= M'_1) \\ = {} & M'_1 + M_0 \cap M'_2 \leq M'_1 + M_1 \cap M'_2 \leq \cdots \leq M'_1 + M_n \cap M'_2 \quad (= M'_2) \\ & \vdots \\ = {} & M'_{n-1} + M_0 \cap M'_m \leq M'_{n-1} + M_1 \cap M'_m \leq \cdots \leq M'_{n-1} + M_n \cap M'_m \; (= M'_m) = M \,. \end{aligned} \tag{A8.4}$$

The modules in the first sequence are given by

$$N_{ij} \coloneqq M_{i-1} + M'_j \cap M_i$$

with $i = 1, \dots, n$, $j = 0, \dots, m$, and the modules in the second sequence are given by

$$N'_{ji} \coloneqq M'_{j-1} + M_i \cap M'_j \,,$$

with $j = 1, \dots, m$, $i = 0, \dots, n$.

The factors of the first sequence are therefore given by

$$F_{ij} \coloneqq N_{ij} / N_{i,j-1}$$

for $i = 1, \dots, n$, $j = 1, \dots, m$ together with the trivial factors

$$N_{i0} / N_{i-1,m} = M_{i-1} / M_{i-1} = 0$$

for every $i = 2, \dots, n$. The factors of the second sequence are given by

$$F'_{ji} \coloneqq N'_{ji} / N_{j,i-1}$$

for $j = 1, \dots, m$, $i = 1, \dots, n$ together with the trivial factors

$$N'_{j0} / N'_{j-1,n} = M'_{j-1} / M'_{j-1} = 0$$

for every $j = 2, \dots, m$. It follows for all $i = 1, \dots, n$ and $j = 1, \dots, m$ from the butterfly lemma that

$$\begin{aligned} F_{ij} &= N_{ij}/N_{i,j-1} \\ &= (M_{i-1} + M'_j \cap M_i)/(M_{i-1} + M'_{j-1} \cap M_i) \\ &\cong (M'_{j-1} + M_i \cap M'_j)/(M'_{j-1} + M_{i-1} \cap M'_j) \\ &= N_{ji}/N_{j,i-1} = F'_{ji} \,. \end{aligned}$$

This shows that the sequences (A8.3) and (A8.4) have the same non-trivial factors up to permutation and isomorphism. By removing all repetition from the sequences (A8.3) and (A8.4) we thus arrive at two equivalent filtrations of M. These resulting filtrations are refinements of (A8.1) and (A8.2) because the M_i appear in the first sequence in the M'_j appear in the second sequence. □

A8.2. The Jordan–Hölder Theorem

A8.11. For the follwing discussion we will require the notion of a *simple module* as introduced in Definition 22.3.

Definition A8.12. A filtration $(M_i)_{i=0}^n$ is a *composition series* if all of its factors M_i/M_{i-1} with $i = 1, \dots, n$ are simple. The factors of a composition series are its *composition factors*.

Lemma A8.13. Let $(M_i)_{i=0}^n$ be a composition series for M.

a) Every filtration which is equivalent to $(M_i)_{i=0}^n$ is again a composition series.

b) The only refinement of $(M_i)_{i=0}^n$ is $(M_i)_{i=0}^n$ itself.

Proof.

a) Every filtration of M which is equivalent to $(M_i)_{i=0}^n$ has up to isomorphism the same factors as $(M_i)_{i=0}^n$, which are then all simple.

b) Let $(M'_j)_{j=0}^m$ be a refinement of $(M_i)_{i=0}^n$. For every $j = 0, \dots, m$ there then exists some some $i = 1, \dots, n$ with $M_{i-1} \leq M'_j \leq M_i$. Then M'_j/M_{i-1} is a submodule of the simple module M_i/M_{i-1}, and it follows that $M'_j/M_{i-1} = 0$ or $M'_j/M_{i-1} = M_i/M_{i-1}$. In the first case we have that $M'_j = M_{i-1}$ and in the second case we have that $M'_j = M_i$.

   This shows that every term of $(M'_j)_{j=0}^m$ already appers in $(M_i)_{i=0}^n$, which shows that $(M'_j)_{j=0}^m = (M_i)_{i=0}^n$. □

Theorem A8.14 (Jordan–Hölder)**.** Suppose that M admits a composition series.

a) Every filtration of M has a refinements which is a composition series.

b) Every two composition series of M are equivalent.

Proof. Let $(M_i)_{i=0}^n$ be a composition series for M.

a) Let $(M'_j)_{j=0}^m$ be another filtration of M. Then $(M'_j)_{j=0}^m$ and $(M_i)_{i=0}^n$ have equivalent refinements by Schreier's theorem. It follows from Lemma A8.13 that $(M'_j)_{j=0}^m$ admits a refinements that is equivalent to $(M_i)_{i=0}^n$ and which is therefore itself a composition series.

b) Let $(M'_j)_{j=0}^m$ be another composition series of M. Then $(M_i)_{i=0}^n$ and $(M'_j)_{j=0}^m$ have equivalent refinements by Schreier's theorem, which are then just the compositions series themselves by Lemma A8.13. □

Corollary A8.15.

a) Every two composition series of M have the same length and up to permutation and isomorphism the same composition factors.

b) If M admits a composition series of length n then every filtration of M has length $\leq n$.

c) A filtration of M is a composition series if and only if it has maximal length among all filtrations.

Proof.

a) This follows from the Jordan Hölder theorem.

b) This follows from the Jordan Hölder theorem.

c) If $(M_i)_{i=0}^n$ is a composition series of M then every filtration $(M'_j)_{j=0}^m$ of M has a refinements $(M''_k)_{k=0}^\ell$ which is equivalent to $(M_i)_{i=0}^n$. It follows from part a) that $n = \ell \geq m$. This shows that composition series have maximal length among all filtrations.

   Suppose that a $(M_i)_{i=0}^n$ of M is not a composition series. Then there exists some $i = 1, \dots, n$ for which the factor M_i/M_{i-1} is not simple. Then M_i/M_{i-1} contains a nonzero proper submodule, which then correspond to a proper submodule $N \lneq M_i$ with $M_{i-1} \lneq N$. Then

$$0 = M_0 \lneq M_1 \lneq \cdots \lneq M_{i-1} \lneq N \lneq M_i \lneq \cdots \lneq M_n = M$$

   is a refinement of $(M_i)_{i=0}^n$ of length $n+1$, which shows that $(M_i)_{i=0}^n$ does not have maximal length among all filtrations. □

A8.16. We finish by showing that an R-module admits a composition series if and only if it is both noetherian and artinian. We will not use this result during the main text.

Lemma A8.17. If M is artinian then it contains a simple submodule.

Proof. The set of nonzero submodules of M contains a minimal element, which is then a simple submodule. □

Proposition A8.18. The R-module M has a composition series if and only if it is both noetherian and artinian.

Proof. Suppose that M has a composition series of length n. Then every strictly increasing (resp. strictly decreasing) sequence of submodules of M has at most length n by part b) of Corollary A8.15. This shows that M is both noetherian and artinian.

Suppose that M is both noetherian and artinian. If $M = 0$ then M has a (unique) composition series of length 0 so suppose that $M \neq 0$. It then follows that M contains a simple submodule M_1 by Lemma A8.17. If $M/M_1 = 0$ then $M = M_1$ and

$$0 = M_0 \lneq M_1 = M$$

is a composition series of M. Otherwise the quotient M/M_1 is nonzero and again artinian by Proposition A2.7 and thus contains a simple submodule. This simple submodule is then of the form M_2/M_1 for some submodule $M_2 \leq M$ with $M_1 \lneq M_2$.

If the above process terminates after n steps then we arrive at a filtration

$$0 = M_0 \lneq M_1 \lneq M_2 \lneq \cdots \lneq M_n = M$$

with simple factors M_i/M_{i-1} for $i = 1, \ldots, n$, i.e. at a composition series of M. Otherwise we would construct a strictly increasing sequence of submodules

$$0 = M_0 \lneq M_1 \lneq M_2 \lneq \cdots$$

which would contradict M being noetherian. □

Bibliography

[AM15] Michael Atiyah and Ian G. Macdonald. *Introduction to Commutative Algebra.* 1st ed. Addison-Wesley Series in Mathematics. Westview Press, Dec. 2015. ISBN: 9780813350189.

[AM57] A. A. Albert and Benjamin Muckenhoupt. "On matrices of trace zeros". In: *The Michigan Mathematical Journal* 4.1 (1957), pp. 1–3. DOI: 10.1307/mmj/1028990168. URL: https://doi.org/10.1307/mmj/1028990168.

[Beh72] Ernst-August Behrens. *Ring Theory.* Trans. by Clive Reis. Pure and Applied Mathematics. Elsevier Science, 1972. ISBN: 9780080873572.

[Cla12] Pete L. Clark. "Noncommutative Algebra". 2012. URL: http://math.uga.edu/~pete/noncommutativealgebra.pdf.

[DaS17] Patrick Da Silva. "Non-commutative Algebra". June 2017. URL: http://userpage.fu-berlin.de/dasilvap/notes/Non-commutative-Algebra-02-06-17.pdf.

[DF04] David S. Dummit and Richard M. Foote. *Abstract Algebra.* Wiley, 2004. ISBN: 9780471433347.

[Dix63] J. Dixmier. "Représentations irréductibles des algèbres de Lie nilpotentes". In: *An. Acad. Brasil. Ci.* 35 (1963), pp. 491–519. ISSN: 0001-3765.

[DK15] H. Derksen and G. Kemper. *Computational Invariant Theory.* 2nd ed. Encyclopaedia of Mathematical Sciences. 2015. ISBN: 9783662484227.

[Eti+11] P. Etingof et al. "Introduction to representation theory". In: *ArXiv e-prints* (Feb. 2011). arXiv: 0901.0827v5 [math.RT].

[FD93] Benson Farb and R. Keith Dennis. *Noncommutative Algebra.* Graduate Texts in Mathematics. Srpinger New York, 1993. ISBN: 9780387940571. DOI: 10.1007/978-1-4612-0889-1.

[Fle00] Peter Fleischmann. "The Noether Bound in Invariant Theory of Finite Groups". In: *Advances in Mathematics* 156.1 (2000), pp. 23–32. ISSN: 0001-8708. DOI: https://doi.org/10.1006/aima.2000.1952. URL: http://www.sciencedirect.com/science/article/pii/S0001870800919522.

[Fog01] John Fogarty. "On Noether's bound for polynomial invariants of a finite group". In: *Electronic Research Announcements* 7 (2001), p. 5. ISSN: 1935-9179. URL: http://aimsciences.org//article/id/9d13e48f-6b04-4ef9-bb7d-0aa0027725c6.

[GW04] K. R. Goodearl and R. B. Warfield Jr. *An Introduction to Noncommutative Noetherian Rings.* 2nd ed. London Mathematical Society Student Texts. Cambridge University Press, 2004. DOI: 10.1017/CBO9780511841699.

[Isa09] I. Martin Isaacs. *Algebra: A Graduate Course*. Graduate Studies in Mathematics. American Mathematical Society, 2009. ISBN: 978-0-8218-4799-2.

[Kna16] Anthony W. Knapp. *Advanced Algebra*. Second Digital Edition. 2016. URL: http://www.math.stonybrook.edu/~aknapp/download/a2-alg-coverandinside.pdf.

[KP96] Hanspeter Kraft and Claudio Procesi. "Classical Invariant Theory, A Primer". Preliminary Version. July 1996.

[Lam91] T.Y. Lam. *A First Course in Noncommutative Rings*. 1st ed. Graduate Texts in Mathematics. Springer New York, 1991. ISBN: 0387975233.

[Lan05] Serge Lang. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2005. ISBN: 9780387953854.

[MO12] Martin Brandenburg. *The Rabinowitz Trick*. MathOverflow. Mar. 2012. URL: https://mathoverflow.net/q/90666.

[MO15] Lewis Topley. *Generators of associated graded algebra*. MathOverflow. Nov. 2015. URL: https://mathoverflow.net/q/224454.

[MS18a] Jendrik Stelzner. *Proof of Maschke's theorem: Why is $\hat{p}$ again a projection?* Mathematics Stack Exchange. June 2018. URL: https://math.stackexchange.com/q/2644102.

[MS18b] Eric Wofsey. *Is* $\operatorname{Hom}(E, M)$ *simple as an* $\operatorname{End}(M)$*-module if E is simple?* Mathematics Stack Exchange. July 2018. URL: https://math.stackexchange.com/q/2859823.

[Noe15] Emmy Noether. "Der Endlichkeitssatz der Invarianten endlicher Gruppen". In: *Mathematische Annalen* 77.1 (Mar. 1915), pp. 89–92. ISSN: 1432-1807. DOI: 10.1007/BF01456821. URL: https://doi.org/10.1007/BF01456821.

[NV04] Constantin Năstăsescu and Freddy Van Oystaeyen. *Methods of Graded Rings*. Lecture Notes in Mathematics no. 1836. Springer-Verlag Berlin Heidelberg, 2004. ISBN: 978-3-540-20746-7. DOI: 10.1007/b94904.

[Pie82] Richard S. Pierce. *Associative Algebras*. Graduate Texts in Mathematics. Springer New York, 1982. ISBN: 9781475701654. DOI: 10.1007/978-1-4757-0163-0.

[Qui69] Daniel Quillen. "On the endomorphism ring of a simple module over an enveloping algebra". In: *Proc. Amer. Math. Soc.* 21 (1969), pp. 171–172. ISSN: 0002-9939.

[Rie65] Marc Aristide Rieffel. "A general Wedderburn theorem". In: *Proc. Nat. Acad. Sci. U.S.A.* 54 (1965), p. 1513.

[Sch91] Barbara J. Schmid. "Finite groups and invariant theory". In: *Topics in Invariant Theory*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1991, pp. 35–66. ISBN: 978-3-540-47592-7.

[Sha14] Joel H. Shapiro. "Burnside's Theorem on Matrix Algebras". Aug. 2014. URL: http://joelshapiro.org/Pubvit/Downloads/BurnsideThm/burnside.pdf.

[Spe07] David Speyer. *The Nullstellensatz and Partitions of Unity*. Secret Blogging Seminar. Version 2018-06-29. Dec. 2007. URL: https://sbseminar.wordpress.com/2007/12/14/the-nullstellensatz-and-partitions-of-unity.

[Weh06] David L. Wehlau. "The Noether Number in Invariant Theory". June 2006.

[Wey46] Hermann Weyl. *The Classical Groups: Their Invariants and Representations*. Second Edition, with Supplements (Eight Printing, 1973). Princeton mathematical series. Princeton University Press, 1946. ISBN: 0691079234.

[Yua12] Qiaochu Yuan. *The double commutant theorem*. Annoying Precision. Version 2018-07-30. Nov. 2012. URL: https://qchu.wordpress.com/2012/11/11/the-double-commutant-theorem.