Algebra II

Winter Semester 2018/19

24th January 2019

Contents

These are notes of the lecture "Algebra II", taught by Prof. Dr. Catharina Stroppel at the University of Bonn in the winter semester 2018/19.

Lecture website:
http://guests.mpim-bonn.mpg.de/enorton/alg2.html

References

[Hun80] Thomas W. Hungerford. *Algebra*. Springer New York, 1980.

[Kna06a] Anthony W. Knapp. *Basic Algebra*. Birkhäuser Boston, 2006.

[Kna06b] Anthony W. Knapp. *Advanced Algebra*. Birkhäuser Boston, 2006.

[Pro06] Claudio Procesi. *Lie Groups. An Approach through Invariants and Representations*. Springer New York, 2006.

[Bor12] Armand Borel. *Linear Algebraic Groups*. Springer New York, 2012.

[Hum75] James E. Humphreys. *Linear Algebraic Groups*. Springer New York, 1975.

[Spr08] Tonny A. Springer. *Linear Algebraic Groups*. Birkhäuser Boston, 2008.

[October 8, 2018]

I. Group actions

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

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

$$\begin{array}{rcl} G \times X & \to & X \\ (g,x) & \mapsto & g.x \end{array}$$

such that

(A1) $e.X = x$ and

(A2) $(gh).x = g.(h.x)$

for all $x \in X$ and $g, h \in G$. We call then X a *G-set*.

Definition. Given a set X, define

$$S(X) := \{f \colon X \to X \mid f \text{ bijective}\},$$

the *symmetric group* of X (with composition as group multiplication).

Given a G-set X and $g \in G$, let $\pi_g \in S(X)$ be defined as $\pi_g(x) = g.x$.

Lemma I.1. *For any group G and set X we have a bijective correspondence*

$$\begin{array}{rcl} \{G\text{-actions on } X\} & \xleftrightarrow{1:1} & \{\text{Group homomorphisms } G \to S(X)\} \\ \pi & \mapsto & \hat{\pi} = (g \mapsto (x \mapsto \pi(g,x) = g.x)) \\ ((g,x) \mapsto \varphi(g)(x)) = \mathring{\varphi} & \leftarrow\!\shortmid & \varphi. \end{array}$$

Proof. Left to the reader. $\square$

Examples. Let G be a group.

1) G acts on itself by
   - left multiplication: $g.x = gx$ (left regular action)
   - "right multiplication": $g.x = xg^{-1}$ (right regular action)
   - conjugation $g.x = gxg^{-1}$

2) Any set X is a G-set via the *trivial action* $g.x = x$.

3) Let X, Y be G-sets. then G acts on $\mathrm{Maps}(X,Y) := \{f \colon X \to Y\}$ via $(g.f)(x) = g.(f(g^{-1}.x))$. Special case: the action Y is trivial, then $(g.f)(x) = f(g^{-1}.x)$.

Definition. 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 $x \in X$. We write

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

Lemma I.2. *Let G be a group.*

1) *If X is a G-set then* $\mathrm{id}_X \in \mathrm{Hom}_G(X,X)$.

2) *If X, Y, Z are G-sets, $f_1 \in \mathrm{Hom}_G(X,Y)$ and $f_2 \in \mathrm{Hom}_G(Y,Z)$ then $f_2 \circ f_1 \in \mathrm{Hom}_G(X,Z)$.*

Proof. Left to the reader. $\square$

Examples. Let G be a group.

1) If G acts on itself by left multiplication then

$$\begin{array}{rcl} \mathrm{Hom}_G(G,G) & \cong & G \quad \text{(as sets)} \\ f & \mapsto & f(e) \\ (x \mapsto xa) = m_a & \leftarrow\!\shortmid & a. \end{array}$$

2) If X, Y are trivial G-sets then $\mathrm{Hom}_G(X,Y) = \mathrm{Maps}(X,Y)$.

Definition. Let X be a G-set. For $x \in X$ let $G_x = \{g.x \mid g \in G\}$ be the *orbit* of x. We write

$$G \mathbin{\backslash\!\backslash} X := \{G_x \mid x \in X\}.$$

Note that $G_x = G_y$ iff $y \in G_x$.

Remark. We can view $G \mathbin{\backslash\!\backslash} X$ as a G-set via the trivial action. Then can$\colon X \to G \mathbin{\backslash\!\backslash} X, x \mapsto G_x$ is G-equivariant.

Definition. Let X be a G-set. Then

$$X^G := \{x \in X \mid \forall g \in G : g.x = x\}$$

is the *set of G-fixed points* or *G-invariants* in X.

Lemma I.3. *Let X, Y be G-sets and $f \in \mathrm{Hom}_G(X,Y)$. Then, $f(X^G) \subseteq Y^G$.*

Proof. Let $x \in X^G$. For all $g \in G$, we have $g.f(x) = f(g.x) = f(x)$. Therefore, $f(x) \in Y^G$. $\square$

Thus, f induces a map $f^G\colon X^G \to Y^G$ by restriction.

Lemma I.4. *Let G be a group.*

1) *If X is a G-set then* $\mathrm{id}_X^G = \mathrm{id}_{X^G}$.

2) *If X, Y, Z are G-sets, and $f_1 \in \mathrm{Hom}_G(X, Y)$ and $f_2 \in \mathrm{Hom}_G(Y, Z)$ then* $(f_2 \circ f_1)^G = f_2^G \circ f_1^G$.

Proof. Left to the reader. $\square$

Lemma I.5. *Let X, Y be G-sets. Then* $\mathrm{Hom}_G(X, Y) = \mathrm{Maps}(X, Y)^G$.

Proof. $f \in \mathrm{Hom}_G(X, Y) \Leftrightarrow \forall g \in G, x \in X : f(g.x) = g.f(x) \Leftrightarrow \forall g \in G, x \in X : g^{-1}.f(g.x) = g^{-1}.(g.f(x)) = f(x) \Leftrightarrow \forall g \in G, x \in X : g.f(g^{-1}.x) = f(x) \Leftrightarrow f \in \mathrm{Maps}(X, Y)^G$. $\square$

Definition. Let X be a G set and k a field. A map $f\colon X \to k$ is *G-invariant* if $f(g.x) = f(x)$ for all $g \in G$ and $x \in X$.

Example. Let $G = {}^{\mathbb{Z}}/_{2\mathbb{Z}} = \{e, s\}$ and $k = \mathbb{R}$. Let G act on $\mathbb{R}$ by $s.\lambda = -\lambda$. Any polynomial $p(t) \in \mathbb{R}[t]$ can be viewed as an element in $\mathrm{Maps}(\mathbb{R}, \mathbb{R})$. Then $p(t) = \sum a_i t^i$ is G-invariant iff $p(t)$ is even (i.e. $a_i = 0$ for odd i).

Proof.
$$\begin{aligned}
& p(t) \text{ is } G\text{-invariant} \\
\Leftrightarrow\quad & \forall \lambda \in \mathbb{R} : p(s.\lambda) = p(\lambda) \\
\Leftrightarrow\quad & \forall \lambda \in \mathbb{R} : p(-\lambda) = p(\lambda) \\
\Leftrightarrow\quad & \forall \lambda \in \mathbb{R} : \sum_i (-1)^i a_i \lambda^i = \sum_i a_i \lambda^i \\
\Leftrightarrow\quad & \forall \lambda \in \mathbb{R} : 2 \sum_{i \text{ odd}} a_i \lambda^i = 0 \\
\Leftrightarrow\quad & a_i = 0 \text{ for all odd } i
\end{aligned}$$
$\square$

Remark. $f\colon X \to k$ is G-invariant iff $f \in \mathrm{Maps}(X, k)^G$ where we have trivial G-action on k.

Lemma I.6 (Universal property of invariant maps)**.** *Let X be a G-set, k a field (or a commutative ring with 1). Then $f\colon X \to k$ is G-invariant iff f factors through* can *(i.e. $\exists! \overline{f}\colon G \backslash\!\backslash X \to k$ such that $f = \overline{f} \circ \mathrm{can}$).*

$$\begin{tikzcd}
X \arrow[r, "f"] \arrow[d, "\mathrm{can}"'] & k \\
G \backslash\!\backslash X \arrow[ur, dashed, "\exists! \overline{f}"'] &
\end{tikzcd}$$

Proof.
$$\begin{aligned}
& f \text{ is } G\text{-invariant} \\
\Leftrightarrow\quad & \forall g \in G, x \in X : f(g.x) = f(x) \\
\Leftrightarrow\quad & f \text{ is constant on orbits} \\
\Leftrightarrow\quad & \overline{f} \text{ exists (namely } \overline{f}(G_x) = f(x), \text{ obviously unique)}
\end{aligned}$$
$\square$

Lemma I.7. *Let X be a finite G-set and k a field (or commutative ring with 1). Then:*

1) $\mathrm{Maps}(X,k)$ *is a k-vector space (or k-module) with pointwise addition and scalar multiplication.*

2) *A k-basis of* $\mathrm{Maps}(X,k)$ *is given by*

$$\mathcal{X}_x\colon y \mapsto \begin{cases} 1 & \text{if } x = y \\ 0 & \text{otherwise} \end{cases}$$

where $x \in X$.

3) $\mathrm{Maps}(X,k)^G$ *forms a subspace (or submodule) with basis*

$$\mathcal{X}_{\mathcal{G}}\colon y \mapsto \begin{cases} 1 & \text{if } y \in \mathcal{G} \\ 0 & \text{otherwise} \end{cases}$$

where $\mathcal{G} \in G \setminus\!\!\setminus X$.

Proof.

1) Clear.

2) Generating system: Let $f \in \mathrm{Maps}(X,k)$. Then $f = \sum_{x\in X} f(x)\mathcal{X}_x$, as we have $\sum_{x\in X} f(x)\mathcal{X}_x(y) = f(y)$ for all $y \in X$.

   Linear independence: Let $\sum_{x\in X} a_x\mathcal{X}_x = 0$ for some $a_x \in k$. Thus, $\sum_{x\in X} a_x\mathcal{X}_x(y) = 0$ for all $y \in X$, and we have $a_y = 0$ for all $y \in X$.

3) Generating system: Let $f \in \mathrm{Maps}(X,k)^G$. Hence, f is constant on orbits, and we have $f = \sum_{\mathcal{G}\in G\setminus\!\setminus X} a_{\mathcal{G}}\mathcal{X}_{\mathcal{G}}$ with $a_{\mathcal{G}} = f(x)$ for $x \in \mathcal{G}$.

   Linear independence: As in 2). □

If X is an infinite set we often replace $\mathrm{Maps}(X,k)$ by

$$kX := \{f\colon X \to k \mid \operatorname{supp} f \text{ is finite}\}$$

where $\operatorname{supp} f := \{x \in X \mid f(x) \neq 0\}$ is the *support* of f.

Note. We have

$$\begin{aligned} \operatorname{supp}(f_1 + f_2) &\subseteq \operatorname{supp} f_1 \cup \operatorname{supp} f_2, \\ \operatorname{supp}(\lambda f) &\subseteq \operatorname{supp} f \end{aligned}$$

for all $f_1, f_2, f \in \mathrm{Maps}(X,k)$ and $\lambda \in k \setminus \{0\}$. Thus, $kX \subseteq \mathrm{Maps}(X,k)$ together with the 0-function is a vector space (usually just call it kX as well).

kX is preserved under G-action. Let $f \in kX, g \in G$. Then

$$\begin{aligned} & (g.f)(x) \neq 0 \\ \Leftrightarrow \quad & f(g^{-1}.x) \neq 0 \\ \Leftrightarrow \quad & g^{-1}.x \in \operatorname{supp} f \\ \Leftrightarrow \quad & x \in \underbrace{\{g.y \mid y \in \operatorname{supp} f\}}_{\text{finite}}. \end{aligned}$$

Lemma I.7 generalizes to kX.

Lemma I.8. *Let G be a group and R a ring. Let G act on R by ring homomorphisms (i.e. if $\pi\colon R \to R$ is the action then $\pi_g\colon R \to R$ is a ring homomorphism for all $g \in G$) then R^G is a subring of R.*

Proof. Let $r_1, r_2 \in R^G$. To show: $r_1 + r_2, r_1 r_2 \in R^G$. For $g \in G$ we have $g.(r_1 + r_2) = \pi_g(r_1 + r_2) = \pi_g(r_1) + \pi_g(r_2) = g.r_1 + g.r_2 = r_1 + r_2$. Similarly, $g.(r_1 r_2) = r_1 r_2$. $\square$

Example. Even polynomials form a subring of $\mathbb{R}[t]$.

Definition. If G, H are groups and X a G-set and an H-set then the two actions *commute* if

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

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

[October 8, 2018]

[October 11, 2018]

II. Representations of groups

Definition. Let G be a group, V a k-vector space and $G \times V \to V$ an action. This action is *linear* if $\pi_g\colon V \to V$ is a linear map for all $g \in G$. Then V is called a *G-space* or a *representation* of G.

Example. If V is a k-vector space then $\mathrm{GL}(V)$ acts linearly on V by $g.v = g(v)$ for all $g \in \mathrm{GL}(V)$ and $v \in V$. We call this the *standard representation.*

Remark. We have a bijection

$$\begin{aligned} \{\text{linear } G\text{-actions on } V\} \quad & \overset{1:1}{\longleftrightarrow} \quad \{\text{group homomorphisms } G \to \mathrm{GL}(V)\}, \\ \pi \quad & \longmapsto \quad (g \mapsto \pi_g). \end{aligned}$$

Examples.

1) Let X be a G-set. Then kX is a representation (the *regular representation* of kX) of G via
$$g.\left(\sum_{x\in X} a_x\mathcal{X}_x\right) = \sum_{x\in X} a_x\mathcal{X}_{g.x}.$$

2) Let V and W be representations of G over K. Then the G-action on $\operatorname{Maps}(V,W)$ induces a G-action on $\operatorname{Hom}_k(V,W) = \{f\colon V\to W \mid f\ k\text{-linear}\}$.

3) Let V and W be representations of G over k. Then $V\oplus W$ and $V\otimes W$ are representations of G, called direct sum and tensor product via $g.(v,w) = (g.v, g.w)$ and $g.(v\otimes w) = (g.v)\otimes(g.w)$ extended linearly.

Definition. Let V be a representation of G over k.

- A *subrepresentation* of V is a vector subspace U of V such that $g.u\in U$ for all $g\in G$ and $u\in U$. It is *proper* if $0\neq U\neq V$.
- V is *irreducible* if $V\neq 0$ and there is no proper subrepresentation.
- V is *indecomposable* if it cannot be written as a decomposition $V = U_1\oplus U_2$ such that U_1 and U_2 are proper subrepresentations.
- V is *completely reducible* if $V = \sum_{i\in I} V_i$ where V_i are irreducible subrepresentations (for some set I).

Example. Let
$$G = \left\{\begin{pmatrix} a & b\\ 0 & c\end{pmatrix} \,\middle|\, a,b,c\in\mathbb{C}, a,c\neq 0\right\}$$
act on $V=\mathbb{C}^2$ by standard action. Then $U = \left\langle\begin{pmatrix}1\\0\end{pmatrix}\right\rangle$ is a proper subrepresentation of V, but V is not irreducible. But V is indecomposable since U is the unique proper subrepresentation. To see this, assume $U' = \left\langle\begin{pmatrix}x\\y\end{pmatrix}\right\rangle$ to be a proper subrepresentation. Then
$$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}x+y\\y\end{pmatrix}\in U',$$
and as U' is a subspace, we have $\begin{pmatrix}y\\0\end{pmatrix}\in U'$ and therefore $U'=U$. V is also not completely irreducible.

Definition. Let G be a group and k a field. The group algebra of G over k is the k-algebra given by the k-vector space
$$kG = \{f\colon G\to k \mid \operatorname{supp} f \text{ is finite}\}$$

with multiplication given by convolution of functions

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

with unit $1 = \mathcal{X}_e$.

Indeed, we have

$$(f \cdot \mathcal{X}_e)(x) = \sum_{y \in G} f(y) \underbrace{\mathcal{X}_e(y^{-1}x)}_{\text{nonzero iff } y = x} = f(x) \quad \text{and} \quad (\mathcal{X}_e \cdot f)(x) = \sum_{y \in G} \underbrace{\mathcal{X}_e(y)}_{\text{nonzero iff } y = 1} f(y^{-1}x) = f(x)$$

for all $f \in kG$. It remains to check associativity and distributivity.

Remark. The group algebra can be defined in the same way over any commutative ring with 1. We write

$$\sum_{g \in G} a_g g := \sum_{g \in G} a_g \mathcal{X}_g$$

where $a_g \in k$ and almost all $a_g = 0$.

Lemma II.1. *The algebra structure on kG is given by extending the multiplication on G bilinearly.*

Proof. We have

$$(\mathcal{X}_g \cdot \mathcal{X}_h)(x) = \sum_{y \in G} \mathcal{X}_g(y) \mathcal{X}_h(y^{-1}x) = \begin{cases} 1 & \text{if } h = g^{-1}x \\ 0 & \text{otherwise} \end{cases} = \mathcal{X}_{gh}(x).$$

By definition the convolution product extends this bilinearly. □

Note. kG is commutative iff G is abelian.

Lemma II.2. *Let G be a group and V a k-vector space. Then*

$$\begin{array}{rcl} \{\textit{linear } G\textit{-actions on } V\} & \overset{1:1}{\longleftrightarrow} & \{kG\textit{-module structures on } V\}, \\ (G \times V \to V) & \mapsto & \left(\left(\sum_{g \in G} a_g g \right) .v := \sum_{g \in G} a_g (g.v) \right). \end{array}$$

Proof. Left to the reader. □

Definition. Let V and W be representations of G over k. A *morphism* (of representations) from V to W si a linear, G-equivariant map $f \colon V \to W$. Denote $\mathrm{Hom}_G(V, W) := \{f \colon V \to W \text{ morphisms of representations}\}$ and $\mathrm{End}_G(V) := \mathrm{Hom}_G(V, V)$.

Note. $\mathrm{Hom}_G(V,W)$ is a vector space. Write $V \cong W$ if there exists an isomorphism $V \to W$.

Lemma II.3. *Let G be a group and k a field. Representations of G over k together with morphisms of representations form a category $\mathrm{Rep}_k(G)$.*

Proof. See Lemma II.2. □

Example. For a field k, the k-vector spaces together with k-linear maps form a category Vect_k.

Corollary II.4. *Let k be a field. The assignments*

$$\begin{aligned} F\colon \mathrm{Rep}_k(G) &\to \mathrm{Vect}_k \\ V &\mapsto V^G \\ f &\mapsto f^G\colon V^G \to W^G \end{aligned}$$

define a functor from $\mathrm{Rep}_k(G)$ to Vect_k, the functor of G-invariants.

Proof. Left to the reader. □

Lemma II.5. *If $f\colon V \to W$ is a morphism of representations of G then $\ker f$ and $\operatorname{im} f$ are subrepresentations of V respectively W.*

Proof. $\ker f$ and $\operatorname{im} f$ are subspaces since f is linear. Let $g \in G$ and $x \in \ker f$. Then $f(g.x) = g.f(x) = g.0 = 0$ and $g.x \in \ker f$, thus $\ker f$ is a subrepresentation.

Let $y \operatorname{im} f$ and $x \in V$ with $f(x) = y$. We get $g.y = g.(f(x)) = f(g.x) \operatorname{im} f$. □

Remark. It can be shown that $\mathrm{Rep}_k(G)$ is an abelian category.

Lemma II.6 (Schur's lemma)**.** *Let G be a group and V, W irreducible representations of G over k.*

1) $\mathrm{Hom}_G(V,W) = 0$ *if* $V \not\cong W$. *If* $V \cong W$, *we have* $\mathrm{Hom}_G(V,W) \neq 0$ *and every non-zero morphism is an isomorphism.*

2) *If $k = \overline{k}$ and V and W are finite-dimensional then*

$$\mathrm{Hom}_G(V,W) \cong \begin{cases} k & \text{if } V \cong W \\ 0 & \text{if } V \not\cong W \end{cases}$$

as representations.

Proof.

1) Assume $V \cong W$ and $0 \neq f \in \mathrm{Hom}_G(V,W)$. This implies $\ker f \neq V$ and $\operatorname{im} F \neq 0$. By Lemma II.5 it follows $\ker f = 0$ and $\operatorname{im} f = W$, since f is a morphism and V and W are irreducible. As f is linear, f is an isomorphism.

2) Assume $V \cong W$ and $0 \neq \alpha, \beta \in \mathrm{Hom}_G(V, W)$. It is enough to show $\beta = \lambda\alpha$ for some $\lambda \in k$. By 1) α has an inverse α^{-1} (which is again a morphism) and we have $\alpha^{-1} \circ \beta \in \mathrm{End}_G(V)$. If $k = \overline{k}$ and V is finite-dimensional $\alpha^{-1} \circ \beta$ has eigenvectors. We define $K := \ker(\alpha^{-1} \circ \beta - \lambda \, \mathrm{id}_V) \neq 0$ for some $\lambda \in k$. Now $\alpha^{-1} \circ \beta - \lambda \, \mathrm{id}_v \in \mathrm{End}_G(V)$ (the reader may check this statement), thus K is a subrepresentation of V, hence $K = V$, since V is irreducible and $K \neq 0$. Therefore, $\alpha^{-1} \circ \beta = \lambda \, \mathrm{id}_V$ and $\beta = \lambda\alpha$. □

Corollary II.7. *Let $k = \overline{k}$ and V_i $(1 \leq i \leq r)$ be pairwise non-isomorphic irreducible finite-dimensional representations of G over k. Let $W_i := V_i^{\oplus n_i} := V_i \oplus \ldots \oplus V_i$ for some $n_i \in \mathrm{Z}_{>0}$ (a representation of G). Then*

$$\mathrm{End}_G(W_1 \oplus \ldots \oplus W_r) \cong \mathrm{M}_{n_1 \times n_1}(k) \oplus \ldots \oplus M_{n_r \times n_r}(k)$$

as algebras.

Proof. We have

$$\mathrm{End}_G(W_1 \oplus \ldots \oplus W_r) = \mathrm{Hom}_G\left(\bigoplus_{i=1}^{r}\bigoplus_{j=1}^{n_i} V_i, \bigoplus_{i=1}^{r}\bigoplus_{j=1}^{n_i} V_i\right)$$

and by Schur's lemma, since $V_i \cong V_i$, and $\mathrm{End}_G(V_i) \cong k$, we get

$$\begin{aligned} &\cong \mathrm{End}_G(V_1^{\oplus n_1}) \oplus \ldots \oplus \mathrm{End}_G(V_r^{\oplus n_r}) \\ &\cong \mathrm{M}_{n_1 \times n_1}(k) \oplus \ldots \oplus M_{n_r \times n_r}(k). \end{aligned}$$
□

[October 11, 2018]

[October 15, 2018]

Theorem II.8 (Maschke's theorem)**.** *Let G be a finite group and k a field such that* $\mathrm{char}\, k \nmid |G|$ *(in particular* $\mathrm{char}\, k = 0$ *is allowed). The the finite-dimensional representations of G over k are completely reducible.*

Proof. It is enough to show that for any finite-dimensional representation V of G the following holds: any subrepresentation U of V has a complement in W in V which is again a subrepresentation; so $V = U \oplus W$ as representations. Let U be such a subrepresentation and choose a vector space complement U' so $V = U \oplus U'$ as vector spaces.

Define now $\hat{p}\colon V \to U$ by

$$\hat{p}(v) = \frac{1}{|G|} \sum_{g \in G} \underbrace{g^{-1}. \underbrace{p(g.v)}_{\in U}}_{\in U} \in U.$$

Now:

- We have $\hat{p}(u) = \frac{1}{|G|}\sum_{g\in G} g^{-1}.p(g.h.v) = \frac{1}{|G|}\sum_{g\in G} g^{-1}.g.u = u$ for all $u \in U$.

- $\hat{p}$ is G-equivariant, as for any $h \in G$ and $v \in V$

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

Therefore, $V = \operatorname{im}\hat{p} \oplus \ker\hat{p} = U \oplus \ker\hat{p}$ since $\hat{p}$ is G-equivariant. $W := \ker\hat{p}$ is a subrepresentation of V. □

Warning. Maschke's theorem does not hold in general if $\operatorname{char} k \mid |G|$. For example, take $G = \mathbb{Z}/2\mathbb{Z} = \{e, s\}$, $k = \mathbb{F}_2$ and $V = kG$ the regular representation. Then $\langle e+s\rangle_k$ is a 1-dimensional subrepresentation, but in fact the unique one. Therefore, it has no complement. (Note: if $\operatorname{char} k \neq 2$ then $\langle e+s\rangle_k$ is also a 1-dimensional subrepresentation and a complement of the above one).

III. Invariant polynomial functions

III.1. Gradings and filtrations

Definition. Let A be a k-algebra. A *grading* (or $\mathbb{Z}$-*grading*) on A is a decomposition

$$A = \bigoplus_{i\in IZ} A_i$$

into vector subspaces A_i such that $A_iA_j \subseteq A_{i+j}$ for all $i, j \in \mathbb{Z}$. We call then A a *graded algebra*. The A_i ($i \in \mathbb{Z}$) are the *graded* (or *homogeneous*) *components*. An element $a_i \in A_i$ is called *homogeneous* (of degree i).

Definition. A *grading* of a ring R is a decomposition $R = \bigoplus_{i\in\mathbb{Z}} R_i$ into $\mathbb{Z}$-modules such that $R_iR_j \subseteq R_{i+j}$ for all $i, j \in \mathbb{Z}$. We call then R a *graded* ring and the R_i the *graded/homogeneous components*.

Lemma III.1. *Let k be a field and A a k-algebra with* 1.

$$A = \bigoplus_{i\in\mathbb{Z}} A_i \text{ is a graded algebra.} \iff A = \bigoplus_{i\in\mathbb{Z}} A_i \text{ is a graded ring and } k1 \subseteq A_0.$$

Proof.

"$\Leftarrow$" $A = \bigoplus_{i\in\mathbb{Z}} A_i$ is a decomposition into k-vector spaces; in particular into $\mathbb{Z}$-modules. We have to show $k1 \subseteq A_0$.

Write $1 = \sum_{i\in\mathbb{Z}} e_i$ with $e_i \in A_i$ and almost all $e_i = 0$. Then for any $a \in A_j$ we have $a = a1 = \sum_{i\in\mathbb{Z}} ae_i$. As $ae_i \in A_{j+i}$, we have $a = ae_0$ because the sum $A = \bigoplus_{i\in\mathbb{Z}} A_i$ is direct. Similarly we get $e_0 a = a$. Thus, $e_0 = a = ae_0$ for all $a \in A$, and we have $1 = e_0 \in A_0$ and finally $k1 = ke_0 \subseteq A_0$ since A_0 is a vector space.

"$\Rightarrow$" We have to show that A_i is closed under scalar multiplication for all $i \in \mathbb{Z}$. Let $\lambda \in k$ and $i \in \mathbb{Z}$. Then $\lambda A_i = (\lambda 1)A_i \subseteq A_0 A_i \subseteq A_{0+i} = A_i$. $\square$

Examples.

1) Let A be any k-algebra. It is a graded algebra via the "stupid grading" $A = \bigoplus_{i\in\mathbb{Z}} A_i$ where
$$A_i = \begin{cases} A & \text{if } i = 0, \\ 0 & \text{if } i \neq 0. \end{cases}$$

2) Let $R = \mathbb{Z}$ or $R = k$ for a field. Then $A = R[X_1, \ldots, X_n]$ is a graded ring respectively a graded algebra where $A = \sum_{i\in\mathbb{Z}} A_i$ is given by
$$A_i = \begin{cases} 0 & \text{if } i < 0, \\ \left\langle \left\{ X_1^{a_1} \cdots X_n^{a_n} \,\middle|\, \sum_{j=1}^n a_j = i \right\} \right\rangle_R & \text{else,} \end{cases}$$
because clearly the monomials $X_1^{a_1} \cdots X_n^{a_n}$ with $a_i \in \mathbb{Z}_{\geq 0}$ (and by convention $X_1^0 \cdots X_n^0 = 1$) form an R-basis of $R[X_1, \ldots, X_n]$ and $(X_1^{a_1} \cdots X_n^{a_n})(X_1^{b_1} \cdots X_n^{b_n}) = (X_1^{a_1+b_1} \cdots X_n^{a_n+b_n})$, so that $a_i a_j \in A_{i+j}$ for all basis elements $a_i \in A_i$ and $a_j \in A_j$ (then also $A_i A_j \subseteq A_{i+j}$).

3) Let V be a k-vector space. Consider the vector space
$$\mathrm{T}(V) := k \oplus V \oplus (V \otimes V) \oplus \ldots = k \oplus \bigoplus_{d\geq 1} V^{\otimes d} =: \bigoplus_{d\geq 0} V^{\otimes d},$$
the *tensor algebra*. We claim that $\mathrm{T}(V)$ is an algebra by setting
$$\underbrace{(v_{i_1} \otimes \ldots \otimes v_{i_d})}_{\in V^{\otimes d}} \underbrace{(v_{j_1} \otimes \ldots \otimes v_{j_{d'}})}_{\in V^{\otimes d'}} = \underbrace{v_{i_1} \otimes \ldots \otimes v_{i_d} \otimes v_{j_1} \otimes \ldots \otimes v_{j_{d'}}}_{\in V^{\otimes (d+d')}}$$
for any v_{i_r}, v_{j_s} in a chosen basis $\{v_i \mid i \in I\}$ of V ($1 \leq r \leq d$, $1 \leq s \leq d'$) and extended linearly to $\mathrm{T}(V)$ with
$$\underbrace{\lambda}_{\in V^{\otimes 0}} \cdot \underbrace{v}_{\in V^{\otimes d}} := \underbrace{\lambda v}_{\in V^{\otimes d}} \qquad \text{and} \qquad \underbrace{v}_{\in V^{\otimes d}} \cdot \underbrace{\lambda}_{\in V^{\otimes 0}} := \underbrace{\lambda v}_{\in V^{\otimes d}}.$$
We also claim that $\mathrm{T}(V) = \bigoplus_{i\in\mathbb{Z}} \mathrm{T}(V)_i$ with
$$\mathrm{T}(V)_i := \begin{cases} V^{\otimes i} & \text{if } i \geq 0 \\ 0 & \text{otherwise} \end{cases}$$
is then a graded algebra.

Definition. Let A be a k-algebra. A *filtration* of A is a (possibly infinite) sequence $F_\bullet(A)$ of vector subspaces of the form

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

such that

1) $F_i(A)F_j(A) \subseteq F_{i+j}(A)$ for all $i, j \in \mathbb{Z}_{\geq -1}$ and
2) $\bigcup\limits_{i \geq -1} F_i(A) = A$.

An algebra with a filtration is a *filtered* algebra.

Proposition III.2. *If A is a filtered algebra with filtration $F_\bullet(A)$ then we can consider the vector space*

$$\operatorname{gr} A := \bigoplus_{i \in \mathbb{Z}} (\operatorname{gr} A)_i \quad \textit{where} \quad (\operatorname{gr} A)_i = \begin{cases} {}^{F_i(A)}/_{F_{i-1}(A)} & \textit{if } i \geq 0, \\ 0 & \textit{if } i < 0. \end{cases}$$

Then $\operatorname{gr} A$ *becomes a graded algebra by defining the multiplication*

$$(a + F_{i-1}(A))(b + F_{j-1}(A)) := ab + F_{i+j-1}(A)$$

for any $a \in F_i(A)$ and $b \in F_j(A)$. It is called the associated graded algebra *to the filtered algebra $(A, F_\bullet(A))$.*

Proof. We have to show that the multiplication is well-defined. Note that we have

$$\begin{aligned} F_{i-1}(A)b &\subseteq F_{i-1}(A)F_j(A) \subseteq F_{i+j-1}(A), \\ aF_{j-1}(A) &\subseteq F_i(A)F_{j-1}(A) \subseteq F_{i+j-1}(A), \\ F_{i-1}(A)F_{j-1}(A) &\subseteq F_{i+j-2}(A) \qquad \subseteq F_{i+j-1}(A). \end{aligned}$$

Therefore, we have

$$(a + F_{i-1}(A))(b + F_j(A)) = (c + F_{i-1}(A))(d + F_j(A))$$

if $a + F_{i-1}(A) = c + F_{i-1}(A)$ in ${}^{F_{i+j}(A)}/_{F_{i+j-1}(A)}$ and $b + F_j(A) = d + F_j(A)$ for all $a, c \in F_j(A)$ and $b, d \in F_j(A)$.

Associativity and distributivity follow from the same properties in A. □

Proposition III.3. *Let $A = \bigoplus_{i \in \mathbb{Z}} A_i$ be a graded algebra such that $A_i = 0$ for $i < 0$. Then define*

$$F_j(A) = \bigoplus_{0 \leq i \leq j} A_i$$

for all $j \geq 0$. Then

$$0 =: F_{-1}(A) \subseteq F_0(A) \subseteq F_1(A) \subseteq \ldots \subseteq A \tag{*}$$

turns into a filtered algebra.

Proof. Obviously $F_j(A) \subseteq A$ are vector subspaces for all $j \geq -1$ and (*) is a sequence of nested vector spaces.

2) Any $a \in A$ can be written as $a = \sum_{i=0}^{\infty} a_i$ with $a_i \in A_i$ where almost all $a_i = 0$. There exists $j > 0$ such that $a \in F_j(A)$ and we have
$$A \subseteq \bigcup_{j \geq -1} F_j(A).$$

1) Let $A \in F_r(A)$ and $b \in F_s(A)$. We can write $a = \sum_{i=1}^{r} a_i$ and $b = \sum_{i=1}^{s} b_i$ for some $a_i, b_i \in A_i$. Thus we get
$$ab \in \sum_{\substack{0 \leq i \leq r \\ 0 \leq j \leq s}} \underbrace{a_i b_j}_{A_{i+j}} \in \bigoplus_{l=0}^{r+s} A_l = F_{r+s}(A).$$
□

Remark. At this point Professor Stroppel seems not to have numbered this proposition in her notes. Therefore, the next Lemma will have the same number.

Examples.

1) Let $R = \mathbb{Z}$ or $R = k$ a field. Consider $A = R[X_1, \ldots, X_n]$. This is a filtered algebra by setting
$$F_j(A) = \left\langle \left\{ X_1^{a_1} \cdots X_n^{a_n} \;\middle|\; \sum_{i=1}^{n} a_i = j \right\} \right\rangle_R$$
for $j \geq 0$ ($F_{-1}(A) = 0$).

2) Let $R = k[t]$ for any field k. Consider $\mathrm{End}_k(k[t])$ (linear endomorphisms). There are the two following interesting elements in $\mathrm{End}_k(k[t])$:
$$\begin{aligned} X \colon k[t] &\to k[t] \\ p &\mapsto tp \end{aligned} \qquad\qquad \begin{aligned} \partial \colon k[t] &\to k[t] \\ p &\mapsto p' := \text{formal derivation} \end{aligned}$$
Let A be the subalgebra of $\mathrm{End}_k(k[t])$ generated by X and ∂. This is called the (first) *Weyl algebra* $\mathcal{A}_1$.

We claim that A has basis $\{X^a \partial^b \mid a, b \in \mathbb{Z}_{\geq 0}\}$ (with $X^0\partial^0 = 1$). The reader may check this using the formula $\partial X = X\partial + \mathrm{id}$. Furthermore, one can define a filtration on A via $F_j(A) = \left\langle \{X^a \partial^b \mid a + b \leq j\} \right\rangle$ for $j \geq 0$.

[October 15, 2018]

[October 18, 2018]

Remark. For $(A, F_\bullet(A))$ a filtered algebra the canonical map

$$\begin{aligned} \mathrm{can}\colon A &\to \operatorname{gr} A = \bigoplus_{i\geq 0} {}^{F_i(A)}/_{F_{i-1}(A)} \\ a &\mapsto (a + F_{i-1}(A))_{i\geq 0} \end{aligned}$$

is in general *not* an algebra homomorphism.

Definition. Let $A = \bigoplus_{i\in\mathbb{Z}} A_i$ be a graded algebra and M and A-module. Then a *grading* on M is a decomposition $M = \bigoplus_{i\in\mathbb{Z}} M_i$ into vector spaces such that $A_i M_j \subseteq M_{i+j}$ for all $i, j \in \mathbb{Z}$. Then M is called a *graded* module.

For graded A-modules $M = \bigoplus_{i\in\mathbb{Z}} M_i$ and $N = \bigoplus_{i\in\mathbb{Z}} N_i$, a morphism of graded A-modules from M to N is a morphism $f\colon M \to N$ of A-modules such that $f(M_i) \subseteq N_i$ for all $i \in \mathbb{Z}$.

Remark. Graded A-modules with graded A-module homomorphisms form a category (where A is a graded algebra).

III.2. Symmetric polynomials

Definition. Let k b a field. Let $G := S_n = S(\{1, \dots, n\})$ act linearly on $K[X_1, \dots, X_n]$ by

$$g.X_1^{a_1} X_2^{a_2} \cdots X_n^{a_n} = X_{g(1)}^{a_1} X_{g(2)}^{a_2} \cdots X_{g(n)}^{a_n}. \tag{*}$$

A polynomial in $k[X_1, \dots, X_n]^G$ is called a *symmetric* polynomial (in n variables).

Remark. We could replace k by any commutative ring R with 1 and extend (*) R-linearly to get an action of G on $R[X_1, \dots, X_n]$.

Examples. In $K[X_1, X_2, X_3]^{S_3}$ we have e.g. the following elements:

$$\begin{aligned} p_2^{(3)} &= X_1^2 + X_2^2 + X_3^2 \\ h_2^{(3)} &= X_1^2 + X_1X_2 + X_1X_3 + X_2^2 + X_2X_3 + X_3^2 \\ e_2^{(3)} &= X_1X_2 + X_1X_3 + X_2X_3 \\ m_{(4,4,2)}^{(3)} &= X_1^4X_2^4X_3^2 + X_1^4X_2^2X_3^4 + X_1^2X_2^4X_3^4 + X_1^2X_2^4X_3^4 \end{aligned}$$

Definition. Let $n \in \mathbb{Z}_{>0}$ and $r \in \mathbb{Z}_{\geq 0}$. Define the symmetric polynomials

$$p_r^{(n)} := X_1^r + X_2^r + \ldots + X_n^r,$$

the r-th *power symmetric polynomial* (with $p_0^{(n)} = n$),

$$h_r^{(n)} := \sum_{|a|=r} X_1^{a_1} X_2^{a_2} \cdots X_n^{a_n}$$

where $a = (a_i)_{1\leq i\leq n} \in \mathbb{Z}^n_{\geq 0}$ with $|a| = \sum_{i=1}^n a_i$, the r-th *complete symmetric polynomial* ($h_0^{(n)} = 1$),

$$e_r^{(n)} := \sum_{1\leq i_1<\ldots<i_r\leq n} X_{i_1}X_{i_2}\cdots X_{i_r} = \sum_{\substack{I\subseteq\{1,\ldots,n\}\\ |I|=r}} \prod_{i\in I} X_i,$$

the r-th *elementary symmetric polynomial* (with $e_0^{(n)} = 1$ and $e_r^{(n)} = 0$ if $r > n$).

Lemma III.3. *For all $n \in \mathbb{Z}_{>0}$ we have in $\mathbb{Z}[X_1, \ldots, X_n][t]$*

$$\prod_{i=1}^n (t - X_i) = t^n - e_1^n t^{n-1} + e_2^{(n)} t^{n-2} + \ldots + (-1)^n e_n^{(n)}.$$

Proof. The coefficient of t^{n-j} on the left hand side equals

$$\sum_{i\leq i_1<\ldots<i_j\leq n} (-X_{i_1})(-X_{i_2})\cdots(-X_{i_j}) = (-1)^j e_j^{(n)}.$$

□

Theorem III.4 (Fundamental theorem of symmetric polynomials)**.** *The elementary symmetric polynomials $e_1^{(n)}, \ldots, e_n^{(n)}$ generate $k[X_1, \ldots, X_n]^{S_n}$ as a k-algebra. Moreover they are algebraically independent over k. That means*

$$\begin{array}{rcl} k[X_1, \ldots, X_n]^{S_n} & \to & k[t_1, \ldots, t_n] \\ e_j^{(n)} & \mapsto & t_j \end{array}$$

is an isomorphism of algebras.

Lemma III.5. *Let G be a group and V_i ($i \in I$) representations of G (over some fixed field k). Then*

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

as vector subspaces of $\bigoplus_{i\in I} V_i$.

Proof.

"$\supseteq$" Obvious.

"$\subseteq$" Let $v = \sum_{i\in I} v_i \in (\bigoplus_{i\in I} V_i)^G$. Then we have

$$v = g.v = g.\left(\sum_{i\in I} v_i\right) = \sum_{i\in I} g.v_i$$

for all $g \in G$ since the sum is direct. We get $v_i = g.v_i$ for all $i \in I$ and $g \in G$, and therefore $v_i \in V_i^G$ for all $i \in I$. □

Lemma III.6. *A polynomial $f \in k[X_1, \ldots, X_n]$ is symmetric if and only if its homogeneous parts $f_i \in k[X_1, \ldots, X_n]$ are symmetric.*

Proof. Let $A = k[X_1, \ldots, X_n] = \sum_{i \in \mathbb{Z}} k[X_1, \ldots, X_n]_i$ the decomposition (since A is a graded algebra) where

$$k[X_1, \ldots, X_n]_i = \begin{cases} 0 & \text{if } i < 0, \\ \left\langle \left\{ X_1^{a_1} \cdots X_n^{a_n} \;\middle|\; \sum_{j=1}^n a_j = i \right\} \right\rangle & \text{otherwise.} \end{cases}$$

$G = S_n$ acts on A as above and preserves $k[X_1, \ldots, X_n]_i =: A_i$. By Lemma III.5 we get

$$k[X_1 \ldots, X_n]^{S_n} = A^G = \bigoplus_{i \in \mathbb{Z}} A_i^G = \bigoplus_{i \in \mathbb{Z}} k[X_1, \ldots, X_n]_i^{S_n}$$

□

The following formula holds for all $1 \leq r \leq n$ ($n \in \mathbb{Z}_{>0}$).

$$e_r^{(n)} = e_r^{(n-1)} + X_n e_{r-1}^{(n-1)}$$

Proof.

$$\begin{aligned} e_r^{(n)} &= \sum_{\substack{I \subseteq \{1, \ldots, n\} \\ |I| = r}} \prod_{i \in I} X_i = \sum_{\substack{I \subseteq \{1, \ldots, n-1\} \\ |I| = r}} \prod_{i \in I} X_i + X_n \sum_{\substack{I \subseteq \{1, \ldots, n-1\} \\ |I| = r-1}} \prod_{i \in I} X_i \\ &= e_r^{(n-1)} + X_n e_r - 1^{(n-1)} \end{aligned}$$

□

Lemma III.7. *A polynomial $f \in k[X_1, \ldots, X_n]$ is symmetric if and only if it can be expressed as a polynomial in the $e_r^{(n)}$'s (over k).*

Proof.

"⇒" We have $e \in k[X_1, \ldots, X_n]^{S_n}$. But $k[X_1, \ldots, X_n]^{S_n}$ is a subring, even a subalgebra.

"⇐" Let $f \in k[X_1, \ldots, X_n]^{S_n}$ a symmetric polynomial. We use induction on n.

For $n = 1$ we have $k[X_1]^{S_1} = k[X_1]^{\{e\}} = k[X_1] = k\left[e_1^{(1)}\right]$.

Assume the lemma for $n - 1$. Let $d = \deg f$. If $d \leq 1$, the claim is obvious. Let $d \geq 2$ and assume the lemma holds for any symmetric polynomial h with $\deg h < d$.

Consider

$$\begin{aligned} q\colon k[X_1, \ldots, X_n] &\to k[X_1, \ldots, X_n]/(X_n) \cong k[X_1, \ldots, X_{n-1}], \\ p(x_1, \ldots, x_n) &\mapsto p(x_1, \ldots, x_{n-1}, 0). \end{aligned}$$

Check that q is an algebra homomorphism. We have:

- $q(e_j^{(n)}) = e_j^{(n-1)}$ for all $0 \leq j > n$.
- $q(e_n^{(n)}) = 0$.

- $q(f) \in k[X_1,\dots,X_n]^{S_{n-1}}$, because for $g \in S_{n-1}$

$$\begin{aligned} g.(q(f)) &= (q(f))(X_{g^{-1}(1)}, X_{g^{-1}(2)}, \dots, X_{g^{-1}(n-1)})) \\ &= q(f(X_{g^{-1}(1)}, X_{g^{-1}(2)}, \dots, X_{g^{-1}(n)})) \\ &= q((g.f)(X_1,\dots,X_n)) \end{aligned}$$

  and as f is symmetric,

$$= q(f).$$

By induction $q(f)$ is a polynomial $P\Big(e_1^{(n-1)},\dots,e_{n-1}^{(n-1)}\Big)$ in $e_1^{(n-1)},\dots,e_{n-1}^{(n-1)}$. Set $g = P\Big(e_1^{(n)},\dots,e_{n-1}^{(n)}\Big) \in k[X_1,\dots,X_n]$. Because q is an algebra homomorphism we have

$$q(g) = P\Big(q\Big(e_1^{(n)}\Big),\dots,q\Big(e_n^{(n)}\Big)\Big) = P\Big(e_1^{(n-1)},\dots,e_{n-1}^{(n-1)},0\Big) = q(f).$$

Therefore, $q(f-g) = 0$ in ${}^{k[X_1,\dots,X_n]}/_{(X_n)}$, and we get $X_n \mid f-g$.

By assumption, f is symmetric, by construction, g is symmetric. Thus, $f-g$ is symmetric, and $X_i \mid f-g$ for all $1 \le i \le n$, and we have $X_1X_2\cdots X_n \mid f-g$. Set

$$h = \frac{f-g}{X_1X_2\cdots X_n} = \frac{f-g}{e_n^{(n)}}$$

(here we use that $k[X_1,\dots,X_n]$ is a unique factorization domain). Now due to $\deg g \le \deg f = d$ we have $\deg h < d$. By induction on degree h canb e written as apolynomial in the $e_1^{(n)},\dots,e_n^{(n)}$. Then, $f-g = e_n^{(n)}h$ as well as $f = e_n^{(n)}h + g$ can be written as such a polynomial by definition of g. □

Proof ot the Fundamental theorem of symmetric polynomials.
We still have to show that the $e_1^{(n)},\dots,e_n^{(n)}$ are algebraically independent (over k). We use induction on n. For $n=1$ we have $k[X_1]^{S_1} = k[X_1] = k[e_1^{(1)}]$.

Assume the claim holds for $n-1 \ge 1$, but it does not hold for n. Then there exists a polynomial $0 \ne P \in k[t_1,\dots,t_n]$ such that $P\Big(e_1^{(n)},\dots,e_n^{(n)}\Big) = 0$. Let P be of minimal possible degree. Then

$$0 = q\Big(P\Big(e_1^{(n)},\dots,e_n^{(n)}\Big)\Big) = P\Big(q\Big(e_1^{(n)}\Big),\dots,q\Big(e_n^{(n)}\Big)\Big) = P\Big(e_1^{(n-1)},\dots,e_{n-1}^{(n-1)},0\Big)$$

and by induction hypothesis $X_n \mid P$.

Therefore, there exists a $\hat{p} \in k[t_1,\dots,t_n]$ such that $P = t_n\hat{P}$. In particular $\hat{P} \ne 0$ and $\deg \hat{P} < \deg P$. We have $0 = P\Big(e_1^{(n)},\dots,e_n^{(n)}\Big) = e_n^{(n)}\hat{P}\Big(e_1^{(n)},\dots,e_n^{(n)}\Big)$. Thus, $\hat{P}\Big(e_1^{(n)},\dots,e_n^{(n)}\Big) = 0$ since $e_n^{(n)} \ne 0$ and $P \mid 0$. This contradicts the minimality of $\deg P$. □

Remark. The proof gives an algorithm how to express a symmetric polynomial f in the $e_1^{(n)},\dots,e_n^{(n)}$.

Remark. The proof and theorem also hold for $\mathbb{Z}[X_1, \ldots, X_n]^{S_n}$.

To better understand the interaction ot the symmetric polynomials $e_r^{(n)}$, $p_r^{(n)}$ and $h_i^{(n)}$ we use *generating series* in $k[X_1, \ldots, X_n][\![t]\!]$. For fix $n \in \mathbb{Z}_{>0}$ we define

$$E(t) := \sum_{r=0}^{n} e_r^{(n)} t^r, \qquad H(t) := \sum_{r \geq 0} h_r^{(n)} t^r, \qquad P(t) := \sum_{r \geq 0} p_{r+1}^{(n)} t^r.$$

Lemma III.8.

1) $E(t) = \prod_{i=1}^{n} (1 + X_i t)$

2) $H(t) = \prod_{i=1}^{n} \frac{1}{1 - X_i t}$

3) $P(t) = \sum_{i=1}^{n} \frac{1}{1 - X_i t}$

Proof.

1) Clear.

2) $1 - X_i t$ is invertible in $k[X_1, \ldots, X_n][\![t]\!]$, namely with the inverse $Q_i(t) = \frac{1}{1-X_i t} := 1 + X_i + X_i^2 t^2 + \ldots$. Then $\prod_{i=1}^{n} \frac{1}{1-X_i t} = Q_1(t) Q_2(t) \cdots Q_n(t)$. But here the coefficient of t_j equals $h_j^{(n)}$.

3) Left to the reader. □

Corollary III.9. *For all $s \geq 1$ we have*

$$h_s^{(n)} - e_1^{(n)} h_{s-1}^{(n)} + e_2^{(n)} h_{s-2}^{(n)} - \ldots + (-1)^s e_s h_0^{(n)} = 0.$$

The same holds with e and h swapped.

Proof. Left to the reader. □

Corollary III.10. *For all $j \geq 1$ we have*

$$j h_j^{(n)} = p_1^{(n)} h_{j-1}^{(n)} + p_2^{(n)} h_{j-2}^{(n)} + \ldots + p_{j-1}^{(n)} h_1^{(n)} + p_j^{(n)} h_0^{(n)}.$$

Proof. Let $H^r(t)$ be the formal derivation of $H(t)$ with respect to t, so $H_r'(t) = \sum_{r \geq 0} r h_r^{(n)} t^{r-1}$. On the other hand (by Lemma III.8)

$$H'(t) = \sum_{i=1}^{n} \left(\frac{X_i}{(1 - X_i t)^2} \prod_{j \neq i} \frac{1}{1 - X_j t} \right) = \sum_{i=1}^{n} \frac{X_i}{1 - X_i t} \left(\prod_{j=1}^{n} \frac{1}{1 - X_j t} \right).$$

By comparing coefficients of t^{r-1} we get

$$r h_r^n = \sum_{s=1}^{r} p_s^{(n)} h_{r-s}^{(n)}$$

using Lemma III.8 2) and 3). □

[October 18, 2018]

[October 22, 2018]

Corollary III.11 (Newton identities). *For all $r \geq 0$ one has*

$$p_r^{(n)} - e_1^{(n)} p_{r-1}^{(n)} + \ldots + (-1)^r e_r^{(n)} p_0^{(n)} = 0.$$

Proof. Left to the reader. □

Corollary III.12. *Let k be a field or $k = \mathbb{Z}$. There exist polynomials $F_1, \ldots, F_n \in k[t_1, \ldots, t_n]$ such that*

$$h_j^{(n)} = F_j(e_1^{(n)}, \ldots, e_n^{(n)}) \quad \textit{und} \quad e_j^{(n)} = F_j\left(h_1^{(n)}, \ldots, h_n^{(n)}\right) = 0$$

for all $1 \leq j \leq n$.

Proof. We have $h_1^{(n)} = X_1 + \ldots + X_n = e_1^{(n)}$. Set $F_1(t_1, \ldots, t_n) = t_1$. Now assume $F_1, \ldots, F_{s-1}$ exist for $1 \leq s \leq n$. Define

$$F_s := t_1 F_{s-1} - t_2 F_{s-2} + \ldots + (-1)^{s-2} t_{s-1} + (-1)^{s-1} t_s.$$

By induction and Corollary III.9 we get

$$F_s = e_1^{(n)} h_{s-1}^{(n)} - e_2^{(n)} h_{s-2}^{(n)} + \ldots + (-1)^{s-2} e_{s-1}^{(n)} h_1 + (-1)^{s-1} e_s^{(n)} h_0^{(n)} = h_s^{(n)}.$$

By switching th ole of the e's and h's (using $e_1^{(n)} = h_1^{(n)}$) and Corollary III.9 again gives $F_s\left(h_1^{(n)}, \ldots, h_n^{(n)}\right) = e_s^{(n)}$. □

Theorem III.13. *Let k be a field. Then there exists a unique algebra homomorphism*

$$\begin{aligned} \hat{\Phi}\colon k[X_1, \ldots, X_n]^{S_n} &\to k[X_1, \ldots, X_n]^{S_n} \\ e_j^{(n)} &\mapsto h_j^{(n)} \end{aligned}$$

for all $0 \leq j \leq n$. Moreover $\hat{\Phi}^2 = \mathrm{id}$ and so $\hat{\Phi}$ is an isomorphism.

Proof. By the Fundamental theorem of symmetric polynomials we have an isomorphism of algebras

$$\begin{aligned} \Phi\colon k[X_1, \ldots, X_n]^{S_n} &\to k[t_1, \ldots, t_n], \\ e_j^{(n)} &\mapsto t_j. \end{aligned}$$

By the universal property of the polynomial ring we have a unique algebra homomorphism

$$\begin{aligned} \overline{\Phi}\colon k[t_1, \ldots, t_n] &\to k[X_1, \ldots, X_n]^{S_n}, \\ t_j &\mapsto h_j^{(n)}. \end{aligned}$$

Now set $\hat{\Phi} := \overline{\Phi} \circ \Phi$. This is an algebra homomorphism.

We have to show that $\hat{\Phi}^2 = \mathrm{id}$. Since the $e_j^{(n)}$ generate $k[X_1,\dots,X_n]^{S_n}$ as an algebra, it is enough to show that $\hat{\Phi}\left(e_j^{(n)}\right) = h_j^{(n)}$ for all $0 \le j \le n$. By Corollary III.12 and construction of $\hat{\Phi}$ we get

$$\hat{\Phi}\left(h_j^{(n)}\right) = \hat{\Phi}\left(F_j\left(e_1^{(n)},\dots,e_n^{(n)}\right)\right) = F_j\left(\hat{\Phi}\left(e_1^{(n)}\right),\dots,\hat{\Phi}\left(e_n^{(n)}\right)\right) = F_j\left(h_1^{(n)},\dots,h_n^{(n)}\right) = e_j^{(n)}$$

for all $0 \le j \le n$. □

Theorem III.14. *Let k be a field with $\operatorname{char} k = 0$ or $\operatorname{char} k > n$. Then the $p_1^{(n)},\dots,p_n^{(n)}$ generate $k[X_1,\dots,X_n]^{S_n}$ as a k-algebra and they are algebraically independent over k.*

Proof. Left to the reader. □

Remark. Theorem III.14 does not hold over $\mathbb{Z}$. Consider $\mathbb{Q}[X_1,X_2]^{S_2}$. There we have $e_2^{(2)} = \frac{1}{2}\left(\left(p_1^{(2)}\right)^2 - p_2^{(2)}\right)$, as one has $(X_1+X_2)^2 - (X_1^2+X_2^2) = 2X_1X_2$. If the theorem holds for $k=\mathbb{Z}$ then there exists an $F \in \mathbb{Z}[t_1,t_2]$ such that $F\left(p_1^{(2)},p_2^{(2)}\right) = e_2^{(n)}$. Viewed as a polynomial in $\mathbb{Q}[t_1,t_2]$ we have $\frac{1}{2}t_1^2 - \frac{1}{2}t_2 - F(t_1,t_2) = G(t_1,t_2)$. It satisfies $G\left(p_1^{(2)},p_2^{(2)}\right) = 0$. This implies $G=0$ because $p_1^{(2)}$ and $p_2^{(2)}$ are algebraically independent over IQ. But this contradicts $F \in \mathbb{Z}[t_1,t_2]$.

We want to find a basis of $k[X_1,\dots,X_n]^{S_n}$. This is another natural occurence of power series.

Definition. Let $A = \bigoplus_{i\in\mathbb{Z}} A_i$ be a graded algebra. Assume $A_i = 0$ for $i<0$ (*non-negatively graded*) and $\dim A_i < \infty$ for all $i \in \mathbb{Z}$. Then define the *Hilbert series*

$$P_A(t) = \sum_{i\ge 0} (\dim A_i) t^i \in \mathbb{N}_0[\![t]\!]$$

(in particular, if $\dim A < \infty$, we have $P_A(t) \in \mathbb{N}_0[t]$).

Examples.

0) For k a field let $A = k[t]$ with standard grading $\bigoplus_{i\ge 0}\langle t^i\rangle$. Then we get

$$P_A(t) = 1 + t + t^2 + \ldots = \frac{1}{1-t}.$$

(Note that $P_A(t)$ is not defined for the "stupid" grading.)

1) If $A = \bigoplus_{i\in\mathbb{Z}}$ and $B = \bigoplus_{i\in\mathbb{Z}} B_i$ are non-negatively graded algebras with $\dim A < \infty > \dim B$ and $\dim A_i < \infty > \dim B_i$ for all $i \in \mathbb{Z}$. Then $A \otimes B$ is an algebra, even a graded ring via

$$A\otimes B = \bigoplus_{i\in\mathbb{Z}} (A\otimes B)_i \quad \text{where} \quad (A\otimes B)_i = \begin{cases} 0 & \text{if } i<0,\\ \bigoplus_{r=0}^{i} A_r \otimes B_{i-r} & \text{otherwise.}\end{cases}$$

It is clear that the $(A \otimes B)_i \subseteq A \otimes B$ are vetorspaces and $\bigoplus_{i\in\mathbb{Z}}(A \otimes B)_i = A \otimes B$ by choosing a homogeneous basis of A and B.

We have to check that $(A \otimes B)_i(A \otimes B)_j \subseteq (A \otimes B)_{i+j}$ for all $i, j \in \mathbb{Z}$. We can assume $i, j \geq 0$ and check the property on a basis. We have

$$\underbrace{(a \otimes b)}_{\in A_i \otimes B_{i-r} \subseteq (A\otimes B)_i} \overbrace{(c \otimes d)}^{\in A_s \otimes B_{j-2} \subseteq (A\otimes B)_j} = \underbrace{ac}_{\in A_i A_s \subseteq A_{i+s}} \otimes \overbrace{bd}^{\in B_{i-r}B_{j-s} \subseteq B_{i+j-r-s}},$$

and we get $ac \otimes bd \in A_{i+s} \otimes B_{i+j-(r+s)} \subseteq (A \otimes B)_{i+j}$. Thus, $A \otimes B$ is a non-negatively graded ring. We have $\dim(A \otimes B)_i = \sum_{r=0}^{i} \dim A_r \dim B_{i-r}$, which results in

$$P_{A\otimes B}(t) = P_A(t)P_B(t).$$

We now consider the special case $A = k[X_1, \ldots, X_n]$ with standard grading. There is an isomorphism of algebras

$$\begin{aligned} A \quad &\cong \quad k[t_1] \otimes k[t_2] \otimes \ldots \otimes k[t_n], \\ X_1^{a_1} X_2^{a_2} \cdots X_n^{a_n} \quad &\longleftarrow\!\shortmid \quad t_1^{a_1} \otimes t_2^{a_2} \otimes \ldots \otimes t_n^{a_n}. \end{aligned} \tag{*}$$

Thus $P_A(t) = P_{k[t_1]}(t) \cdots P_{k[t_n]}(t)$ with the standard grading on $k[t_i]$. (Note that (*) becomes a graded algebra isomorphism.) Hence

$$P_A(t) = (1 + t + t^2 + \ldots)(1 + t + t^2 + \ldots) \cdots (1 + t + t^2 + \ldots) = \prod_{i=1}^{n} \frac{1}{1 - t}.$$

Then

$$P_A(t) = \sum_{j\geq 0} \binom{n + j + 1}{n - 1} t^j$$

where the binomial coefficient counts all the ways o create t^j from the r factors. We want the number of tuples $(j_1, \ldots, j_n) \in \mathbb{Z}^n_{\geq 0}$ with $j_1 + \ldots + j_n = j$. We can think of this by choosing $n - 1$ points as "barriers" out of $n + j - 1$ points.

For $n = 1$, we have $\binom{n+j-1}{0} = 1$, see 0). For $n = 2$, $\binom{j+1}{j}$ is the number of monomials.

2) By the Fundamental theorem of symmetric polynomials we have an isomorphism of algebras

$$\Phi \colon k[X_1, \ldots, X_n] \cong k[t_1, \ldots, t_n],$$

but this is not an isomorphism of graded algebras if we choose the standard gradings on $k[X_1, \ldots, X_n]$ and $k[t_1, \ldots, t_n]$.

Define a grading on $k[t_1, \ldots, t_n]$ by $k[t_1, \ldots, t_n]_i := \Phi\Big(k[X_1, \ldots, X_n]^{S_n}\Big)$. Because Φ is an isomorphism of algebras (in particular of vector spaces) we have

$$A = k[t_1, \ldots, t_n] = \bigoplus_{i\geq 0} k[t_1, \ldots, t_n]_i.$$

We want to calculate $P_A(t)$ with this grading.

We have

$$k[t_1, \dots, t_n] \cong k[t_1] \otimes k[t_2] \otimes \dots \otimes k[t_n]$$

as algebras and as graded algebras by setting $t_i \in k[t_i]$ in degree i (since t_j corresponds to $e_j^{(n)}$ which has degree j). Therefore

$$P_A(t) = \underbrace{(1 + t + t^2 + \dots)}_{t_1 \text{ is of degree } 1} \underbrace{(1 + t^2 + t^4 + \dots)}_{t_2 \text{ is of degree } 2} \cdots \underbrace{(1 + t^n + t^{2n} + \dots)}_{t_n \text{ is of degree } n} = \prod_{j=1}^{n} \frac{1}{1 - t^j}.$$

We now focus on how to express the coefficient of t^j in $P_A(t)$ explicitly. The coefficient of t_j equals the number of tuples $(a_1, \dots, a_n) \in \mathbb{Z}_{\geq 0}^n$ satisfying $1a_1 + 2a_2 + \dots + na_n = j$.

For visualization, consider the following Young diagram consisting of j squares.

$$\begin{array}{|c|c|c|c|c|c|}
\hline
a_n & a_n & a_n & a_n & \cdots & a_n \\
\hline
a_n & a_n & a_n & a_n & \cdots & a_n \\
\hline
\vdots & \vdots & \vdots & & & \\
\hline
a_2 & a_2 & & & & \\
\hline
a_2 & a_2 & & & & \\
\hline
a_1 & & & & & \\
\hline
a_1 & & & & & \\
\hline
a_1 & & & & & \\
\hline
\end{array}$$

In this example, we have $a_1 = 3$, $a_2 = 2$ and $a_n = 2$.

Definition. For $d \in \mathbb{N}$ a sequence $\lambda = (\lambda_1 \geq \lambda_2 \geq \dots)$ with $\lambda_i \in \mathbb{Z}_{\geq 0}$ is a *partition* of d if $\sum_{i=1}^{\infty} \lambda_i = d$. We write $|\lambda| := \sum_{i=1}^{\infty}$ and let $l(\lambda)$ be maximal such that $\lambda_i \neq 0$ and call it the *length* of λ. We set

$$\mathrm{Par}(d) := \{\text{partitions of } d\} \quad \text{und} \quad \mathrm{Par} := \bigcup_{d \geq 0} \mathrm{Par}(d).$$

Definition. Define a partial ordering on Par by setting $\lambda \leq \mu$ for $\lambda, \mu \in \mathrm{Par}$ if we have

$$\sum_{i=1}^{r} \lambda_i \leq \sum_{i=1}^{r} \mu_i$$

for all $r \geq 0$.

Definition. For $\lambda \in \mathrm{Par}$ we define the following elements in $k[X_1, \dots, X_n]^{S_n}$.

$$\begin{aligned}
e_\lambda^{(n)} &:= e_{\lambda_1}^{(n)} e_{\lambda_2}^{(n)} \cdots && (\lambda_1 \leq n) \\
h_\lambda^{(n)} &:= h_{\lambda_1}^{(n)} h_{\lambda_2}^{(n)} \cdots \\
p_\lambda^{(n)} &:= p_{\lambda_1}^{(n)} p_{\lambda_2}^{(n)} \cdots \\
m_\lambda^{(n)} &:= \sum_{g \in S_n} X_{g(1)}^{\lambda_1} X_{g(2)}^{\lambda_2} \cdots X_{g(n)}^{\lambda_n} && (l(\lambda) \leq n)
\end{aligned}$$

They are all homogeneous of degree $|\lambda|$.

[October 22, 2018]

[October 25, 2018]

Definition. For $\lambda \in \mathrm{Par}$ let λ^t be the *transposed partition* given by $\lambda_i^t = |\{j \mid \lambda_j = i\}|$. In this case, the young diagram is “flipped”.

Theorem III.15. *The* $\left\{e_\lambda^{(n)}\right\}$ *and* $\left\{h_\lambda^{(n)}\right\}$ *for* $\lambda \in \mathrm{Par}$ *with* $\lambda_i \leq n$ *form a* k*-vector space of* $k[X_1, \ldots, X_n]^{S_n}$ *for* k *any field or* $k = \mathbb{Z}$*. Moreover* $\left\{m_\lambda^{(n)}\right\}$ *for* $\lambda \in \mathrm{Par}$ *with* $l(\lambda) \leq n$ *is also basis.*

Proof. By the Fundamental theorem of symmetric polynomials the monomials in the $e_j^{(n)}$'s are linearly independent, because the $e_j^{(n)}$'s are algebraically independent. Moreover, they generate as a vector space because the $e_j^{(n)}$'s generate as an algebra. Thus, the $\left\{e_\lambda^{(n)}\right\}$ with $\lambda \in \mathrm{Par}$ and $\lambda_i \leq n$ form a basis. Then the $\left\{h_\lambda^{(n)}\right\}$ form a basis by applying the transformation of Theorem III.13.

In $e_\lambda^{(n)} = e_{\lambda_1}^{(n)} e_{\lambda_2}^{(n)} \cdots e_{\lambda_{l(\lambda)}}^{(n)}$ the maximum possible degree of λ_2 is λ_2^t etc. In fact we have

$$e_\lambda^{(n)} = m_{\lambda^t}^{(n)} + \sum_{\mu \leq \lambda^t} m_{\mu_t}^{(n)}.$$

Therefore the $m_{\lambda^t}^{(n)}$ with $\lambda_i^t \leq n$ form a basis, since the $e_\lambda^{(n)}$ with $\lambda_i \leq n$ do. As one has $\{\lambda \in \mathrm{Par} \mid \lambda_i \leq n\} = \{\lambda \in \mathrm{Par} \mid l(\lambda^t) \leq n\}$ the $m_\lambda^{(n)}$ for $\lambda \in \mathrm{Par}$ with $l(\lambda) \leq n$ form a basis. □

III.3. Polynomial maps

In this section k is an infinite field, V a finite-dimensional k-vector space and $v_1, \ldots, v_n$ a basis of V.

Definition. We set $\mathcal{P}_k(V) = \{f \colon V \to k \mid f \text{ polynomial}\}$ where f is *polynomial* if

$$f\left(\sum_{i=1}^n \alpha_i v_i\right) = p(\alpha_1, \ldots, \alpha_n)$$

for some polynomial $p \in k[t_1, \ldots, t_n]$.

Remark.

- Clearly $\mathcal{P}_k(V)$ is a k-vector space with pointwise addition and scalar multiplication.
- The property “polynomial” does not depend on the choice of a basis.

Proof. Let $w_1, \dots, w_n$ be a basis of V and $w_j = \sum_{i=1}^n \beta_{ij} v_i$. Then we get

$$\begin{aligned} f\left(\sum_{j=1}^n \alpha_j w_j\right) &= f\left(\sum_{j=1}^n \alpha_j \sum_{i=1}^n \beta_{ij} v_i\right) = f\left(\sum_{i=1}^n \sum_{j=1}^n \alpha_j \beta_{ij} v_i\right) \\ &= p\left(\sum_{j=1}^n \alpha_j \beta_{1j}, \dots, \sum_{j=1}^n \alpha_j \beta_{nj}\right) \end{aligned}$$

for some $p \in k[t_1, \dots, t_n]$ as f is polynomial. But the last expression depends polynomial on $\alpha_1, \dots, \alpha_n$; it equals $p'(\alpha_1, \dots, \alpha_n)$ for some polynomial p'. $\square$

Lemma III.16. *Let $W \subseteq V$ be a vector subspace. If $f \in \mathcal{P}_k(V)$ we get $f|_W \in \mathcal{P}_k(W)$.*

Proof. We choose a basis $w_1, \dots, w_m$ of W and extend it to a basis $w_1, \dots, w_n$ of V. Now $f(\sum_{i=1}^m \alpha_1 w_1) = p(\alpha_1, \dots, \alpha_m, 0, \dots, 0)$ for some $p \in k[X_1, \dots, X_n]$ as $f \in \mathcal{P}_k(V)$. Consider the image $\tilde{p}$ of p under the canonical map

$$k[X_1, \dots, X_n] \to {}^{k[X_1,\dots,X_n]}/_{(X_{m+1},\dots,X_n)} \cong k[X_1, \dots, X_m].$$

Then by construction $f(\sum_{i=1}^m \alpha_i w_i) = \tilde{p}(\alpha_1, \dots, \alpha_m)$ with $\tilde{p} \in k[X_1, \dots, X_m]$. $\square$

Definition. For $f, g \in \mathcal{P}_k(V)$ define fg as $(fg)(v) = f(v)g(v)$ for all $v \in V$. This turns $\mathcal{P}_k(V)$ into a k-algebra.

Theorem III.17. *There is an isomorphism of k-algebras*

$$\begin{aligned} k[X_1, \dots, X_n] &\to \mathcal{P}_k(V), \\ p &\mapsto f_p = \left(\sum_{i=1}^n \alpha_i v_i \mapsto p(\alpha_1, \dots, \alpha_n)\right). \end{aligned}$$

Proof. Define for $1 \le j \le n$ the j-th *coordinate function* $\varphi_j \colon V \to k$ by $\varphi_j(\sum_{i=1}^n \alpha_i v_i) = \alpha_j$. Obviously we have $\varphi_j \in \mathcal{P}_k(V)$. By the universal property of the polynomial algebra $k[X_1, \dots, X_n]$ there exists a unique algebra homomorphism

$$\begin{aligned} \beta \colon k[X_1, \dots, X_n] &\to \mathcal{P}_k(V), \\ X_j &\mapsto \varphi_j. \end{aligned}$$

Then $\beta(X_1^{a_1} \cdots X_n^{a_n})(v) = (\varphi_1^{a_1} \cdots \varphi_n^{a_n})(v)$. By the definition of multiplication $\mathcal{P}_k(V)$ one gets $(\varphi_1^{a_1} \cdots \varphi_n^{a_n})(\sum_{i=1}^n \alpha_i v_i) = \alpha_1^{a_1} \cdots \alpha_n^{a_n}$. Thus β sends p to f_p.

By definition β is surjective. Now assume $\beta(p) = 0$. Then $f_p(\sum_{i=1}^n \alpha_i v_i) = 0$ for all $(\alpha_1, \dots, \alpha_n) \in k^n$, hence $p(\alpha_1, \dots, \alpha_n) = 0$ for all $(\alpha_1, \dots, \alpha_n) \in k^n$. As k is infinite we get $p = 0$. Therefore β is an isomorphism. $\square$

Remark. The theorem does not hold for finite fields in general. For example, take $p(t) = t^2 + t \in \mathbb{F}_2[t]$. In this case we have $p(1) = 1 + 1 = 0 = 0 + 0 = p(0)$, so $p(\lambda) = 0$ for all $\lambda \in \mathbb{F}_2$, but $p \neq 0$. Therefore the β in the proof does not have to be injective.

Remark III.18. At this point Professor Stroppel seems to have skipped a number in her notes.

Definition. $f \in \mathcal{P}_k(V)$ is *homogeneous* of degree d if $f(\lambda v) = \lambda^d f(v)$ for all $\lambda \in k$ and $v \in V$.

Proposition III.19. *We have*

$$\mathcal{P}_k(v) = \bigoplus_{d \geq 0} \mathcal{P}_k(V)_d \quad \textit{where} \quad \mathcal{P}_k(V)_d = \{f \in \mathcal{P}_k \mid f \textit{ is homogeneous of degree } d\}$$

and $\mathcal{P}_k(V)$ becomes a non-negatively graded algebra.

Proof. Clearly $\mathcal{P}_k(V)_d \cap \mathcal{P}_k(V)_{d'} = 0$ if $d \neq d'$, as otherwise we have $\lambda^d f(v) = f(\lambda v) = \lambda^{d'} f(v)$, or $\lambda^d - \lambda^{d'} = 0$ for all $\lambda \in k$ and $v \in V$. But $t^d - t^{d'}$ only has finitely many roots which contradicts the infinity of k. We get $\bigoplus_{d \geq 0} \mathcal{P}_k(V)_d \subseteq \mathcal{P}_k(V)$ via the isomorphism β from Theorem III.17 which maps a monomial $p = X_1^{a_1} \cdots X_n^{a_n} \in k[X_1, \ldots, X_n]$ to f_p with $f_p(\sum_{i=1}^n \lambda_i v_i) = p(\lambda_1, \lambda_n)$. Then $f_p(\lambda v) = p(\lambda\lambda_1, \ldots, \lambda\lambda_n) = \lambda^{a_1 + \ldots + a_n} p(\lambda_1, \ldots, \lambda_n)$. Hence f_p is homogeneous of degree $d = a_1 + \cdots + a_n$. Hence

$$\begin{aligned} \beta(k[X_1, \ldots, X_n]) = \beta\left(\bigoplus_{d \geq 0} k[X_1, \ldots, X_n]_d\right) &= \bigoplus_{d \geq 0} \beta(k[X_1, \ldots, X_n]_d) \\ &\subseteq \bigoplus_{d \geq 0} \mathcal{P}_k(V)_d \subseteq \mathcal{P}(V). \end{aligned}$$

But Theorem III.17 gives that $\operatorname{im} \beta = \mathcal{P}_k(V)$, hence $\bigoplus_{d \geq 0} \mathcal{P}_k(V)_d = \mathcal{P}_k(v)$. Altogether β is an isomorphism of graded algebras. $\square$

Definition. Let W be a k-vector space. $f \colon W \to V$ is *polynomial* if the functions $f_i \colon W \to k$ defined by

$$f(w) = \sum_{i=1}^n f_i(w) v_i$$

are polynomial. Denote $\mathcal{P}_k(W, V) := \{f \colon W \to V \mid f \text{ polynomial}\}$.

Remark. The property is independent of the choice of a basis. Let $w_1, \ldots, w_n$ be a basis of V and $w_i = \sum_{j=1}^n \alpha_{ij} v_j$. Then we have for $w \in W$

$$f(w) = \sum_{i=1}^n f_i(w) w_i = \sum_{i=1}^n \sum_{j=1}^n f_i(w) \alpha_{ji} v_j.$$

If f is polynomial in the w_i then it is also polynomial in the v_i.

Remark. Consider the special case $V = k$. Then $f\colon W \to V = k$ is polynomial iff $f \in \mathcal{P}_k(W)$.

Lemma III.20. *Finite dimensional maps together with polynomial maps form a category.*

Proof. Left to the reader. □

Lemma III.21. *$\mathcal{P}_k(W,V)$ for W a finite-dimensional k-vector space is a $\mathcal{P}_k(W)$-module via*

$$(f.g)(w) = f(w)g(w)$$

for all $w \in W$ for $f \in \mathcal{P}_k(W)$ and $g \in \mathcal{P}_k(W,V)$.

Proof. Clearly $\mathrm{Maps}(W,V)$ is a $\mathrm{Maps}(W,k)$-module via the same rule. We have to check that $\mathcal{P}_k(W,V)$ is preserved under the action of $\mathcal{P}_k(W) \subseteq \mathrm{Maps}(W,k)$. So let $f \in \mathcal{P}_k(W)$ and $g \in \mathcal{P}_k(W,V)$ and let $w_1,\dots,w_m$ be a basis of W. Then

$$\begin{aligned}(fg)\left(\sum_{i=1}^m \lambda_i w_i\right) &= f\left(\sum_{i=1}^m \lambda_i w_i\right)g\left(\sum_{i=1}^m \lambda_i w_i\right) = \sum_{j=1}^m p(\lambda_1,\dots,\lambda_m)g_j\left(\sum_{i=1}^m \lambda_i w_i\right)v_j \\ &= \sum_{j=1}^m \underbrace{p(\lambda_1,\dots,\lambda_m)q_j(\lambda_1,\dots,\lambda_m)}_{=:(fg)_j\left(\sum_{i=1}^m \lambda_i w_i\right)} v_j = \sum_{j=1}^m (fg)_j\left(\sum_{i=1}^m \lambda_i w_i\right)v_j\end{aligned}$$

for some $p, q_1,\dots,q_m \in k[X_1,\dots,X_m]$ as f and the g_j are polynomial. As the $(fg)_j$ are polynomial in $\lambda_1,\dots,\lambda_n$ we are done. □

Proposition III.22. *For $f \in \mathcal{P}_k(W,V)$ define $f^*\colon \mathcal{P}_k(V) \to \mathcal{P}_k(W)$ by $f^*(h) = h \circ f$, the* comorphism attached to f*. f^* is an algebra homomorphism.*

Proof. For $f \in \mathcal{P}_k(W,V)$ and $h \in \mathcal{P}_k(V)$ we have $h \circ f \in \mathcal{P}_k(W)$ by Lemma III.20. For $h_1, h_2, h \in \mathcal{P}_k(V)$, $\lambda \in k$ and $w \in W$ we get

$$\begin{aligned}(f^*(h_1+h_2))(w) &= (h_1+h_2)(f(w)) = h_1(f(w)) + h_2(f(w)) \\ &= (f^*(h_1))(w) + (f^*(h_2))(w) = (f^*(h_1)+f^*(h_2))(w)\end{aligned}$$

and

$$(f^*(\lambda h))(w) = (\lambda h)(f(w)) = \lambda h(f(w)) = \lambda(f^*(h))(w) = ((\lambda f^*)(h))(w).$$

Thus f^* is linear. One easily checks that $f^*(h_1h_2) = f^*(h_1)f^*(h_2)$. Altogether f^* is an algebra homomorphism. □

[October 25, 2018]

[October 29, 2018]

Proposition III.23. *There is a (contravariant) functor*

$$\begin{array}{rcl} F\colon \mathrm{Pol}_k := \left\{\substack{\textit{finite-dimensional } k\textit{-vector spaces}\\ \textit{with polynomial maps}}\right\} & \to & \left\{\substack{k\textit{-algebras with}\\ \textit{algebra homomorphisms}}\right\}^{\mathrm{op}} := \mathrm{Alg}_k^{\mathrm{op}}, \\ W & \mapsto & \mathcal{P}_k(W), \\ f \in \mathcal{P}_k(W,V) & \mapsto & f^*\colon \mathcal{P}_k(V) \to \mathcal{P}_k(W). \end{array}$$

Proof. We know that $\mathcal{P}_k(W)$ is a k-algebra and f^* an algebra homomorphism by Proposition III.22. By definition we have $\mathrm{id}_W \mapsto \mathrm{id}_W^* = \mathrm{id}_{\mathcal{P}_k(W)}$. Finally we get for $f_1 \in \mathcal{P}_k(W,V)$, $f2 \in \mathcal{P}_k(Z,W)$ and $h \in \mathcal{P}_k(V)$

$$(f_1 \circ f_2)^*(h) = (f_2^* \circ f_1^*)(h) = (h \circ f_1) \circ f_2 = h \circ (f_1 \circ f_2) = (f_1 \circ f_2)^*(h). \qquad \square$$

Theorem III.24. *The functor F from Proposition III.23 is fully faithful, i.e. the map*

$$\begin{array}{rcl} \Omega\colon \mathcal{P}_k(W,V) & \to & \mathrm{Hom}_{\mathrm{Alg}_k}(\mathcal{P}_k(V), \mathcal{P}_k(W)) \\ f & \mapsto & f^* \end{array}$$

is an isomorphism of k-vector spaces for all finite-dimensional k-vector spaces V and W.

Proof. Clearly Ω is lineary. We have to show that it is invertible.

Let $v_1, \dots, v_n$ be a basis of V and consider the isomorphism of algebras

$$\begin{array}{rcl} \beta\colon k[X_1, \dots, X_n] & \to & \mathcal{P}_k(V) \\ x_j & \mapsto & \varphi_j. \end{array}$$

By the universal property of the polynomial algebra we have

$$\begin{array}{rcl} \Psi\colon \mathcal{P}_k(W)^{\oplus n} & \to & \mathrm{Hom}_{\mathrm{Alg}_k}(k[X_1, \dots, X_n], \mathcal{P}_k(w)) \\ (f_1, \dots, f_n) & \mapsto & \Psi(f) := (X_j \mapsto f_j). \end{array}$$

On the other hand we have

$$\begin{array}{rcl} \Phi\colon \mathcal{P}_k(W)^{\oplus n} & \to & \mathcal{P}_k(W,V) \\ (f_1, \dots, f_n) & \mapsto & f := w \mapsto \sum_{i=1}^n f_i(w) w_i \\ (f_1, \dots, f_n) & \leftarrow\!\shortmid & f = w \mapsto \sum_{i=1}^n f_i(w) w_i. \end{array}$$

As these maps are inverse Φ is a bijection. Again let $f \in \P_k(W,V)$, $w \in W$ and $f(w) = \sum_{i=1}^n f_i(w) w_i$. Then $f^*(\varphi_j)(w) = (\varphi_j \circ f)(w) = \varphi_j(f(w)) = f_i(w)$, or $f^*(\varphi_j) = f_j$ for alle $1 \leq j \leq n$. Therefore by definition

$$\Omega(\Psi(f_1, \dots, f_n)) = \Omega(f) = f^* = \Psi(f_1, \dots, f_n) \circ \beta^{-1}$$

because $f^*(\varphi_j) = \Psi(f_1, \dots, f_n)(\beta^{-1}(\varphi_j)$ for all $1 \leq j \leq n$ (and f^* is an algebra homomorphism, hence defined by the $f^*(\varphi_j)$).

Now Ψ is invertible, and so is $\Omega \circ \Phi$ and finally Ω. $\square$

III.4. Covariants

Let k be a field of infinite cardinality.

Remark. Let $\pi\colon W \to V$ be a linear map of finite-dimensional k-vector spaces. Then $\pi \in \mathcal{P}_k(W,V)$ is homogeneous of degree 1. To see this choose bases $v_1,\dots,v_n$ and $w_1,\dots,w_m$ of V and W, respectively. Now we get

$$\pi\left(\sum_{j=1}^m \lambda_j w_j\right) = \sum_{j=1}^m \lambda_j \underbrace{\pi(w_j)}_{\sum_{i=1}^n \beta_{ij} v_i} = \sum_{i=1}^n \underbrace{\left(\sum_{j=1}^m \beta_{ij}\lambda_j\right)}_{\text{polynomial in } \lambda_1,\dots,\lambda_m} v_i.$$

Let G be a group and V a finite-dimensional representation of G. Then $\mathcal{P}_k(V)$ is a representation of G via

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

for all $g \in G$, $f \in \mathcal{P}_k(V)$ and $v \in V$. We have to show that $g.f$ is again in $\mathcal{P}_k(V)$ (the rest is clear, since V is a representation). Now $g.f = f \circ \pi_{g^{-1}}$ is a composition of polynomial maps and therefore by Lemma III.20 polynomial.

Definition. Let G be a group and V, W finite-dimensional representations of G (over k). A map $f\colon W \to V$ is *covariant* if it is polynomial and G-equivariant. Denote $\mathrm{Cov}_k(W,V) = \mathrm{Cov}(W,V) := \{f\colon W \to V \mid f \text{ covariant}\}$.

0) If $f \in \mathrm{Hom}_G(W,V)$ we have $f \in \mathrm{Cov}(W,V)$.

1) Let V be a finite-dimensional representation of G. Then $f\colon V \to V^{\otimes d}$ given by $f(x) = x^{\otimes d}$ is covariant and homogeneous of degree d because

$$f\left(\sum_{i=1}^n \lambda_i w_i\right) = \left(\sum_{i=1}^n \lambda_i w_i\right)^{\otimes d} = \sum_{\substack{I=(i_1,\dots,i_d)\\ \in\{1,\dots,n\}^d}} \underbrace{\prod_{i\in I} \lambda_i}_{\lambda_I} \underbrace{\bigotimes_{i\in I} v_i}_{v_I}.$$

   Note that $\left\{v_i \,\middle|\, I \in \{1,\dots,n\}^d\right\}$ forms a basis of $V^{\otimes d}$. Definite $p_I \in k[t_1,\dots,t_n]$ by $p_I(t_1,\dots,t_n) = t_1^{a_1}\cdots t_d^{a_d}$ where $a_k = |\{j \mid i_j = h\}|$. Then $p_I(\lambda_1,\dots,\lambda_n) = \lambda_I$ and f is polynomial. f is G-equivariant since $f(g.v) = (g.v)^{\otimes d} = g.v^{\otimes d}$. Thus f is covariant.

2) Let $V = \mathrm{M}_{n\times n}(k)$ and $G = \mathrm{GL}_n(k)$ act on V by conjugation. Then

$$\begin{aligned} f_m\colon V &\to V \\ A &\mapsto A^m \end{aligned}$$

   is covariant for all $m \geq 1$.

Lemma III.25. *Let V, W be finite-dimensional representations of a group G. Then $f\colon W \to V$ is covariant if and only if $f^*\colon \mathcal{P}_k(V) \to \mathcal{P}_k(W)$ is G-invariant.*

Note: The action of G on $\mathrm{Hom}_{\mathrm{Alg}_k}(\mathcal{P}_k(V), \mathcal{P}_k(W))$ is given by $(g.h)(\varphi) = g.(h(g^{-1}.\varphi))$ for all $g \in G$, $h \in \mathrm{Hom}_{\mathrm{Alg}_k}(\mathcal{P}_k(V), \mathcal{P}_k(W))$ and $\varphi \in \mathcal{P}_k(v)$.

Proof. Left to the reader. □

Proposition III.26. *Let V, W be finite-dimensional representations of a group G and $f \in \mathrm{Cov}_k(W, V)$. Then*

$$f^*\Big(\mathcal{P}_k(V)^G\Big) \subseteq \mathcal{P}_k(W)^G.$$

Proof. Let $h \in \mathcal{P}_k(V)^G$ and $g \in G$. For all $w \in W$ we have

$$\begin{aligned}(g.f^*(h))(w) &= (g.(h \circ f))(w) = (h \circ f)(g^{-1}.w) = h(f(g^{-1}.w)) = h(g^{-1}.f(w)) \\ &= (g.h)(f(w)) = h(f(w)) = (f^*(h))(w).\end{aligned}$$

□

Proposition III.27. *Let V, W be finite-dimensional k-vector spaces. The $\mathcal{P}_k(W)$-module structure on $\mathcal{P}_k(W, V)$ induces a $\mathcal{P}_k(W)^G$-module structure on $\mathrm{Cov}(W, V)$ if V, W are representations of G by restriction.*

Proof. $\mathcal{P}_k(W)^G$ is a subring of $\mathcal{P}_k(W)$, and by Lemma I.8 even a subalgebra. Let $f \in \mathrm{Cov}(W, V)$, $h \in \mathcal{P}_k(W)^G$, $g \in G$ and $w \in W$. Then we have

$$\begin{aligned}(h.f)(g.w) &= h(g.w)f(g.w) = h(w)f(g.w) = h(w)(g.f(w)) = g.(h(w)f(v)) \\ &= g.(h.f)(w),\end{aligned}$$

and hence $h.f$ is G-equivariant. □

IV. Invariants of matrix actions

Let k be a field of infinite cardinality.

Theorem IV.1 (Invariant Theorem I)**.** *Let $G = \mathrm{SL}_n(k)$ act on $\mathrm{M}_{n\times n}(k)$ by left multiplication. Then*

$$\det\colon \mathrm{M}_{n\times n}(k) \to k$$

generates $\mathcal{P}_k(\mathrm{M}_{n\times n}(k))^G$ as a k-algebra and it is algebraically independent, i.e.

$$\begin{array}{rcl} k[t] & \to & \mathcal{P}_k(\mathrm{M}_{n\times n}(k))^G \\ t & \mapsto & \det \end{array}$$

is an isomorphism of k-algebras.

Proof. Obviously, det is polynomial. It is also G-invariant, as we have $(S.\det)(A) = \det(S^{-1}A) = \det A$ for all $S \in G$ and $A \in \mathrm{M}_{n\times n}(k)$.

We have to prove that det is algebraically independent. Let $p \in k[t]$ with $p(\det) = 0$. We get $(p(\det))(A) = p(\det(A)) = 0$ for all $A \in \mathrm{M}_{n\times n}(k)$. Thus, $p(\lambda) = 0$ for all $\lambda \in k$ because det is surjective. But this implies $p = 0$ as k is of infinite cardinality.

It is left to show that det generates $\mathcal{P}_k(\mathrm{M}_{n\times n}(k))^G$ as an algebra. Let $f \in \mathcal{P}_k(\mathrm{M}_{n\times n}(k))^G$. Since f is polynomial there exists a $p \in k[t_{11},\dots,t_{nn}]$ such that $f(A) = p(a_{11},\dots,a_{nn})$ for all $A = \sum_{1\le i,j\le n} a_{ij}E_{ij}$ using a basis E_{ij} $(1 \le i,j \le n)$.

Consider the algebra homomorphism

$$\begin{aligned}\Psi\colon k[X_{11},\dots,X_{nn}] &\to k[t]\\ X_{ij} &\mapsto \begin{cases}0 & \text{if } i \neq j\\ 1 & \text{if } i = j \neq 1\\ t & \text{if } i = j = 1.\end{cases}\end{aligned}$$

Set $\overline{p} = \Psi(p)$. Then $\overline{p}(\lambda) = p(\mathrm{diag}(\lambda,1,\dots,1))$ for $\lambda \in k$. Consider $A \in \mathrm{GL}_n(k)$, $B = \mathrm{diag}(\det A, 1,\dots,1)$ and $S := AB^{-1} \in G$. Then

$$f(A) = f(SB) = f(B) = \overline{p}(\det A) = (\overline{p}(\det))(A).$$

Therefore $f = \overline{p}(\det) = 0$ when restricted to $\mathrm{GL}_n(k)$.

We now claim the *Zariski property I*: If $h \in \mathcal{P}_k(\mathrm{M}_{n\times n}(k))$ such that $h|_{\mathrm{GL}_n(k)} = 0$ then $h = 0$. We will prove this in Corollary IV.8.

As a consequence $f = \overline{p}(\det)$ as elements in $\mathcal{P}_k(\mathrm{M}_{n\times n}(k))^G$. Hence f is contained in the subalgebra generated by det, and $\mathcal{P}_k(\mathrm{M}_{n\times n}(k))^G$ is generated as an algebra by det. $\square$

Let $\chi_A(t) = \det(tI_n - A)$ denote the characteristic polynomial of $A \in \mathrm{M}_{n\times n}(k)$. We can expand this to

$$\chi_A(t) = t^n - s_1(A)t^{n-1} + s_2(A)t^{n-2} - \ldots + (-1^n)s_n(A)$$

with $s_i \in \mathcal{P}_k(\mathrm{M}_{n\times n}(k))$ for all $1 \le i \le n$. For $A = \mathrm{diag}(d_1,\dots,d_n)$ we have $s_i(A) = e_i^{(n)}(d_1,\dots,d_n)$.

[October 29, 2018]

[November 5, 2018]

Theorem IV.2 (Invariant Theorem II). *Let $G = \mathrm{GL}_n(k)$ act on $\mathrm{M}_{n\times n}(k)$ by conjugation $S.A = SAS^{-1}$ for $S \in \mathrm{GL}_n(k)$ and $A \in \mathrm{M}_{n\times n}(k)$. Then $\mathcal{P}_k(\mathrm{M}_{n\times n}(k))^G$ is generated as a k-algebra by $s_1,\dots,s_n$. Moreover these elements are algebraically independent over k, i.e.*

$$\begin{aligned}\mathcal{P}_k(\mathrm{M}_{n\times n}(k))^G &\to k[t_1,\dots,t_n]\\ s_i &\mapsto t_i\end{aligned}$$

is an isomorphism of k-algebras.

Proof. Obviously, $s_i \in \mathcal{P}_k(\mathrm{M}_{n\times n}(k))$. They are G-invariant because $\chi_A(t)$ is invariant under conjugation. Thus $s_i \in \mathcal{P}_k(\mathrm{M}_{n\times n}(k))^G$ for all $1 \le i \le n$.

Now let us show that the s_i are algebraically independent. Take $p \in k[t_1, \dots, t_n]$ such that $p(s_1, \dots, s_n) = 0$. Then $p(s_1, \dots, s_n)(A) = 0$ for all $A \in \mathcal{P}_k(\mathrm{M}_{n\times n}(k))$, so also for all diagonal matrices $\mathrm{diag}(d_1, \dots, d_n)$. Using our observation from above we get $p\left(e_1^{(n)}, \dots, e_n^{(n)}\right)(d_1, \dots, d_n) = 0$ for all $d_i \in k$. Thus $p\left(e_1^{(n)}, \dots, e_n^{(n)}\right) = 0$. By the Fundamental theorem of symmetric polynomials we get $p = 0$ as the $e_i^{(n)}$ are algebraically independent.

We still need to prove that the s_i generate $\mathcal{P}_k(\mathrm{M}_{n\times n}(k))^G$ as an algebra. Take $f \in \mathcal{P}_k(\mathrm{M}_{n\times n}(k))^G$. Since it is polynomial, there exists a $p \in k[t_{11}, \dots, t_{nn}]$ such that $f(A) = p(a_{11}, \dots, a_{nn})$ for $A = (a_{ij})$. Define the algebra homomorphism

$$\begin{aligned} \Phi\colon k[t_{11}, \dots, t_{nn}] &\to k[t_1, \dots, t_n] \\ t_{ij} &\mapsto \begin{cases} t_i & \text{if } i = j \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

and $\overline{p} := \Phi(p)$. Hence $f(\mathrm{diag}(d_1, \dots, d_n)) = \overline{p}(d_1, \dots, d_n)$ by definition.

Now we want to show that $\overline{p}$ is symmetric, i.e. $\overline{p} \in k[t_1, \dots, t_n]^{S_n}$. We already have an isomorphism of algebras

$$\begin{aligned} \beta\colon k[t_1, \dots, t_n] &\to \mathcal{P}_k(k^n) \\ t_i &\mapsto \varphi_i \text{ (coordinate function)} \end{aligned}$$

in standard basis. Now β is S_n-equivariant if we let S_n act on k^n by permuting the standard basis vectors e_i. It is enough to show that $\beta(\overline{p})$ is S_n invariant. Realise $g \in S_n$ as a permutation matrix A_g such that $A_g E_i = E_{g(i)}$. For $D = \mathrm{diag}(d_1, \dots, d_n)$ we have $A_g D A_{g^{-1}} = \mathrm{diag}\left(d_{g^{-1}(1)}, \dots, d_{g^{-1}(n)}\right)$. We gets

$$\begin{aligned} (g.\beta(\overline{p}))(d_1, \dots, d_n) &= \beta(\overline{p})\left(g^{-1}.(d_1, \dots, d_n)\right) = \beta(\overline{p})\left(d_{g^{-1}(1)}, \dots, d_{g^{-1}(n)}\right) \\ &= f\left(\mathrm{diag}\left(d_{g^{-1}(1)}, \dots, d_{g^{-1}(n)}\right)\right) = f(A_{g^{-1}} D A_g) \\ &= f\left(A_{g_{-1}} D (A_{g^{-1}})^{-1}\right) = f(D) \end{aligned}$$

for all $g \in S_n$ as f is G-invariant. Thus $\overline{p}$ is a symmetric polynomial.

By the Fundamental theorem of symmetric polynomials we have a $q \in k[t_1, \dots, t_n]$ with $\overline{p} = q\left(e_1^{(n)}, \dots, e_n^{(n)}\right)$. For $D = \mathrm{diag}(d_1, \dots, d_n)$ we have

$$f(D) = q\left(e_1^{(n)}, \dots, e_n^{(n)}\right)(d_1, \dots, d_n) = q(s_1, \dots, s_n)(D).$$

Therefore $f - q(s_1, \dots, s_n) = 0$ whe restricted to diagonal matrices.

We now claim the *Zariski property II*: If $h \in \mathcal{P}_k(\mathrm{M}_{n\times n}(k))^G$ such that $h|_{\substack{\text{diagonal}\\\text{matrices}}} = 0$ then $h = 0$. We will prove this later (see Lemma IV.11).

As a consequence $f - q(s_1, \dots, s_n) = 0$ (on all matrices in $\mathrm{M}_{n\times n}(k)$). It follows that $s_1, \dots, s_n$ generate $\mathcal{P}_k(\mathrm{M}_{n\times n}(k))^G$. $\square$

Another family of elements in $\mathcal{P}_k(\mathrm{M}_{n\times n}(k))^{\mathrm{GL}_n(k)}$ (under conjugation action) are the *power traces*

$$\begin{aligned} \mathrm{Tr}_j\colon \mathrm{M}_{n\times n}(k) &\to k \\ A &\mapsto \mathrm{Tr}(A^j). \end{aligned}$$

Obviously $\mathrm{Tr}_j \in \mathcal{P}_k(\mathrm{M}_{n\times n}(k))$. They are $\mathrm{GL}_n(k)$-invariant as we have

$$(S.\,\mathrm{Tr}_j)(A) = \mathrm{Tr}_j(S^{-1}AS) = \mathrm{Tr}(S^{-1}A^jS) = \mathrm{Tr}(A^j) = \mathrm{Tr}_j(A)$$

for all $S \in \mathrm{GL}_n(k)$ and $A \in \mathrm{M}_{n\times n}(k)$.

Theorem IV.3. *Let $n \geq 1$ and k an infinite field with $\operatorname{char} k = 0$ or $\operatorname{char} k > n$. Then $\mathrm{Tr}_1, \ldots, \mathrm{Tr}_n$ generate $\mathcal{P}_k(\mathrm{M}_{n\times n}(k))^{GL_n(k)}$ as a k-algebra and are algebraically independent. Hence*

$$\begin{aligned} k[t_1, \ldots, t_n] &\to \mathcal{P}_k(\mathrm{M}_{n\times n}(k))^{\mathrm{GL}_n(k)} \\ t_j &\mapsto \mathrm{Tr}_j \end{aligned}$$

defines an isomorphism of k-algebras.

Proof. Let $D = \operatorname{diag}(d_1, \ldots, d_n)$ be a diagonal matrix. Then

$$\mathrm{Tr}_j(D) = \mathrm{Tr}(D^j) = \sum_{i=1}^n d_1^j = p_j^{(n)}(d_1, \ldots, d_n).$$

By Theorem III.14 the $p_i^{(n)}$ generate $k[X_1, \ldots, X_n]^{S_n}$ as a k-algebra (under the given assumptions in k) and they are algebraically independent. Now argue as in the proof of the Invariant Theorem II with $e_j^{(n)}$ replaced by $p_j^{(n)}$. □

Definition. Let W be a finite-dimensional k-vector space (k infinite field). $X \subseteq W$ is *Zariski-dense* (over k) if $f|_X = 0$ implies $f = 0$ for all $f \in \mathcal{P}_k(W)$. Let $X \subseteq Y \subseteq W$. Then X is *Zariski-dense in Y* (over k) if $f|_X = 0$ implies $f|_Y = 0$ for all $f \in \mathcal{P}_k(W)$.

Examples.

0) An infinite subset $X \subseteq k$ is Zariski-dense.

1) Let $U \subsetneq W$ be a vector subspace. Then U is not Zariski-dense in W.

   Proof. Let $w_1, \ldots, w_u$ be a basis of U. Extend it to a basis $w_1, \ldots, w_n$ of W. Consider the map

$$\begin{aligned} \pi\colon W &\to k \\ \sum_{i=1}^n \lambda_i w_i &\mapsto \lambda_n w_n. \end{aligned}$$

   Obviously $\pi \in \mathcal{P}_k(W)$. Now note that $\pi|_U = 0$, but $\pi \neq 0$. □

Remark. Zariski density depends on k, e.g. $\mathbb{R} \subseteq \mathbb{C}$ is not dense over $\mathbb{R}$ but it is over $\mathbb{C}$.

Lemma IV.4. *Let k be an infinite field and $k \subseteq L$ a field extension as well as W a finite-dimensional k-vector space. Let $W_L := L \otimes_k W$.*

1) *$k^n \subseteq L^n$ is Zariski-dense over L for all $n \geq 1$.*

2) *$W \subseteq W_L$ (by $w \mapsto 1 \otimes w$) is also Zariski-dense over L.*

Proof. Left to the reader. □

Lemma IV.5. *Let k be an infinite field and $k \subseteq L$ a field extension as well as W a finite-dimensional k-vector space. Let $W_L := L \otimes_k W$. Then there exists a unique algebra homomorphism* $\mathrm{incl}\colon \mathcal{P}_k(W) \to \mathcal{P}_L(W_L)$ *such that the diagram*

$$\begin{tikzcd} W \arrow[r, "\mathrm{can}", "w\mapsto 1\otimes w"'] \arrow[d, "f"'] & W_L \arrow[d, "\mathrm{incl}(f)"] \\ k \arrow[r, hook] & L \end{tikzcd}$$

commutes for all $f \in \mathcal{P}_k(W)$. Moreover $\mathrm{incl}(f)$ *is surjective.*

Proof. Let $w_1, \ldots, w_n$ be a basis of W. Let $\varphi_1, \ldots, \varphi_n$ be the coordinate functions in $\mathcal{P}_k(W)$. Then $1 \otimes w_1, \ldots, 1 \otimes w_n$ is a basis of W_L. Let $\psi_1, \ldots, \psi_n$ be the corresponding coordinate functions in $\mathcal{P}_L(W_L)$. Define $\mathrm{incl}(\varphi_i) = \psi_j$. This results in a unique k-algebra homomorphism since the $\psi_1, \ldots, \psi_n$ are algebraically independent over L. The map is injective as the basis $\varphi_i^a = \varphi_i^{a_1} \cdots \varphi_i^{a_n}$ with $a = (a_1, \ldots, a_n) \in \mathbb{Z}^n_{\geq 0}$ is mapped to linearly independent elements.

Now we show that the above diagram commutes. For $f \in \mathcal{P}_k(W)$ we write $f = p(\varphi_1, \ldots, \varphi_n)$ for some polynomial $p \in k[t_1, \ldots, t_n]$. Then

$$(\mathrm{incl}(f) \circ \mathrm{can})\left(\sum_{i=1}^n \lambda_i w_i\right) = p(\psi_1, \ldots, \psi_n)\left(\sum_{i=1}^n \lambda_i (1 \otimes w_i)\right) = p(\lambda_1, \ldots, \lambda_n),$$

but on the other hand

$$f\left(\sum_{i=1}^n \lambda_i w_i\right) = p(\varphi_1, \ldots, \varphi_n)\left(\sum_{i=1}^n \lambda_i w_i\right) = p(\lambda_1, \ldots, \lambda_n).$$

Finally, assume that incl' is another such algebra homomorphism. We have $\mathrm{incl}(f) = \mathrm{incl}'(f) \in \mathcal{P}_L(W_L)$ for all $f \in \mathcal{P}_k(W)$. By definition $(\mathrm{incl}(f) - \mathrm{incl}'(f))|_W = 0$. By Lemma IV.4 2) $W \subseteq W_L$ is dense over L. Therefore $\mathrm{incl}(f) = \mathrm{incl}'(f)$ for all $f \in \mathcal{P}_L(W_L)$. □

Corollary IV.6. *Let k be an infinite field and $k \subseteq L$ a field extension as well as W a finite-dimensional k-vector space. Let $W_L := L \otimes_k W$. Then*

$$\begin{aligned} \Phi\colon \mathcal{P}_k(W)_L &\to \mathcal{P}_L(W_L) \\ \lambda \otimes f &\mapsto \lambda\,\mathrm{incl}(f) \end{aligned}$$

is an isomorphism of k-algebras.

Proof. Take k-bases φ^a and ψ^a of $\mathcal{P}_k(W)$ and $\mathcal{P}_L(W_L)$ for $a \in \mathbb{Z}^n_{\geq 0}$, respectively. Then $\Phi(1 \otimes \varphi^a) = \mathrm{incl}(\varphi^a) = \psi^a$, a basis vector over L. Hence Φ is an isomorphism of k-vector spaces since it sends a basis to a basis. It is an algebra homomorphism by Lemma IV.5. □

Lemma IV.7. *Let k be an infinite field and W a finite-dimensional k-vector space. For $h \in \mathcal{P}_k(W) \setminus \{0\}$ define $W_h := \{w \in W \mid h(w) \neq 0\}$. Then $W_h \subseteq W$ is Zariski-dense (over k).*

Proof. Let $f \in \mathcal{P}_k(W)$ with $f|_{W_h} = 0$. Then $fh = 0$ as we have $(fh)(w) = f(w)h(w) = 0$ for all $w \in W$. Since $\mathcal{P}_k(W)$ is an integral domain we have $f = 0$ since $h \neq 0$. □

Corollary IV.8. $\mathrm{GL}_n(k) \subseteq \mathrm{M}_{n\times n}(k)$ *is Zariski-dense (over k). This proves Zariski property I.*

Proof. Use Lemma IV.7 with $W = \mathrm{M}_{n\times n}(k)$ and $h = \det$. □

[November 5, 2018]

[November 8, 2018]

In the proofs of Invariant Theorem I and Invariant Theorem II we assumed the following properties:

Zariski property I: If $f \in \mathcal{P}_k(\mathrm{M}_{n\times n}(k))$ such that $f|_{\mathrm{GL}_n(k)} = 0$ then $f = 0$.

Zariski property II: If $f \in \mathcal{P}_k(\mathrm{M}_{n\times n}(k))^{\mathrm{GL}_n(k)}$ such that $f|_{\substack{\text{diagonal}\\\text{matrices}}} = 0$ then $f = 0$.

We already proved Zariski property I in Corollary IV.8.

Lemma IV.9. *Let G be a group, W a finite-dimensional representation of G over k and $f \in \mathcal{P}_k(W)^G$.*

1) *If $X \subseteq W$ such that $G.X = \{g.x \mid g \in G, x \in X\}$ is Zariski-dense and if $f|_X = 0$ then $f = 0$.*

2) *If there exists a Zariski-dense orbit then f is constant.*

Proof.

1) As f is G-invariant we have $f(g.x) = f(x) = 0$ for all $g \in G$ and $x \in X$. Thus, $f|_{G.X} = 0$, and $f = 0$ as $G.X$ is Zariski-dense.

2) As f is G-invariant it is constant on G-orbits. Let O be a dense G-orbit. Then there exists a $\lambda \in k$ such that $(f-\lambda)|_O = 0$. As O is dense, we get $f - \lambda = 0$ or $f = \lambda$. □

Proposition IV.10. *Let $k = \overline{k}$. Define*

$$\mathrm{Diag}_n(k) := \{A \in \mathrm{M}_{n\times n}(k) \mid A \textit{ diagonizable}\}.$$

Then $\mathrm{Diag}_n(k)$ is Zariski-dense in $\mathrm{M}_{n\times n}(k)$.

Proof. Let $f \in \mathcal{P}_k(\mathrm{M}_{n\times n}(k))$ such that $f|_{\mathrm{Diag}_n(k)} = 0$. We show that $f = 0$. Let $A \in \mathrm{M}_{n\times n}(k)$. As $k = \overline{k}$, A has a Jordan normal form, i.e. $S \in \mathrm{GL}_n(k)$ such that SAS^{-1} is in Jordan normal form with diagonal entries $b_1, \ldots, b_n \in k$ (not necessarily distinct). Define functions $D, M, \varphi \colon k \to \mathrm{M}_{n\times n}(k)$ as follows. Fix pairwise distinct $a_1, \ldots, a_n \in k$ (possible since $|k| = \infty$). Now set

$$\begin{aligned} D(z) &= z\,\mathrm{diag}(a_1, \ldots, a_n), \\ M(z) &= SAS^{-1} + D(z), \\ \varphi(z) &= S^{-1}M(z)S = A + S^{-1}D(z)S. \end{aligned}$$

Note that the eigenvalues of $\varphi(z)$ are $b_1 + a_1 z, \ldots, b_n + a_n z$ and $\varphi(0) = A$.

The eigenvalues of $\varphi(z)$ are pairwise distinct for all but finitely many $z \in k$. To see this choose $z \in k$ such that $b_i + a_i z = b_j + a_j z$ for $i \neq j$. Then $z = \frac{b_i - b_j}{a_j - a_i}$. So z is uniquely determined by this equation.

Thus $\varphi(z) \in \mathrm{Diag}_n(k)$ and $f(\varphi(z)) = 0$ for all but finitely many $z \in k$. Now we have $f \circ \varphi \in \mathcal{P}_k(W)$ such that $f \circ \varphi$ vanishes on all but finitely many $z \in k$. But as $|k| = \infty$ we get $f \circ \varphi = 0$ and $0 = f(\varphi(0)) = f(A)$. □

In particular Zariski property II holds for $k = \overline{k}$: Take $f \in \mathcal{P}_k(\mathrm{M}_{n\times n}(k))^{\mathrm{GL}_n(k)}$ such that $f|_{\mathrm{D}_n(k)} = 0$ where $D_n(k)$ is the set of diagonal matrices in $\mathrm{M}_{n\times n}(k)$. By Lemma IV.9 we get $f|_{\mathrm{Diag}_n(k)} = 0$ and by Proposition IV.10 $f = 0$.

Lemma IV.11. *Let k be an infinite field and $L = \overline{k}$. If $f \in \mathcal{P}_k(\mathrm{M}_{n\times n}(k))^{\mathrm{GL}_n(k)}$ then* $\mathrm{incl}(f) \in \mathcal{P}_L(\mathrm{M}_{n\times n}(k))^{\mathrm{GL}_n(k)}$.

We claim that this Lemma implies Zariski property II.

Proof. Let $f \in \mathcal{P}_k(\mathrm{M}_{n\times n}(k))^{\mathrm{GL}_n(k)}$ such that $f|_{\mathrm{D}_n(k)} = 0$. Consider $\hat{f} = \mathrm{incl}(f)$. By definition of incl we have $\hat{f}(A) = f(A)$ for all $A \in \mathrm{D}_n(k)$ (note that $\mathrm{D}_n(k) \subseteq D_n(L) = \mathrm{D}_n(k)_L$ by scalar extension). Thus $\hat{\ }|_{\mathrm{D}_n(k)} = 0$. As $\mathrm{D}_n(k)$ is Zariski-dense in $\mathrm{D}_n(L) = \mathrm{D}_n(k)_L$ by Lemma IV.4 2) we get $\hat{f}|_{D_n(L)} = 0$. Then $\hat{f} = 0$ by Lemma IV.11 and the discussion above. As incl is injective by Lemma IV.5 we have $f = 0$. □

Proof of Lemma IV.11. Let $f \in \mathcal{P}_k(\mathrm{M}_{n\times n}(k))^{\mathrm{GL}_n(k)}$. Denote $\hat{f} = \mathrm{incl}(f)$. Define

$$\begin{aligned} \gamma \colon \mathrm{M}_{n\times n}(k) \times \mathrm{M}_{n\times n}(L) &\to L \\ (A, B) &\mapsto \hat{f}(AB) - \hat{f}(BA). \end{aligned}$$

We want to show that $\gamma = 0$. For $S \in \mathrm{GL}_n(k)$ and $A \in \mathrm{M}_{n\times n}(k)$ we have $f(SA) = f(SASS^{-1}) = f(AS)$ as f is $\mathrm{GL}_n(k)$-invariant. Thus $\hat{f}(AS) = f(AS) = f(SA) = \hat{f}(SA)$ and $\gamma(S, A) = 0$ for all $S \in \mathrm{GL}_n(k)$ and $A \in \mathrm{M}_{n\times n}(k)$.

Fix $S \in \mathrm{GL}_n(k)$ and define

$$\begin{array}{rcl} \gamma_S\colon \mathrm{M}_{n\times n}(L) & \to & L \\ A & \mapsto & \gamma(S, A). \end{array}$$

We have $\gamma_S \in \mathcal{P}_L(\mathrm{M}_{n\times n}(L))$ and $\gamma_S|_{\mathrm{M}_{n\times n}(k)} = 0$. As $\mathrm{M}_{n\times n}(k)$ is dense in $\mathrm{M}_{n\times n}(k)_L = \mathrm{M}_{n\times n}(L)$ (over L) we get $\gamma_S = 0$. Therefore $\gamma(S, A) = 0$ for all $S \in \mathrm{GL}_n(k)$ and $A \in \mathrm{M}_{n\times n}(L)$.

Fix $A \in \mathrm{M}_{n\times n}(L)$ and define

$$\begin{array}{rcl} \gamma^A\colon \mathrm{M}_{n\times n}(L) & \to & L \\ B & \mapsto & \gamma(B, A). \end{array}$$

Again $\gamma^A \in \mathcal{P}_L(\mathrm{M}_{n\times n}(L))$ and $\gamma^A|_{\mathrm{GL}_n(k)} = 0$. The reader may check that $\mathrm{GL}_n(k)$ is Zariski-dense in $\mathrm{M}_{n\times n}(L)$ over L. Then $\gamma^A = 0$. As A as arbitrary we get $\gamma = 0$.

Now let $S \in \mathrm{GL}_n(L)$ and $A \in \mathrm{M}_{n\times n}(L)$. Then $\hat{f}(SAS^{-1}) = \hat{f}(AS^{-1}S) = \hat{f}(A)$, and $\hat{f} \in \mathcal{P}_l(\mathrm{M}_{n\times n}(L))^{\mathrm{GL}_n(L)}$. □

V. Semisimple modules and the Artin-Wedderburn theorem

In this section R is a ring with 1, but not necessarily commutative. Modules are left modules.

V.1. Semisimple modules

Definition. An R-module M is called *irreducible* if $M \neq 0$ and if M has no other submodules other than 0 and M.

Proposition V.1. *Let M be an R-module. Then the following are equivalent:*

1) *M is the sum off irreducible submodules, i.e. there exists a collection $(L_i)_{i\in I}$ of irreducible submodules $L_i \subseteq M$ such that $M = \sum_{i\in I} M_i$.*

2) *M is isomorphic to a direct sum of irreducible R-modules, i.e. there exists a collection $(L_i)_{i\in I}$ of irreducible R-modules L_i such that $M \cong \bigoplus_{i\in I} L_i$.*

3) *Every submodule of M has a complement, i.e. for every submodule $M' \subseteq M$ there exists a submodule $M'' \subseteq M$ such that $M' \cap M''$ and $M' + M'' = M$.*

Proof. Left to the reader. □

Definition. An R-module is called *semisimple* if it satisfies one of the equivalent conditions from Proposition V.1.

Examples.

1) Let $R = k$ a field. The irreducible R-modules are the 1-dimensional k-vector spaces as every k-vector space has a basis. Thus every k-vector space is semisimple.

2) Let k be a field and
$$R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \,\middle|\, a, b, c \in k \right\}.$$
Let $M = k^2$ with the obvious R-module structure. Then $M' = \left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\rangle_k$ is a proper submodule, and M is not irreducible. But M' does not have a complement, thus M' does not have a complement, and M is not semisimple.

3) Let G be a finite group and $R = kG$ such that $\operatorname{char} k \nmid |G|$. By Maschke's theorem every finite-dimensional kG-module is semisimple.

Lemma V.2.

1) *If $(M_i)_{i \in I}$ is a collection of semisimple R-modules then $\bigoplus_{i \in I} M_i$ is semisimple.*

2) *Let M be semisimple and $N \subseteq M$ a submodule. Then N and ${}^{M}\!/_{N}$ are semisimple.*

Proof.

1) As the M_i are semisimple there exist irreducible modules $L_i^{(j)}$ with $j \in J_i$ such that $M_i \cong \bigoplus_{j \in J_i} L_i^{(j)}$. Then we have
$$\bigoplus_{i \in I} \bigoplus_{j \in J_i} L_i^{(j)} = \bigoplus_{i \in I} M_i.$$

2) N is semisimple: It is enough to show that any submodule of N has a complement in N. Consider a submodule $U \subseteq N$ which also is a submodule of M. Since M is semisimple there exists a complement C of U in M, i.e. $M = U \oplus C$ as R-modules. Set $C' = N \cap C$. We want to show that $N = U \oplus C'$. Take $y \in N$. Then we have $n \in U$ and $c \in C$ such that $y = u + c$. Now $c = y - u \in N$ since $u \in U \subseteq N$. Then $c \in C \cap N = C'$. We get $N = U + C'$ and then $N = U \oplus C'$ since $U \cap C = 0$.

${}^{M}\!/_{N}$ is semisimple: We have ${}^{M}\!/_{N} \cong C'$ as R-modules. Since C' is a submodule of N it is semisimple by 1). Hence ${}^{M}\!/_{N}$ is semisimple. □

[November 8, 2018]

[November 12, 2018]

Definition. Let M be an R-module and L an irreducible R-module. Then

$$\mathrm{Iso}_L(M) := \sum_{\substack{E \subseteq M \text{ submodule} \\ E \cong L \text{ as } R\text{-modules}}} E$$

is the *L-isotypic component* of M.

Lemma V.3 (Schur's lemma)**.** *Let M be an irreducible R-module. Then:*

1) *Let N be an irreducible R-module and $f\colon M \to N$ an R-module homomorphism. Then $f = 0$ or f is an isomorphism.*

2) $\mathrm{End}_R(M)$ *is a skew field (i.e. a field, but the multiplication is not necessarily commutative).*

If R is moreover a k-algebra:

3) $\mathrm{End}_R(M)$ *is a division algebra (i.e. an algebra where all nonzero elements have a multiplicative inverse).*

4) *If $\overline{k} = k$ and $\dim_k M < \infty$ then $\mathrm{End}_R(M) \cong k$ by $\lambda \mathrm{id}_M \leftarrow\!\shortmid \lambda$.*

Proof. We omit the proofs of 1), 2) and 3) (see the proof of Schur's lemma for representations).

Now we show 4). We claim that if D is a division algebra (over k) and $\dim_k D < \infty$ we have $D = k$. To see this let $0 \neq a \in D$. The elements $1, a, a^2, \ldots,$ are linearly dependent because $\dim_k D < \infty$. Therefore we have a $p \in k[t]$ with $p(a) = 0$ and $p \neq 0$. Since $k = \overline{k}$ we have $p(t) = \prod_{i=1}^n (t - a_i)$ for some $a_i \in k$. Now $0 = p(a) = \prod_{i=1}^n (a - a_i)$, and we get $a = a_i$ for some i. Thus $a \in k$ and $D = k$.

Now $\mathrm{End}_R(M) \subseteq \mathrm{End}_k(M)$ is finite dimensional by assumption, hence by 3) a finite dimensional divison algebra. Our claim implies 4). □

Lemma V.4. *Let M be a semisimple R-module. Let $\varphi\colon \bigoplus_{i \in I} L_i \to M$ be an isomorphism of R-modules with L_i $(i \in I)$ irreducible. Then*

$$\mathrm{Iso}_L(M) = \varphi\left(\bigoplus_{j \in J} L_j\right)$$

where $J = \{i \in I \mid L_i \cong L\}$.

Proof. Since φ is an R-module isomorphism (hence injective) we have $\varphi(\bigoplus_{i \in I} L_i) = \bigoplus_{i \in I} \varphi(L_i)$ and $\varphi(L_i) \cong L_i$ for all $i \in I$ (by Schur's lemma).

"$\supseteq$": $$\varphi\left(\bigoplus_{j \in J} L_j\right) = \bigoplus_{j \in J} \underbrace{\varphi(L_j)}_{\cong L_j \cong L} = \sum_{j \in J} \varphi(L_j) \subseteq \mathrm{Iso}_L(M).$$

"$\subseteq$": Assume $\mathrm{Iso}_L(M) \nsubseteq \varphi\big(\bigoplus_{j\in J} L_j\big)$. Then there exists a $i_0 \in I$ such that $i_0 \notin J$ and the map

$$f\colon \mathrm{Iso}_l(M) \hookrightarrow M \to \varphi(L_{i_0})$$

($M \to \varphi(L_{i_0})$ by projection) is nonzero. Then there exists a submodule $L \subsetneq M$ such that $f|_L \neq 0$ and f defines a nonzero R-module homomorphism $L \to \varphi(L_{i_0}) \cong L_{i_0}$, contradictory to Schur's lemma since $i_0 \notin J$. □

Definition. We define

$$\mathrm{Irr}(R) := \left\{\substack{\text{isoclasses of irre-}\\ \text{ducible } R\text{-modules}}\right\} := \left\{\substack{\text{irreducible}\\ R\text{-modules}}\right\}/\sim$$

where $L \sim L'$ if $L \cong L'$ as R-modules. We often fix a system of representatives for the isoclasses and identify the set of representatives with $\mathrm{Irr}(R)$.

Remark. $\mathrm{Irr}(R)$ is indeed a set.

Proof. Let L be an irreducible R-module. Pick $0 \neq m \in L$. This generates L as an R-module. We get a surjective R-module homomorphism

$$\begin{aligned}\varphi\colon R &\to L\\ 1 &\mapsto m.\end{aligned}$$

Henc $R/\ker\varphi \cong L$ and $\ker\varphi = \mathrm{Ann}_R(m)$ is a left ideal. Since L is irreducible, $\ker\varphi$ is in fact maximal. But maximal left ideals form a set. □

Example. $R = k$ a field. If V is an R-module (i.e. k-vector space) then $\langle v\rangle \subseteq V$ is a submodule of V for all $v \in V$. Thus $\mathrm{Irr}(R) = \{k\}$.

Lemma V.5. *Let M be a semisimple R-module. Then we have*

$$M = \bigoplus_{L\in\mathrm{Irr}(R)} \mathrm{Iso}_L(M),$$

the isotypic decomposition*.*

Proof. As M is semisimple there exists an isomorphism of R-modules $\varphi\colon \bigoplus_{i\in I} L_i \to M$ with irreducible modules L_i ($i \in I$). Now group summands which belong to the same isomorphism class in $\mathrm{Irr}(R)$ and use Lemma V.4. □

Example. If $R = k$ a field then

$$M = \bigoplus_{L\in\mathrm{Irr}(k)=\{k\}} \mathrm{Iso}_L(M) = \underbrace{\mathrm{Iso}_k(M)}_{k\text{-isotypic component}}$$

and we get $M \cong \bigoplus_{i\in I} k$. The existence of such an isomorphism is equivalent to the existence of a basis. Each such iso corresponds to a choice of a basis.

V.2. Hilbert's theorem

Theorem V.6 (Hilbert's theorem). *Let G be a group and W a finite-dimensional representation of G over k (k an infinite field). Assume $\mathcal{P}_k(W) \cong \bigoplus_{i\in I} L_i$ as representations of G with irreducible L_i ($i \in I$). Then $\mathcal{P}_k(W)^G$ is finitely generated as a k-algebra.*

Remark. The assumption says precisely that $\mathcal{P}_k(W)$ is a semisimple kG-module.

Remarks.

- If G is a finite group and $\operatorname{char} k \nmid |G|$ then $\mathcal{P}_k(W) = \bigoplus_{d\geq 0} \mathcal{P}_k(W)_d$ (see Proposition III.19) is a graded algebra with finite-dimensional homogeneous components $\mathcal{P}_k(W)_d$ with are then finite-dimensional representations of G.

  By Maschke's theorem $\mathcal{P}_k(W)$ is semisimple and so $\mathcal{P}_k(W) = \bigoplus_{d\geq 0} \mathcal{P}_k(W)_d$ is semisimple by Lemma V.2.

- In the case $R = kG$ for some group G the semisimplicity is often called *complete reducibility*.

Goal. We want to find examples where Hilbert's theorem holds. This will lead us to *reductive groups* ($\mathrm{SL}_n(k)$, $\mathrm{GL}_n(k)$, algebraically closed fields, ...).

Lemma V.7. *Let $B = \bigoplus_{d\geq 0} B_d$ be a non-negatively graded k-algebra. Consider the (two-sided) ideal $B_+ \cong \bigoplus_{d>0} B_d$. If B_d is a finitely generated ideal in B, then B is finitely generated as a B_0-algebra. Moreover one can finite a finite generating set of homogeneous elements.*

Proof. Left to the reader. $\square$

Lemma V.8. *Let A be a commutative k-algebra, G a group acting on A by algebra automorphisms. Assume $A = \sum_{i\in I} L_i$ as representations of G with the L_i ($i \in I$) irreducible. (i.e. A is a semisimple kG-module). Then:*

1) *$A = A^G \bigoplus N$ as representations where $A^G = \sum_{j\in J} L_j$ and $N = \sum_{i\in I\setminus J} L_i$ with $J = \{i \in I \mid L_i \cong T\}$ and the trivial representation T.*

2) *The* Reynolds operator *$\pi\colon A \to A^G$ (projection) satisfies $\pi(ba) = b\pi(a)$ for all $b \in A^G$ and $a \in A$.*

Proof.

1) This follows from the isotypic decomposition $A^G = \mathrm{Iso}_T(A)$ and

$$N = \bigoplus_{\substack{L\in \mathrm{Irr}(kG)\\ L\not\cong T}} \mathrm{Iso}_L(A).$$

2) For $s \in A^G$ consider $m_b\colon A \to A$ by $a \mapsto ba$. This is an morphism of representations as we have $m_b(g.a) = b(g.a) = (g.b)(g.a) = g.(ba) = g.m_b(a)$ for all $a \in A$ and $g \in G$. By SCHUR'S LEMMA the restriction of m_b to any L_i has image isomorphic to L_i or 0. Thus $m_b(A^G) \subseteq A^G$ and $m_b(N) \subseteq N$. For $b \in A^G$ and $a \in A$ we have $\pi(ba) = \pi(ba_1 + a_2) = ba_1 = b\pi(a)$ where $a = a_1 + a_2$ with $a_1 \in A^G$ and $a_2 \in N$. $\square$

Proof of HILBERT'S THEOREM. Set $A := \mathcal{P}_k(W)$. We know that $A = \bigoplus_{d\geq 0} A_d$. By Lemma V.8 we have $A = A^G \oplus N$ (with the notation from there). If $I \subseteq A^G$ is an ideal then

$$\pi(IA) = I\pi(A) = IA^G = I \tag{*}$$

using the definition of π and $1 \in A^G$. By Lemma III.5 we have $A^G = \bigoplus_{d\geq 0} A_d^G$ and we can take $I := A_+^G = \bigoplus_{d>0} A_d^G$. Then $\tilde{I} = IA$ is the ideal in A generated by I. Since A is noetherial (because $A \cong k[X_1, \ldots, X_n]$) we can find $f_1, \ldots, f_m \in I$ which generate $\tilde{I}$ (for some $m \in \mathbb{N}$).

We claim that $f_1, \ldots, f_m$ generate I as in ideal in A^G. By (*) any $x \in I$ is contained in $\pi(IA)$, hence $x = \pi(\sum_{i=1}^m f_i a_i)$ for some $a_i \in A$. Using Lemma V.8 2) we get $x = \sum_{i=1} f_i \pi(a_i)$. As $\pi(a_i) \in A^G$ for all i the claim follows.

Now apply Lemma V.7 to $B = A^G$ with $B_+ = \bigoplus_{d\geq 0} A_d^G$. Then A^G is finitely generated as a B_0-algebra. But $B_0 = A_0^G = A_0 = k1 = k$. Hence A^G is a finitely generated k-algebra. $\square$

V.3. Semisimple rings and algebras

Definition. A ring R (with 1) is semisimple if it is semisimple as a left mdoule over itself (via the regular action given by left multiplication). In this case $R = \bigoplus_{i\in \mathrm{Irr}(R)} \mathrm{Iso}_L(R)$. An algebra A is semisimple if it is semisimple as a ring.

Definition. A ring R (with 1) is simple if $R \neq 0$ and $R = \mathrm{Iso}_L(R)$ for some irreducible R-module L. An algebra is simple if it is simple as a ring.

[November 12, 2018]

[November 15, 2018]

Remark. Simple rings are semisimple.

Example.

1) $R = k$ is a simple ring.

2) Let G finite group and k a field with $\operatorname{char} k \nmid |G|$. By MASCHKE'S THEOREM kG is a semisimple ring.

3) Let $R = \mathrm{M}_{n\times n}(D)$ with $n \in \mathbb{Z}_{>0}$ and D a division algebra. Then R is a simple ring/k-algebra.

Proof. For $1 \leq i \leq n$ let

$$G = \{A \in \mathrm{M}_{n\times n}(D) \mid \text{nonzero entries only in } i\text{-th column}\}.$$

Then $R = \mathrm{M}_{n\times n}(D) = \bigoplus_{i=1}^n C_i$ as R-modules because $E_{ab}E_{ji} = \delta_{jb}E_{ai}$ and $C_i \cong D^n$ as R-modules and $C_i \cong D^n$ as R-modules by $E_{ji} \mapsto e_j$ (the j-th basis vector). Now D^n is an irreducible R-module since R acts trasitively on D^n (because then any nonzero submodule is already D^n). Thus $R \cong \bigoplus_{i=1}^n L$ with $L \cong D^n$ irreducible, and R is simple. □

Lemma V.9. *Let R be a simple ring. Then $|\mathrm{Irr}(R)| = 1$.*

Proof. As R is simple we have $R = \mathrm{Iso}_L(R)$ for some irreducible R-module L by definition. Assume that L' is another irreducible R-module with $L \ncong L'$. Then pick $0 \neq m \in L'$ and obtain a surjective R-module homomorphism $R \to L'$ by $1 \mapsto m$. Hence we get a nonzero R-module homomorphism $\mathrm{Iso}_L(R) \to L'$. Thus there exists a nonzero R-module homomorphism $L \to L'$ which is a contradiction to Schur's lemma. We get $L \cong L'$. □

Proposition V.10. *Let R be a semisimple ring and M an R-module homomorphism. Then M is semisimple as an R-module.*

Proof. Let $\{m_i\}_{i\in I}$ be a set of generators of the R-module M. We get a surjective R-module homomorphism

$$\begin{aligned} \bigoplus_{i\in I} R &\to M \\ (0,\dots,0,1,0,\dots,0) &\mapsto m_j. \end{aligned}$$

Now R is semisimple, and it is also semisimple as a left R-module. By Lemma V.2 $\bigoplus_{i\in I} R$ is a semisimple R-module and then also the quotient M. □

Proposition V.11. *Let R be a semisimple ring. Then we can find irreducible R-modules L_i with $i \in I$ finite such that*

$$R \cong \bigoplus_{i\in I} L_i.$$

Proof. As R is a semisimple ring we can find irreducible R-modules L_i $(i \in J)$ such that $\varphi\colon \bigoplus_{i\in J} L_i \to R$ is an isomorphism of R-modules. Write $1 = \sum_{i\in J} e_i$ with $e_i \in L_i$ and finitely many e_i nonzero. Let $I = \{i \in J \mid e_i \neq 0\}$. Then

$$f = \varphi\Big|_{\bigoplus_{i\in I}} : \bigoplus_{i\in I} L_i \to R.$$

f is injective (because φ is) and $1 \in \mathrm{im}\, f$. We get $R1 \subseteq \mathrm{im}\, f$ because it is an R-module homomorphism. Thus f is surjective and an isomorphism. □

Motivation. Assume R is a ring and M an R-module. Then M is an $R' := \mathrm{End}_R(M)$-module via $f.m = f(m)$ for all $f \in R'$ and $m \in M$. We call R' the *centralizer* of the R-action on M. What is now the centralizer of the R'-action on M? By definition we have $R'' = \mathrm{End}_{R'}(M) = \mathrm{End}_{\mathrm{End}_R(M)}(M)$. We are interested in situations where $R'' = R'$ (the *double centralizer property*).

Theorem V.12 (Jacobson density theorem I)**.** *Let R be a ring with 1 and M a semisimple R-module. Consider the map*

$$\begin{aligned} \Phi\colon R &\to \mathrm{End}_{\mathrm{End}_R(M)}(M) \\ r &\mapsto (m \mapsto rm). \end{aligned}$$

Then the image of Φ is "dense" in the following sense: For all $f \in \mathrm{End}_{\mathrm{End}_R(M)}(M)$ and $m_1, \ldots, m_s \in M$ there exists an $a \in R$ such that $f(m_i) = am_i$ for all $1 \le i \le s$.

Remark.

1) Consider $\Phi\colon R \to \mathrm{End}_{\mathrm{End}_R(M)}(M) \subseteq \mathrm{Maps}(M, M)$ with the discrete topology. Then $\operatorname{im}\Phi$ is dense in $\mathrm{End}_{\mathrm{End}_R(M)}(M)$ in the topological sense.

2) In the special case $M = R$ (an R-module via left multiplication) the Jacobson density theorem I gives an isomorphism of algebras

$$R \xmapsto{m \mapsto rm} \mathrm{End}_{\mathrm{End}_R(M)}(M) \xmapsto{\mathrm{id}} \mathrm{End}_R R \xmapsto{f \mapsto f(1)} R.$$

Proof of Jacobson density theorem I. As we have $\Phi(r)(f.m) = \Phi(r)(f(m)) = rf(m) = f(rm) = f.(\Phi(r)(m))$ for all $f \in \mathrm{End}_R(M)$, $m \in M$ and $r \in R$, Φ is well-defined.

First we assume $s = 1$. Let $m = m_1 \in M$. Since M is a semisimple R-module the submodule Rm has a complement, i.e. $M = Rm \oplus C$ as R-modules. Consider $\pi\colon M = Rm \oplus C \to Rm \hookrightarrow R$ by projection. Clearly $\pi \in \mathrm{End}_R(M)$. For any $f \in \mathrm{End}_{\mathrm{End}_R(M)}(M)$ we have $\pi \circ f = f \circ \pi$. Thus $f(m) = f(\pi(m)) = \pi(f(m)) \in Rm$, so there exists an $a \in R$ such that $f(m) = am$.

For the general case let $m_1, \ldots, m_s \in M$ and $f \in \mathrm{End}_{\mathrm{End}_R(M)}(M)$. Define

$$\begin{aligned} \hat{f} := \bigoplus_{i=1}^{s} f\colon M^s &\to M^s \\ (n_1, \ldots, n_s) &\mapsto (f(n_1), \ldots, f(n_s)). \end{aligned}$$

The reader may check that $\hat{f} \in \mathrm{End}_{\mathrm{End}_R(M^s)}(M^s)$. Using the case $s = 1$ there exists an $a \in R$ such that $\hat{f}((m_1, \ldots, m_s)) = a(m_1, \ldots, m_s)$. But we also have $\hat{f}((m_1, \ldots, m_s) = (f(m_1), \ldots, f(m_s))$, so we get $f(m_i) = am_i$ for all $1 \le i \le s$. $\square$

Corollary V.13. *Let k be a field and A a k-algebra with 1. Let M be a finite-dimensional semisimple A-module. Then*

$$\begin{aligned} \Phi\colon A &\longrightarrow \operatorname{End}_{\operatorname{End}_A(M)}(M) \\ a &\longmapsto (m \mapsto am) \end{aligned}$$

is surjective.

Proof. We have $k \subseteq \operatorname{End}_A(M)$, hence $\operatorname{End}_{\operatorname{End}_A(M)}(M) \subseteq \operatorname{End}_k(M)$. Let $m_1, \ldots, m_s \in M$ be a basis of M. For $f \in \operatorname{End}_{\operatorname{End}_A(M)}(M)$ we find an $a \in A$ such that $f(m_i) = am_i$ for all $1 \leq i \leq s$ by the Jacobson density theorem I. Now f is determined on a basis of M, and we get $f(m) = am$ for all $m \in M$. $\square$

Theorem V.14 (Jacobson density theorem II)**.** *Let R be a ring with 1 and N a semisimple R-module. Let $n_1, \ldots, n_s \in N$ be linearly independent over $\operatorname{End}_R(M)$ and $n_1', \ldots, n_s' \in N$ arbitrary. Then there is an $r \in R$ such that $rn_i = n_i'$ for all $1 \leq i \leq s$.*

Remark. That means that N^s is generated by $n_1, \ldots, n_s$.

Proof. Let $x = (n_1, \ldots, n_s) \in N^s$. Now N^s is semisimple. Hence Rx has a complement in N^s, say $N^s = Rx \oplus C$. Consider $\pi\colon N^s \to C \hookrightarrow N^s$ by projection. Clearly $\pi \in \operatorname{End}_r(N^s)$. We can realize π as a matrix $A = (a_{ij}) \in \mathrm{M}_{s\times s}(\operatorname{End}_R(N))$. Then $a_{i1}n_1 + a_{i2}n_2 + \ldots + a_{is}n_s = 0$ for all $1 \leq i \leq s$ since $\pi(Rx) = 0$. Therefore $a_{ij} = 0$ for all $1 \leq i, j \leq s$ because $n_1, \ldots, n_s$ are linearly independent over $\operatorname{End}_R(N)$. We get $A = 0$, $\pi = 0$ and $C = 0$, so $N^s = Rx$. The claim follows. $\square$

Corollary V.15 (Burnside theorem – coordinate form)**.** *Let $k = \overline{k}$ a field, V a finite-dimensional k-vector space and $A \subseteq \operatorname{End}_k(V)$ a subalgebra such that V is an irreducible A-module. Then $A = \operatorname{End}_k(V)$.*

Proof. We have $\operatorname{End}_k(V) = k$ by Schur's lemma. Now $\Phi\colon A \to \operatorname{End}_{\operatorname{End}_A(V)}(V) = \operatorname{End}_k(V)$ is surjective by the Theorem V.14, hence an isomorphism. $\square$

Corollary V.16 (Burnside theorem – coordinate free)**.** *Let $k = \overline{k}$ and $A \subseteq \mathrm{M}_{n\times n}(k)$ be a subalgebra such that k^n is irreducible as an A-module. Then $A = \mathrm{M}_{n\times n}(k)$.*

Corollary V.17. *Let $k = \overline{k}$, A be a k-algebra and M a finite-dimensional A-module. Then the following are equivalent:*

1) *M is an irreducible A-module.*

2) *$\Phi\colon A \to \operatorname{End}_{\operatorname{End}_A(M)}(M)$ is surjective.*

Proof.

1) $\Rightarrow$ 2): By Schur's lemma we have $\operatorname{End}_A(M) = k$, and by the Jacobson density theorem II Φ is surjective.

2) $\Rightarrow$ 1): Let $0 \neq m \in M$. For all $m' \in M$ we have an $\varphi \in \mathrm{End}_k(M)$ such that $\varphi(m) = m'$. Since Φ is surjective there exists an $a \in A$ with $\Phi(a) = \varphi$. Now $m' = \varphi(m) = am$, and M is irreducible. □

Corollary V.18. *Let $k = \overline{k}$, A be a k-algebra and M a finite-dimensional irreducible A-module. Then $(\dim_k M)^2 \leq \dim_k A$.*

Proof. This follows from the surjectivity of $A \to \mathrm{End}_{\mathrm{End}_A(M)}(M) = \mathrm{End}_k(M)$ (using Corollary V.17) because of $\dim_k \mathrm{End}(M) = (\dim_k M)^2$. □

[November 15, 2018]

[November 19, 2018]

Lemma V.19. *Let R_i ($1 \leq i \leq n$) be rings (with 1) and $R := R_1 \times \cdots \times R_n$. Let 1_i be the unit in $R_i \subseteq R$ (i.e. $(1_i)_j = \delta_{ij}$). Let M be an R-module. Then we have:*

1) $1 = \sum_{i=1}^n 1_i$ *is the unit in R.*

2) $1_i M$ *is an R_i-module via restriction of the R-module structure.*

3) $M = \sum_{i=1}^n 1_i M$ *as R-modules where R acts on the right-hand side by*
$$(r_1, \ldots, r_n). \sum_{i=1}^n m_i = \sum_{i=1}^n r_i m_i.$$
Moreover the sum is direct.

4) $\mathrm{End}_R(M) = \prod_{i=1}^n \mathrm{End}_R(1_i M)$.

5) *If M_i is an R_i-module for $1 \leq i \leq n$ then $\bigoplus_{i=1}^n M_i$ is an R-module via*
$$(r_1, \ldots, r_n).(m_1, \ldots, m_n) = (r_1 m_1, \ldots, r_n m_n).$$

6) *M is irreducible if and only if $M = 1_i M$ for some (unique) $1 \leq i \leq n$ and $1_i M$ is irreducible as an R_i-module.*

7) *R is semisimple if and only if each R_i ($1 \leq i \leq n$) is semisimple.*

Proof. The proof is left to the reader. It is advisable to construct a bijection of sets
$$S_1 \times S_2 \times \cdots \times S_n \overset{1:1}{\longleftrightarrow} S$$
where
$$S_i := \{R_i\text{-submodules of } 1_i M\} \quad \text{and} \quad S_i := \{R\text{-submodules of } M\}.$$
□

Corollary V.20. *Let R be a ring such that*

$$R \cong \mathrm{M}_{n_1 \times n_1}(D_1) \times \cdots \times \mathrm{M}_{n_r \times n_r}(D_r)$$

as rings where $n_i \in \mathbb{N}$ and the D_i are skew fields. Then R is a semisimple ring. Moreover we have $|\mathrm{Irr}(R)| = r$.

Proof. We saw that $\mathrm{M}_{n_i \times n_i}(D_i)$ is a simple ring. Thus it is semisimple, and R is semisimple too.

By Lemma V.9 we have $|\mathrm{Irr}(\mathrm{M}_{n_i \times n_i}(D_i))| = 1$ since $\mathrm{M}_{n_i \times n_i}(D_i)$ is simple. Due to Lemma V.19 6) every irreducible R-module is of the form $1_i M$ for some $1 \leq i \leq n$ with $1_i M$ is irreducible as an $\mathrm{M}_{n_i \times n_i}(D_i)$-module (where $\mathrm{M}_{n_i \times n_i}(D_i)$ acts by zero). This implies $|\mathrm{Irr}(r)| \leq r$. It is now enough to show that $1_i M \ncong 1_j M'$ as R-modules for $i \neq j$. Assume we have an isomorphism $\varphi \colon 1_i M \to 1_j M'$. For all $m \in 1_i M$ we get $\varphi(m) = \varphi(1_i m) = 1_i \varphi(m) = 1_i(1_j \varphi(m)) = (1_i 1_j)\varphi(m)$. But $1_i 1_j = 0$ as $i \neq j$. Therefore equality holds. □

V.4. Applicatons of the density theorems

Proposition V.21. *Let $k = \overline{k}$ be a field and A and k-algebra. Assume that $M_1, \ldots, M_s$ are finite-dimensional pairwise non-isomorphic irreducible A-modules. Then*

$$\begin{aligned} \hat{\Phi} \colon A &\to \bigoplus_{i=1}^{s} \mathrm{End}_k(M_i) \\ a &\mapsto ((m_1, \ldots, m_s) \mapsto (am_1, \ldots, am_s)) \end{aligned}$$

is surjective.

Proof. Clearly $\hat{\Phi}$ is well defined since multiplication with $a \in A$ is k-linear.

Now let $M = \bigoplus_{i \in I}^{s} M_i$. By Schur's lemma we have

$$\begin{aligned} \bigoplus_{i=1}^{s} \mathrm{End}_A(M_i) &\cong \mathrm{End}_A(M) \\ (\varphi_1, \ldots, \varphi_s) &\mapsto \hat{\varphi} \colon (m_1, \ldots, m_s) \mapsto (\varphi_1(m_1), \ldots, \varphi_s(m_s)). \end{aligned}$$

and since k is algebraically closed one has $\mathrm{End}_A(M_i) \cong k$ by $\lambda \,\mathrm{id}_{M_i} \leftarrow\!\shortmid \lambda$. Thus $End_A(M) = k^s$ as rings where $(\lambda_1, \ldots, \lambda_s)$ acts on $M = \bigoplus_{i=1}^{s} M_i$ by multiplication. By Corollary V.13 (since M_i and then M are finite-dimensional) we get a surjective map $\Phi \colon A \to \mathrm{End}_{\mathrm{End}_A(M)}(M)$. But as $\mathrm{End}_A(M) = k^s$ and $k^s \cong \prod_{i=1}^{s} \mathrm{End}_k(M_i)$ by Lemma V.19 4) we get $\Phi = \hat{\Phi}$. □

Proposition V.22. *Let K be a field and A be a finite-dimensional k-algebra.*

1) *Any irreducible A-module is finite-dimensional.*

2) *If $k = \overline{k}$ then A has only finitely many irreducible A-modules up to isomorphism.*

Proof.

1) If M is an irreducible A-module then there exists a surjective A-module homorphism $A \to M$. We have $\dim_k M \leq \dim_k A < \infty$.

2) Let L_i ($1 \leq i \leq r$ be pairwise non-isomorphic A-modules. As $k = \overline{k}$ and the L_i are finite-dimensional by 1) we can apply Proposition V.21 to get a surjection $A \to \bigoplus_{i=1}^r \operatorname{End}_k(L_i)$. But the $\operatorname{End}_k(L_i)$ are finite-dimensional because the L_i are irreducible. We now have a surjection $A \to \bigoplus_{i=1}^r k^{\dim L_i}$. Thus $r \leq \dim_k A$, so the number of irreducible A-modules (up to isomorphism) is less than $\dim_k A$. □

Definition. Let R be a ring (not necessarily with 1). Then R^{op} denotes the opposite ring (i.e. $R^{\mathrm{op}} = R$ as abelian groups but with multiplication $a \circ_{\mathrm{op}} b = ba$.

Facts.

1) R is unitary iff R^{op} is unitary.
2) $(R^{\mathrm{op}})^{\mathrm{op}} = R$
3) $R^{\mathrm{op}} = R$ iff R is commutative.
4) D is a skew field iff D^{op} is a skew field.
5) $\left(\prod_{i=1}^s R_i\right)^{\mathrm{op}} = \prod_{i=1}^s R_i^{\mathrm{op}}$ for rings R_i ($1 \leq i \leq s$).

Lemma V.23. *Let D be a skew field and and $n \in \mathbb{N}$. Then*

$$\begin{array}{rccl} \alpha\colon & \mathrm{M}_{n\times n}(D) & \to & (\mathrm{M}_{n\times n}(D^{\mathrm{op}}))^{\mathrm{op}} \\ & A & \mapsto & A^T \end{array}$$

is an isomorphism of rings.

Proof.

$$(\alpha(AB))_{ij} = ((AB)^T)_{ij} = \sum_{k=1}^n a_{jk}b_{ki}$$

$$(\alpha(A)_{ij}\alpha(B))_{ij} = (A^T \circ_{\mathrm{op}} B^T)_{ij} = (B^T A^T)_{ij} = \sum_{k=1}^n b_{ki} \circ_{\mathrm{op}} a_{jk} = \sum_{k=1}^n a_{jk}b_{ki}$$

□

Lemma V.24. *Let R be a ring with 1. Then*

$$\begin{array}{rccl} \Phi\colon & \operatorname{End}_R(R) & \cong & R^{\mathrm{op}} \\ & r & \mapsto & (r' \mapsto r'r) \\ & f(1) & \leftarrow\!\shortmid & f. \end{array}$$

Proof. Obviously, Φ is well-defined, has an inverse and is additive. We have to show that Φ is multiplicative.

$$\Phi(r \circ_{\mathrm{op}} s)(x) = \Phi(sr)(x) = x(sr) = \Phi(r)(xs) = (\Phi(r) \circ \Phi(s)(x))(x)$$

□

Observation. Let D be a skew field. By Schur's lemma $\mathrm{End}_{\mathrm{M}_{n\times n}(D)}(D^n)$ (D^n is an irreducible module) is again a skew field. We want to study the connections between the two.

Special cases:

$n = 1$: $\mathrm{End}_D(D) \cong D^{\mathrm{op}}$.

$D = k$: We get $\mathrm{End}_{\mathrm{M}_{n\times n}(k)}(k^n) \cong k$ by $\lambda\,\mathrm{id}_{\mathrm{M}_{n\times n}(k)} \leftarrow\!\shortmid \lambda$ because

$$\begin{aligned}\mathrm{End}_{\mathrm{M}_{n\times n}(k)}(k^n) &= \{f \in \mathrm{End}_k(k^n) \mid \forall B \in \mathrm{M}_{n\times n}(k) : A_f B = BA_f\}\\ &\cong \{A \in \mathrm{M}_{n\times n}(k) \mid \forall B \in \mathrm{M}_{n\times n}(k) : AB = BA\}\\ &= \mathrm{Z}(\mathrm{M}_{n\times n}(k)) \cong k.\end{aligned}$$

Lemma V.25. *Let D be a skew field and $n \in \mathbb{N}$. Then*

$$\begin{aligned}\Phi\colon D^{\mathrm{op}} &\to \mathrm{End}_{\mathrm{M}_{n\times n}(D)}(D^n)\\ d &\mapsto \varphi_d\colon \begin{pmatrix} x_1\\ \vdots\\ x_n\end{pmatrix} \mapsto \begin{pmatrix} x_1 d\\ \vdots\\ x_n d\end{pmatrix}\end{aligned}$$

is an isomorphism of rings.

Proof. Let $\pi_i\colon D^n \to D$ be the projection onto the i-th component. Φ is well-defined as we have

$$\varphi_d\left(A\begin{pmatrix} x_1\\ \vdots\\ x_n\end{pmatrix}\right) = \begin{pmatrix} (\sum_{i=1}^n a_{1i}x_i)d\\ \vdots\\ (\sum_{i=1}^n a_{ni}x_i)d\end{pmatrix} = \begin{pmatrix} \sum_{i=1}^n a_{1i}(x_i d)\\ \vdots\\ \sum_{i=1}^n a_{ni}(x_i d)\end{pmatrix} = A\varphi_d\left(\begin{pmatrix} x_1\\ \vdots\\ x_n\end{pmatrix}\right).$$

Clearly, Φ is additive. We show that it is multiplicative.

$$\begin{aligned}\Phi(d_1 \circ_{\mathrm{op}} d_2)\left(\begin{pmatrix} x_1\\ \vdots\\ x_n\end{pmatrix}\right) &= \Phi(d_2 d_1)\left(\begin{pmatrix} x_1\\ \vdots\\ x_n\end{pmatrix}\right) = \begin{pmatrix} x_1 d_2 d_1\\ \vdots\\ x_n d_2 d_1\end{pmatrix} = (\varphi_{d_1} \circ \varphi_{d_2})\left(\begin{pmatrix} x_1\\ \vdots\\ x_n\end{pmatrix}\right)\\ &= (\Phi(d_1) \circ \Phi(d_2))\left(\begin{pmatrix} x_1\\ \vdots\\ x_n\end{pmatrix}\right)\end{aligned}$$

For injectivity assume that $\Phi(d_1) = \Phi(d_2)$. We get $d_1 = \pi_i(\varphi_{d_1}(e_i)) = \pi_i(\varphi_{d_2}(e_i)) = d_2$. For surjectivity let $f \in \mathrm{End}_{\mathrm{M}_{n\times n}(D)}(D^n)$. Then f is D-linear with $D \subseteq \mathrm{M}_{n\times n}(D)$ via $d \mapsto \mathrm{diag}(d, \dots, d)$. Let $d_i := \pi(f(e_i))$. Then $f(e_i) = f(E_{ij}e_i = d_i e_i$. Now we get

$$f\left(\begin{pmatrix} x_1\\ \vdots\\ x_n\end{pmatrix}\right) = \sum_{i=1}^n f(x_i e_i) = \sum_{i=1}^n x_i e_i d_i = \begin{pmatrix} x_i d_i\\ \vdots\\ x_n d_n\end{pmatrix}.$$

But for all i, j we have $d_i = \pi_i(f(e_i)) = \pi_i(f(E_{ij}e_j)) = \pi_i(E_{ij}f(e_j)) = \pi_i(E_{ij}e_j d_j) = d_j$. Thus $f = \Phi(d)$ with $d = d_1 = \ldots = d_n$. $\square$

Theorem V.26 (Artin-Wedderburn theorem)**.** *Let R be a semisimple ring with 1. Then there is an isomorphism of rings*

$$R \cong \mathrm{M}_{n_1\times n_1}(D_1) \times \cdots \times \mathrm{M}_{n_r\times n_r}(D_r)$$

for some $n_i \in \mathbb{N}$, $r \in \mathbb{N}$ and some skew fields D_i ($1 \leq i \leq r$). Moreover the $(n_1, D_1), \ldots, (n_r, D_r)$ are unique up to permutation and isomorphism of skew fields.

Corollary V.27. *Let R be a semisimple ring. Then R^{op} is semisimple.*

Proof. This follows from the Artin-Wedderburn theorem, Corollary V.20 and Lemma V.23. ☐

Corollary V.28. *Let A be a finite-dimensional semisimple k-algebra with $k = \overline{k}$. Then there exists an isomorphism of k-algebras $A \cong \mathrm{M}_{n_1\times n_1}(k) \times \ldots \times \mathrm{M}_{n_r\times n_r}(k)$ for some $n_i, r \in \mathbb{N}$.*

Proof. By the Artin-Wedderburn theorem we have $A \cong \mathrm{M}_{n_1\times n_1}(D_1) \times \cdots \times \mathrm{M}_{n_r\times n_r}(D_r)$ as rings and also as k-algebras (we will show this in the proof) for some skew fields D_i and $n_i, r \in \mathbb{N}$. It is finite-dimensional since A is finite-dimensional. Now $k = \overline{k}$ implies $D_i = k$ for all $1 \leq i \leq r$. ☐

Corollary V.29. *Let A be a finite-dimensional semisimple k-algebra with $k = \overline{k}$. Then A has finitely many pairwise non-isomorphic left ideals $I_1, \ldots, I_r$ and $A \cong \mathrm{M}_{n_1\times n_1}(I_1) \times \ldots \times \mathrm{M}_{n_r\times n_r}(I_r)$.*

[November 19, 2018]

[November 22, 2018]

Proof of the Artin-Wedderburn theorem.

Existence: As R is semisimple there exists a finite set I and irreducible R-modules L_i' ($i \in I$) such that $R \cong \bigoplus_{i\in I} L_i'$ by Proposition V.11. We group isomorphic summands and get $R \cong L_i^{\oplus n_1} \oplus \ldots \oplus L_r^{\oplus n_r}$ for irreducible pairwise non-isomorphic R-modules L_i and $n_i \in \mathbb{N}$ (isotypic decomposition).

By Schur's lemma $\mathrm{End}_R(L_i)$ is a skew field. We set $D_i := \mathrm{End}_R(L_i)^{\mathrm{op}}$. Using $\mathrm{End}_R(L_i^{\oplus n_i}) \cong \mathrm{M}_{n_i\times n_i}(\mathrm{End}_R(L_i)) \cong \mathrm{M}_{n_i\times n_i}(D_i^{\mathrm{op}})$ (as rings), Lemma V.23 and Lemma V.24 we get

$$\begin{aligned} R &\cong (R^{\mathrm{op}})^{\mathrm{op}} \cong (\mathrm{End}_R(R))^{\mathrm{op}} \\ &\cong \left(\mathrm{End}_R\left(L_i^{\oplus n_1} \oplus \ldots \oplus L_r^{\oplus n_r}\right)\right)^{\mathrm{op}} \\ &\cong (\mathrm{M}_{n_1\times n_1}(D_i^{\mathrm{op}}) \times \cdots \times \mathrm{M}_{n_r\times n_r}(D_i^{\mathrm{op}}))^{\mathrm{op}} \\ &\cong (\mathrm{M}_{n_1\times n_1}(D_i^{\mathrm{op}}))^{\mathrm{op}} \times \cdots \times (\mathrm{M}_{n_r\times n_r}(D_i^{\mathrm{op}}))^{\mathrm{op}} \\ &\cong \mathrm{M}_{n_1\times n_1}(D_1) \times \cdots \times \mathrm{M}_{n_r\times n_r}(D_r) \qquad (1) \end{aligned}$$

as rings.

Uniqueness: Assume

$$R \cong \mathrm{M}_{m_1\times m_1}(C_1) \times \cdots \times \mathrm{M}_{m_s\times m_s}(C_s) \tag{2}$$

for some skew fields C_i and $m_i, s \in \mathbb{N}$. By Corollary V.20 we have $r = |\mathrm{Irr}(R)| = s$ and $D_i \cong \mathrm{End}_R(L_i)^{\mathrm{op}}$ (see above) where $\mathrm{Irr}(R) = \{L_1, \ldots, L_r\}$. Now consider (2). The irreducible modules are exactly the irreducible $\mathrm{M}_{m_i\times m_i}(C_i)$-modules $C_i^{m_i}$ viewed as modules for (1) (use $\mathrm{Irr}(\mathrm{M}_{m_i\times m_i}(C_i)) \cong C^{m_i}$). But due to Lemma V.25 we have $\mathrm{End}_{\mathrm{M}_{m_i\times m_i}(C_i)}(C_i^{m_i}) \cong C_i^{\mathrm{op}}$. Thus there exists a permutation $\sigma \in S_r$ such that $D_i \cong C_{\sigma(i)}$ and also $n_i = m_{\sigma(i)}$ since the dimensions of the irreducible modules agree. □

Hence we proved: If $R \cong L_1^{\oplus n_1} \oplus \ldots \oplus L_r^{\oplus n_r}$ with irreducible pairwise non-isomorphic R-modules L_i then $|\mathrm{Irr}(R)| = r$ and

$$R \cong \mathrm{M}_{n_1\times n_1}(\mathrm{End}_R(L_1)^{\mathrm{op}}) \times \cdots \times \mathrm{M}_{n_r\times n_r}(\mathrm{End}_R(L_r)^{\mathrm{op}}).$$

Remark. If R is also a finite-dimensional k-algebra then $\mathrm{End}_R(L_i)$ is a divison algebra. All involved isomorphisms are linear, hence we get an algebra homomorphism.

Proof of Corollary V.29. As A is semisimple there exists an isomorphism $\varphi\colon A \cong L_1^{\oplus n_1} \oplus \ldots \oplus L_r^{\oplus n_r}$ where the L_i are irreducible pairwise non-isomorphic A-modules (r is finite since A is finite-dimensional). Then $\varphi^{-1}(L_i) \subseteq A$ is an A-submodule, hence a left ideal I_i of A and I is minimal, since L_i is irreducible. The I_i are pairwise non-isomorphic as the L_i are so. Moreover these must be all minimal ideals (up to isomorphism) since $A = \bigoplus_{i=1}^r I_i^{\oplus n_i}$ and by the Artin-Wedderburn theorem A has precisely r irreducible representations (up to isomorphism). □

Corollary V.30. *Let R be a simple ring. Then $R \cong \mathrm{M}_{n\times n}(D)$ as rings for some unique $n \in \mathbb{N}$ and (up to isomorphism) unique skew field D.*

Proof. As R is simple it is semisimple and $|\mathrm{Irr}(R)| = 1$. Then we apply the Artin-Wedderburn theorem. □

V.5. Application: Brauer groups

Definition. A k-algebra is *central-simple* if it is a finite-dimensional simple algebra and $\mathrm{Z}(A) = k$.

Examples. Consider $A = k$ or $A = \mathrm{M}_{n\times n}(k)$.

Lemma V.31. *Let A, B be finite-dimensional k-algebras. Then $\mathrm{Z}(A) \otimes \mathrm{Z}(B) = \mathrm{Z}(A \otimes B)$ (as subsets of $A \otimes B$).*

Proof.

"$\subseteq$" Clear.

"⊇" Let $z \in \mathrm{Z}(A \otimes B)$. We write $z = \sum_{i=1}^{n} a_i \otimes b_i$ where $a_i \in A$, $b_i \in B$ and the b_i are linearly independent. For all $a \in A$ we have

$$az = \sum_{i=1}^{n} aa_i \otimes b_i = (a \otimes 1)z = z(a \otimes 1) = \sum_{i=1}^{n} a_i a \otimes b_i$$

and $aa_i = a_i a$ for all $1 \leq i \leq n$ since the b_i are linearly independent. This implies $a_i \in \mathrm{Z}(A)$ for all $1 \leq i \leq n$, and similarly $b_i \in \mathrm{Z}(B)$ for all $1 \leq i \leq n$. Therefore $z = \sum_{i=1}^{n} a_i \otimes b_i \in \mathrm{Z}(A) \otimes Z(B)$. □

Lemma V.32. *Let A and B be central-simple algebras. Then $A \otimes B$ is central-simple.*

Proof. It is clear that $A \otimes B$ is finite dimensional. We have $\mathrm{Z}(A \otimes B) = \mathrm{Z}(A) \otimes \mathrm{Z}(B) = k \otimes k = k$. We still have to show that $A \otimes B$ is a simple algebra. It is enough to show that $A \otimes B$ is "simple" (i.e. 0 and $A \otimes B$ are the only two-sided ideals).

Now let $0 \neq I \subseteq A \otimes B$ be a two-sided ideal. We want to show that $I = A \otimes B$. Any $0 \neq u \in I$ can be written as $u = \sum_{i=1}^{n} a_i \otimes b_i$ where $a_i \in A$, $b_i \in B$ and the b_i are linearly independent. We pick u with a minimal such representation (with respect to n). Now $a_i \neq 0$ for all $1 \leq i \leq n$ and $Aa_1A = A$ because A is simple and therefore "simple". Hence there exist $c, c' \in A$ with $ca_1c' = 1$. Let $x := (c \otimes 1)a(c' \otimes 1) = \sum_{i=1}^{n} ca_ic' \otimes b$ and we have $x = 1 \otimes b_1 + a'_2 \otimes b_2 + \ldots + a'_n \otimes b_n$ for some $a'_i \in A$. Note that $x \neq 0$ since the b_i are linearly independent. We get

$$(a \otimes 1)x - x(a \otimes 1) = (aa'_2 - a'_2 a) \otimes b_2 + \ldots + (aa'_n - a'_n a) \otimes b_n = 0$$

by assumption for all $a \in A$. Thus $aa'_i - a'_i a = 0$ for all $2 \leq i \leq n$ since the b_i are linearly independent and $a'_i \in \mathrm{Z}(A) = k$ since A is central simple. Now we can write $x = 1 \otimes b$ for some $b \in B$ ($b \neq 0$ as $x \neq 0$). We have $BbB = B$ since B is simple and hence "simple". This implies $I \supseteq (1 \otimes B)x(1 \otimes B) = I \otimes B$ and $I \supseteq (A \otimes 1)(1 \otimes B) = A \otimes B$. Therefore we get $I = A \otimes B$. □

Definition. Let A and B be central-simple algebras. We call A and B *Brauer equivalent* ($A \sim B$) if $A \cong \mathrm{M}_{n \times n}(D)$ and $B \cong \mathrm{M}_{m \times m}(C)$ with $C \cong D$ as skew fields.

Definition. The *Brauer group* $\mathrm{Br}(k)$ (k a field) has the equivalence classes of $\sim$ as elements. The composition is given by $[A] \circ [B] = [A \otimes B]$. The neutral element is $[k]$, and the inverse of $[A]$ is $[A^{\mathrm{op}}]$.

Proof that $\mathrm{Br}(k)$ *is indeed a group.* By Lemma V.32 $A \otimes B$ is again central-simple, hence $[A] \circ [B] = [A \otimes B]$ is defined. The reader may check that $[A] \circ [B]$ is independent of the choice of the representants.

The composition is commutative ($A \otimes B \cong B \otimes A$). Thus $\mathrm{Br}(k)$ is abelian.

k is the neutral element, since $[A \otimes k] = [A]$.

For the inverse we use the folowing claim: For any finite-dimensional central-simple algebra A with $n = \dim_k A$ we have an isomorphism

$$\begin{aligned} \gamma\colon A \otimes A^{\mathrm{op}} &\cong \mathrm{End}_k(A) \\ a \otimes b &\mapsto (x \mapsto axb). \end{aligned}$$

We check that γ is injective. Obviously $\gamma \neq 0$. $\ker \gamma$ is a two-sided ideal (the calculation is left to the reader). But A and A^{op} and hence $A \otimes A^{\mathrm{op}}$ are central-simple, thus $\ker \varphi = 0$. As $\dim_k(A \otimes A^{\mathrm{op}}) = \dim_k(\mathrm{End}_k(A))$ we get that γ is indeed bijective. □

Examples. Let k be an algebraically closed field. By the ARTIN-WEDDERBURN THEOREM we get $\mathrm{Br}(k) = \{[k]\}$.

Without going into detail one has $\mathrm{Br}(\mathbb{R}) = \{[\mathbb{R}], [\mathbb{H}]\} \cong \mathbb{Z}/2\mathbb{Z}$.

[November 22, 2018]

[November 26, 2018]

VI. The double centralizer theorem

Definition. Let k be a field, W a k-vector space and $S \subseteq \mathrm{End}_k(W)$ a subset. Then

$$S' := \{\varphi \in \mathrm{End}_k(W) \mid \forall s \in S : \varphi \circ s = s \circ \varphi\}$$

is the *commutant* or *centralizer* of S in $\mathrm{End}_k(W)$. We abbreviate $(S')' = S''$ and so on.

Facts.

1) $S' \subseteq \mathrm{End}_k(W)$ is a subalgebra.
2) Let $T \subseteq S \subseteq \mathrm{End}_k(W)$ be subsets. Then $S' \subseteq T'$.
3) $S \subseteq T' \Rightarrow T \subseteq S'$.
4) $S \subseteq S''$.
5) $S = S'''$.
6) $S = T' \Leftrightarrow T = S'$.

Proof.

1), 2) Clear.

3) $S \subseteq T' \Leftrightarrow \forall s \in S : \forall t \in T : st = ts \Leftrightarrow \forall t \in T : \forall s \in S st = ts \Leftrightarrow T \subseteq S'$.

4) $S' \subseteq S' \Rightarrow S \subseteq S''$.

5) $S' \subseteq (S')'' = S'''$ and $S \subseteq S''$ implies $(S'')' \subseteq S'$.

6) $S = T' \Rightarrow S'' = (T')'' = T' \Rightarrow T = S'$. □

Remark. Let V be an A-module (A a k-algebra) and also a B-module (B a k-algebra). If the actions of A and B commute (i.e. $ab = ba$ for all $a \in A, b \in B$) where $a \in$ and $b \in B$ denote the corresponding action in $\mathrm{End}_A(V)$ then V is an $A \otimes B$-module given by $a \otimes b.v = abv = bav$ for all $v \in V$. The reader may check the details.

Lemma VI.1. *Let A and B be k-algebras (k any field), M an A-module and N a B-module. Then $M \otimes N$ is an $A \otimes B$-module via $a \otimes b.m \otimes n = am \otimes bn$ for all $m \in M$ and $n \in N$.*

Proof. One could do explicit calculations, but we will give a better proof. M being an A-modue means a choice of an algebra homomorphism $\varphi\colon A \to \mathrm{End}_k(M)$. Similarly we get an algebra homomorphism $\psi\colon B \to \mathrm{End}_k(N)$. Then consider

$$\begin{tikzcd} A \otimes B \arrow[r, "\varphi\otimes\psi"] \arrow[dr, dashed] & \mathrm{End}_k(M) \otimes \mathrm{End}_k(N) \arrow[d, phantom, "\cong" rotate=-90] \\ & \mathrm{End}_k(M \otimes N). \end{tikzcd}$$

□

Example. Let G and H be groups with representations M and N over a fixed field k, respectively. Note that

$$\begin{array}{rcl} kG \otimes kH & \cong & k(G \otimes H) \\ g \otimes h & \mapsto & (g, h) \end{array}$$

as algebras. $M \otimes N$ is an $kG \otimes kH$-module and hence a representation of $G \otimes H$.

Theorem VI.2 (Double centralizer theorem)**.** *Let k be a field and W a finite-dimensional k-vector space. Let $A \subseteq \mathrm{End}_k(W)$ be a subalgebra. Then the following holds:*

1) *A' is a semisimple algebra (a subalgebra of $\mathrm{End}_k(W)$).*

2) *$A'' = A$.*

Now let k be algebraically closed.

3) *There is a decomposition of $A \otimes A'$-modules*

$$\Phi\colon W \cong \bigoplus_{i=1}^{r} L_i \otimes L'_i$$

(isomorphism as $A \otimes A'$-modules) such that $L_1, \dots, L_r$ are pairwise non-isomorphic irreducible A-modules and $L'_1, \dots, L'_r$ are pairwise non-isomorphic irreducible A'-modules.

4) *The $L_1, \dots, L_r$ and $L'_1, \dots, L'_r$ are precisely the irreducible A-modules and A'-modules up to isomorphism. Hence in particular $|\mathrm{Irr}(A)| = |\mathrm{Irr}(A')|$.*

Remark. More generally if k is an arbitrary field we can replace Φ by $\Phi'\colon W \cong \bigoplus_{i=1}^r L_i \otimes_{D_i} L_i'$ for division algebras $D_i := \mathrm{End}_A(L_i)$. Moreover this isomorphism is the isotypic decomposition for W as an A-module, but also as an A'-module.

Remark. Let A be a k-algebra, M an A-module and N a k-vector space. Then Lemma VI.1 gives an A-module structure on $M \otimes N$ (A-modules are $A \otimes k$-modules), the *multiplicity space*. Note that $M \otimes N \cong M^{\bigoplus \dim N}$ as A-modules if N is finite-dimensional. To see this choose bases $\{m_i\}$ of M and $\{n_i\}$ of N and send $m_i \otimes n_j$ to $\delta_j m_i$.

Proof of the Double centralizer theorem. As A is a semisimple algebra any A-module is semisimple. We get

$$W \cong \bigoplus_{i=1}^{s} L_i^{\oplus n_i} \tag{*}$$

for some $n_i, s \in \mathbb{N}$ and pairwise non-isomorphic irreducible A-modules L_i.

1. $s = |\mathrm{Irr}(A)|$.

   By the Artin-Wedderburn theorem we have $A \cong \prod_{i=1}^r R_i$ for some $m \in \mathbb{N}$ and $R_i \cong \mathrm{M}_{m_i \times m_i}(C_i)$ where C_i is a division algebra and the (m_i, C_i) are unique up to permutation and isomorphism of division algebras. Then $|\mathrm{Irr}(A)| = m$ and so $s \leq m$ (by definition of s). Since $A \subseteq \mathrm{End}_k(W)$ is a subalgebra with have that $1_i W \neq 0$ for any $1 \leq i \leq s$ (1_i is the unit in R_i). Therefore $1_i W$ contains an irreducible R_i-module. For any irreducible R_i-module U_i ($1 \leq i \leq s$) there is an R-submodule in W which is isomorphic to U_i as an R_i-module. Thus $s = m$ and $|\mathrm{Irr}(A)| = s$.

2. A' is a semisimple algebra and $|\mathrm{Irr}(A')| = |\mathrm{Irr}(A)|$.

   Using the Artin-Wedderburn theorem, Schur's lemma and (*) we get an isomorphism of algebras

$$\begin{aligned} A' &= \{b \in \mathrm{End}_k(W) \mid \forall a \in A\colon ba = ab\} = \mathrm{End}_A(W) \\ &\cong \prod_{i=1}^{s} \mathrm{M}_{n_i \times n_i}(\mathrm{End}_A(L_i)) = \prod_{i=1}^{S} \mathrm{M}_{n_i \times n_i}(D_i) \end{aligned}$$

   where $D_i := \mathrm{End}_A(L_i)$ are division algebras. By Corollary V.20 A' is semisimple and $|\mathrm{Irr}(A')| = |\mathrm{Irr}(A)|$.

3. If $U \subseteq W$ is an irreducible A-module, then $\mathrm{Hom}_A(U, W)$ is an irreducible A'-module with action given by $(\beta.f)(u) = \beta(f(u))$ for $f \in \mathrm{Hom}_A(U, W)$, $\beta \in A'$ and $u \in U$.

   This action is well-defined as we have

$$(\beta.f).(au) = \beta(f(au)) = \beta(af(u)) = a\beta(f(u)) = a(\beta.f)(u).$$

   For irreducibility it is enough to show that for any nonzero $f_1, f_2 \in \mathrm{Hom}_A(U, W)$ there exists a $\beta \in A'$ such that $\beta.f_1 = f_2$. For $0 \neq u \in U$ set $v_1 := f_1(u)$ and

$v_2 := f_2(u)$. Since W is semisimple we get $W = Av_1 \oplus C$ for some A-module C. Now define

$$\begin{aligned} \beta\colon W = Av_1 \oplus C &\to W \\ av_1 &\mapsto v_2 \\ c &\mapsto c. \end{aligned}$$

This is obviously k- and A-linear, hence $\beta \in A'$. Now $(\beta.f_1)(u) = \beta(f_1(m)) = v_2 = f_2(u)$ and thus $f_1(au) = f_2(au)$ for all $a \in A$ because β and f_1 are A-linear. As U is irreducible we get $\beta f_1 = f_2$.

4. $L_i' \cong \operatorname{Hom}_A(L_i, W)$ is an irreducible A'-module by 3.. Since L_i is a left D_i-module, L_i' is a right D_i-module and hence a left D_i^{op}-module. Therefore $L_i \otimes_{D_i^{\mathrm{op}}} L_i'$ makes sense.

5. $L_i \otimes_{D_i^{\mathrm{op}}} L_i'$ is an $A \otimes A'$-module via $(a \otimes b).(m \otimes n) = am \otimes bn$ for all$m \in M$, $n \in N$, $a \in A$ and $b \in A'$.

   If k is algebraically closed then $D_i = k = D_i^{\mathrm{op}}$ and it is clear by Lemma VI.1. For the general case we have to check that the action is well-defined. Let $\varphi \in D_i^{\mathrm{op}}$, $f \in L_i'$, $a \in A$ and $b \in A'$. On the one hand, we have

$$(a \otimes b)(x\varphi \otimes f) = (a \otimes b)(\varphi(x) \otimes f) = a\varphi(x) \otimes bf,$$

   on the other hand,

$$\begin{aligned} (a \otimes b)(x \otimes \varphi f) &= (a \otimes b)(x \otimes (f \circ \varphi)) = (ax \otimes (f \circ \varphi)) = ax \otimes (bf)(\varphi) \\ &= ax \otimes \varphi.(bf) = ax \otimes \otimes bf = \varphi(ax) \otimes bf = a\varphi(x) \otimes bf. \end{aligned}$$

6. The map

$$\begin{aligned} \Phi_i\colon L_i \otimes_{D_i^{\mathrm{op}}} L_i' &\to W \\ x \otimes f &\mapsto f(x) \end{aligned}$$

   is an A-module homomorphism (since $\Phi_i(ax \otimes f) = f(ax) = af(x) = a\Phi_i(x \otimes f)$. By Schur's lemma we have $\operatorname{im}\Phi_i \subseteq \operatorname{Iso}_{L_i}(W)$. We claim $\operatorname{im}\Phi_i = \operatorname{Iso}_{L_i}(W)$.

   Let $f_1, \ldots, f_s$ be a basis of $\operatorname{Hom}_A(_i, W) \cong \bigoplus_{i=1}^s L_i^{\otimes n_i}$. Then

$$f_i(x) = \begin{cases} x_i := (0, \ldots, 0, x, 0, \ldots, 0) & \text{if } f_i \text{ is contained in the } i\text{-th copy of } L_i' = \bigoplus_{i=1}^{n_i} \operatorname{Hom}_A(L_i, L_i), \\ 0 & \text{otherwise.} \end{cases} \in L_i^{\oplus n_i}$$

7. Φ_i is injective and we get an isomorphism

$$\begin{aligned} \Phi := \bigoplus_{i=1}^s \Phi_i\colon \bigoplus_{i=1}^s L_i \otimes_{D_i^{\mathrm{op}}} L_i' &\to W \\ x_i \otimes f_i &\mapsto f_i(x_i) \end{aligned}$$

and moreover Φ_i and Φ are $A \otimes A'$-module homomorphisms.

First, assume that k is algebraically closed. Then by 6. Φ_i is surjective and we have

$$\dim(L_i \otimes L_i') = (\dim L_i) \underbrace{(\dim L_i')}_{n_i} = \dim \underbrace{L_i^{\oplus n_i}}_{\mathrm{Iso}_{L_i}(W)} .$$

Thus Φ_i and then Φ is bijective.

Now let k be arbitrary. By 3. L_i' is an irreducible A'-module on $\mathrm{M}_{n_i \times n_i}(D_i)$ (see 2. acts non-trivially. We get $L_i' \cong D_i^{n_i}$ as $\mathrm{M}_{n_i \times n_i}(D_i)$-modules. In particular one has $L_i \otimes_{D_i^{\mathrm{op}}} D_i^{n_i} \cong L_i^{\oplus n_i}$ and we get $\dim(L_i \otimes_{D_i^{\mathrm{op}}} D_i^{n_i} = n_i \dim L_i = \dim \mathrm{Iso}_{L_i}(W)$.

We still have to show that Φ is an homomorphism of $A \otimes A'$-modules. It suffices to show that the Φ_i are $A \otimes A'$-module homomorphisms. Let $x_i \in L_i$, $f_i \in L_i'$, $a \in A$ and $b \in A'$. Then

$$\begin{aligned}
\Phi_i(a.(x_i \otimes f_i)) &= \Phi_i(ax_i \otimes f_i) = f_i(ax_i) = af_i(x_i) = a.\Phi_i(x_i \otimes f_i) \\
&= \Phi_i(b.(x_i \otimes f_i)) = \Phi(x_i \otimes bf_i) = (bf_i)(x_i) = b.f_i(x_i) \\
&= b.\varphi(x_i \otimes f_i).
\end{aligned}$$

8. $A = A''$.

   It is clear that $A \subseteq A''$. As A is semisimple we have $A \cong \prod_{i=1}^{s} \mathrm{M}_{m_i \times m_i}(C_i)$ by the ARTIN-WEDDERBURN THEOREM for some division algebras C_i, $n_i \in \mathbb{N}$ and $r = |\mathrm{Irr}(A)|$. Also $W \cong \bigoplus_{i=1}^{s} L_i^{n_i}$ and we get $L_i \cong C_i^{m_i}$ after renumbering. Now

$$D_i = \mathrm{End}_A(L_i) \cong \mathrm{End}_{\prod_{j=1}^{s} \mathrm{M}_{m_j \times m_j}(C_j^{m_j})}(C_i^{m_i}) = \mathrm{End}_{\mathrm{M}_{m_i \times m_i}(C_i)}(C_i^{m_i}) = C_i^{\mathrm{op}}.$$

   By 2. one has

$$A' = \prod_{i=1}^{s} \mathrm{M}_{n_i \times n_i}(D_i) \cong \prod_{i=1}^{s} \mathrm{M}_{n_i \times n_i}(C_i^{\mathrm{op}}).$$

   We can now apply the same argument for A' instead of A and get

$$A'' \cong \prod_{i=1}^{s} \mathrm{M}_{q_i \times q_i}((C_i^{\mathrm{op}})^{\mathrm{op}}) \quad \text{and} \quad W \cong \bigoplus_{j=1}^{s} (L_i')^{q_i}$$

   as A-modules. But by 7. we have

$$W \cong \bigoplus_{i=1}^{s} L_i \otimes_{D_i^{\mathrm{op}}} L_i' \cong \bigoplus_{i=1}^{s} C_i^{m_i} \otimes_{C_i} L_i' \cong \bigoplus_{i=1}^{s} (L_i')^{m_i}$$

   and therefore $a_i = m_i$ for all $1 \leq i \leq s$. Therefore $A \cong A''$, which implies $A = A''$ as they are finite-dimensional and $A \subseteq A''$. □

[November 26, 2018]

[November 29, 2018]

Corollary VI.3. *Let G and H be finite groups and k an algebraically closed field with* $\operatorname{char} k \nmid |G| \cdot |H|$. *Then for any two irreducible finite-dimensional representations V of G and W of H we have an irreducible representation $V \otimes W$ of $G \times H$ given by $(g,h)(v \otimes w) = gv \otimes hw$. Every irreducible finite-dimensional representation of $G \times H$ is of this form.*

Proof. Consider the algebra homomorphisms $kG \to \operatorname{End}_k(V)$ and $kH \to \operatorname{End}_k(W)$. As V and W are irreducible and finite-dimensional they are surjective. Now

$$\begin{array}{ccc} kG \otimes kH & \twoheadrightarrow & \operatorname{End}_k(V) \otimes \operatorname{End}_k(W) \\ \wr\| & & \wr\| \\ k(G \times H) & \twoheadrightarrow & \operatorname{End}_k(V \otimes W). \end{array}$$

Thus $V \otimes W$ is an irreducible representation of $G \otimes H$.

The converse (to be shown using the Double centralizer theorem) is left to the reader. ☐

Motivation and applications of the next result

Let $k = \mathbb{C}$, $V = \mathbb{C}^2$ and v_1, v_2 the standard basis. Consider two actions on $V \otimes V$:

- Let $G = \operatorname{GL}(V) = \operatorname{GL}_2(\mathbb{C})$ act on V in a natural way. Consider the action on $V \otimes V$ by $g.(v \otimes w) = gv \otimes gw$ for $g \in G$ and $v, w \in V$. This yields a group homomorphism

$$\begin{aligned} \alpha\colon \operatorname{GL}(V) &\to \operatorname{GL}(V \otimes V) \subseteq \operatorname{End}_k(V \otimes V) \\ g &\mapsto \alpha(g)\colon v \otimes w \mapsto gv \otimes gw. \end{aligned}$$

  Let $\langle \operatorname{GL}(\langle v \rangle) \rangle$ be the subalgebra of $\operatorname{End}_k(V \otimes V$ generated by $\operatorname{im} \alpha = \operatorname{im}(k \operatorname{GL}(V) \to \operatorname{End}_k(V \otimes V))$.

- Define an action of $S_2 = \{e, s\}$ on $V \otimes V$ by $s.(v \otimes w) = w \otimes v$. Consider the group homomorphism

$$\beta\colon S_2 \to \operatorname{GL}(V \otimes V) \subseteq \operatorname{End}_k(V \otimes V).$$

  Let $\langle S_2 \rangle$ be the subalg of $\operatorname{End}_k(V \otimes V)$ generated by $\operatorname{im} \beta = \operatorname{im}(kS_2 \to \operatorname{End}_k(V \otimes V)$.

Note that for $g \in \operatorname{GL}(V)$ we have

$$(\alpha(g) \circ \beta(s))(v \otimes w) = \alpha(g(w \otimes v)) = gw \otimes gv = (\beta(s) \circ \alpha(g))(v \otimes w).$$

and hence $\operatorname{im} \alpha \subseteq (\operatorname{im} \beta)' = \langle S_2 \rangle'$ or $\langle \operatorname{GL}(V) \rangle \subseteq \langle S_2 \rangle'$. One can show that equality holds.

Decompose $V \otimes V$ as a representation of S_2.

$$V \otimes V = \mathbb{C}(v_1 \otimes v_1) \oplus \mathbb{C}(v_2 \otimes v_2) \oplus \mathbb{C}(v_1 \otimes v_2 + v_2 \otimes v_1) \oplus \mathbb{C}(v_1 \otimes v_2 - v_2 \otimes v_1).$$

The first three summands are isomorphic to triv (the 1-dimensional trivial representation) and the last one is isomorphic to sign (the 1-dimensional sign representation). Therefore (using multiplicity spaces)

$$V \otimes V \cong \mathrm{triv} \oplus \mathrm{triv} \oplus \mathrm{triv} \oplus \mathrm{sign} \cong \mathrm{triv} \otimes \mathbb{C}^3 \oplus \mathrm{sign} \otimes \mathbb{C}.$$

Decompose $V \otimes V$ as a representation of $\mathrm{GL}(V)$. Consider

$$\begin{aligned} S^2V &= \left(\mathrm{T}(v)/(v\otimes w - w \otimes v)\right)_2 = V\otimes V/(v\otimes w - w\otimes v), \\ \Lambda^2 V &= \left(\mathrm{T}(v)/(v\otimes w + w \otimes v)\right)_2 = V\otimes V/(v\otimes w + w\otimes v). \end{aligned}$$

One can see

$$S^2V \cong \langle v_1 \otimes v_1, v_2 \otimes v_2, v_1 \otimes v_2 + v_2 \otimes v_1\rangle \quad \text{and} \quad \Lambda^2 V \cong \langle v_1 \otimes v_2 - v_2 \otimes v_1\rangle$$

as representations of $\mathrm{GL}(V)$.

We get a decomposition of $V \otimes V$ as a representation of $S_2 \otimes \mathrm{GL}(V)$ (or as $\langle S_2\rangle \otimes \langle \mathrm{GL}(V)\rangle$-modules)

$$V \otimes V \cong \mathrm{triv} \otimes S^2V \oplus \mathrm{sign} \otimes \Lambda^2 V.$$

One can show that S^2V and Λ^2V are irreducible representations of $\mathrm{GL}(V)$. Then the above decomposition is the decomposition into isotypic components.

Generalization. Let k be any field, V a finite-dimensional k-vector space and $d \in \mathbb{Z}_{\geq 0}$. Consider $V^{\otimes d}$ as a representation of $\mathrm{GL}(V)$ via $g(v_1 \otimes \ldots \otimes v_d) = gv_1 \otimes \ldots \otimes gv_d$. Let $\alpha\colon \mathrm{GL}(V) \to \mathrm{GL}(V^{\otimes d}) \subseteq \mathrm{End}_k(V^{\otimes d})$ and $\langle \mathrm{GL}(v)\rangle$ be the subalgebra generated by $\operatorname{im}\alpha$. $V^{\otimes d}$ becomes a representation of S_d via $\sigma(v_1 \otimes \ldots \otimes v_d) = v_{\sigma^{-1}(1)} \otimes \ldots \otimes v_{\sigma^{-1}(d)}$. Consider the group homomorphism $\beta\colon S_d \to \mathrm{GL}(V^{\otimes d}) \subseteq \mathrm{End}_k(V^{\otimes d})$ and the subalgebra $\langle S_d\rangle$ generated by $\operatorname{im}\beta$. For $g \in \mathrm{GL}(V)$ and $\sigma \in S_d$ we obtain

$$(\alpha(g) \circ \beta(\sigma))(v_1 \otimes \ldots \otimes v_d) = (\beta(\sigma) \circ \alpha(g))(v_1 \otimes \ldots \otimes v_d)$$

and thus $\langle \mathrm{GL}(V)\rangle \subseteq \langle S_d\rangle'$ and $\langle S_d\rangle \subseteq \langle \mathrm{GL}(V)\rangle'$.

Theorem VI.4 (Schur-Weyl duality)**.** *Let k be an infinite field, V a finite-dimensional k-vector space and $d \in \mathbb{Z}_{\geq 0}$.*

1) $\mathrm{End}_{S_d}(V^{\otimes d}) = \langle \mathrm{GL}(V)\rangle$.

2) *If* $\operatorname{char} k = 0$ *or* $\operatorname{char} k > d$ *we have* $\mathrm{End}_{\mathrm{GL}(V)}(V^{\otimes d}) = \langle S_d\rangle$.

[November 29, 2018]

[December 3, 2018]

Remark. Assume that $\operatorname{char} k = 0$ or $\operatorname{char} k > d$. Then it follows from the Schur-Weyl duality that the double commutant property holds, as we have $\langle \mathrm{GL}(V)\rangle'' = \operatorname{End}_{\mathrm{GL}(V)}\left(V^{\otimes d}\right)' = \langle S_d\rangle' = \operatorname{End}_{S_d}(V^{\otimes d})$ and similarly $\langle S_d\rangle'' = \langle S_d\rangle$.

Proof.

1) The isomorphism of isomorphism of vector spaces

$$\begin{aligned} \Phi\colon \operatorname{End}_k(V)^{\otimes d} &\to \operatorname{End}_k\left(V^{\otimes d}\right) \\ f_1 \otimes \ldots \otimes f_d &\mapsto (v_1 \otimes \ldots \otimes v_d \mapsto f_1(v_1) \otimes \ldots f_d(v_d)) \end{aligned}$$

is S_d-equivariant where S_d acts on $\operatorname{End}_k\left(V^{\otimes d}\right)$ by $(\sigma f)(x) = \sigma(f(\sigma^{-1}x))$ with $\sigma \in S_d$, $x \in V^{\otimes d}$ and $f \in \operatorname{End}_k\left(V^{\otimes d}\right)$ and on $\operatorname{End}_k(V)^{\otimes d}$ by $\sigma(f_1 \otimes \ldots \otimes f_d) = f_{\sigma^{-1}(1)} \otimes \ldots \otimes f_{\sigma^{-1}(d)}$. To show this take $\sigma \in S_d$. On the one hand,

$$\begin{aligned} \Phi(\sigma f)(v_1 \otimes \ldots \otimes v_d) &= \Phi\Big(f_{\sigma^{-1}(1)} \otimes \ldots \otimes f_{\sigma^{-1}(d)}\Big)(v_1 \otimes \ldots \otimes v_d) \\ &= f_{\sigma^{-1}(1)}(v_1) \otimes \ldots \otimes f_{\sigma^{-1}(d)}(v_d), \end{aligned}$$

and on the other hand,

$$\begin{aligned} (\sigma\Phi(f))(v_1 \otimes \ldots \otimes v_d) &= \sigma\Big(\Phi(f)(v_{\sigma(1)} \otimes \ldots \otimes v_{\sigma(d)})\Big) \\ &= \sigma\Big(f_1(v_{\sigma(1)}) \otimes \ldots \otimes f_d(v_{\sigma(d)})\Big) \\ &= f_{\sigma^{-1}(1)}(v_1) \otimes \ldots \otimes f_{\sigma^{-1}(d)}(v_d). \end{aligned}$$

Corollary VI.5. *Φ induces an isomorphism of k-vector spaces*

$$\left(\operatorname{End}_k(V)^{\otimes d}\right)^{S_d} \cong \left(\operatorname{End}_k\left(V^{\otimes d}\right)\right)^{S_d} = \operatorname{End}_{S_d}\left(V^{\otimes d}\right).$$

Proof. Take invariants for the isomorphism above. □

Now $\langle \mathrm{GL}(V)\rangle \subseteq \operatorname{End}_{S_d}\left(V^{\otimes d}\right) = S_d'$ by definition since the $\mathrm{GL}(V)$- and the S_d-action commute. The image of the map

$$\begin{aligned} F\colon \mathrm{GL}(V) &\to \operatorname{Aut}\left(V^{\otimes d}\right) \subseteq \operatorname{End}_k\left(V^{\otimes d}\right) \cong \operatorname{End}_k(V)^{\otimes d} \\ \varphi &\mapsto \varphi^{\otimes d} \end{aligned}$$

is obviously contained in $\left(\operatorname{End}_k(V)^{\otimes d}\right)^{S_d}$. It is now enough to see that the image of $\langle \mathrm{GL}(V)\rangle$ is the whole of $\operatorname{End}_k\left(V^{\otimes d}\right)^{S_d} = \operatorname{End}_{S_d}\left(V^{\otimes d}\right)$. Now $E := \operatorname{End}_k(V)$ is a finite-dimensional vector space and $\mathrm{GL}(V) \subseteq E$ is a Zariski-dense subset. Then by Lemma VI.6 we get an isomorphism of vector spaces $\langle \mathrm{GL}(V)\rangle \cong \left(\operatorname{End}_k(V)^{\otimes d}\right)^{S_d} \cong \operatorname{End}_{S_d}\left(V^{\otimes d}\right)$ via F and Φ.

2) As $\operatorname{char} k \nmid |S_d| = d!$, kS_d is a semisimple algebra, and $A := \langle S_d \rangle$ is semisimple (note that $\langle S_d \rangle$ is a quotient of kS_d). By 1) we get $A' = \operatorname{End}_{S_d}\left(V^{\otimes d}\right) = \langle \mathrm{GL}(V) \rangle$. Thus $\operatorname{End}_{\mathrm{GL}(V)}\left(V^{\otimes d}\right) = \langle \mathrm{GL}(V) \rangle' = A'' = A$ be the DOUBLE CENTRALIZER THEOREM. $\square$

Lemma VI.6. *Let k be an infinite field, $d \geq 1$, E a finite-dimensional vector space and $X \subseteq E$ a Zariski-dense subset (over k). Then the vector space $\left(E^{\otimes d}\right)^{S_d}$ (the vector space of symmetric tensors) is generated as a vector space by the elements $\left\{x^{\otimes d} \,\middle|\, x \in X\right\} \subseteq \left(E^{\otimes d}\right)^{S_d}$.*

Proof. Let $e_1, \ldots, e_n$ be a basis of E. Then $B = \{e_{i_1} \otimes \ldots \otimes e_{i_d} \mid 1 \leq i_j \leq n\}$ is a k-basis of $E^{\otimes d}$. Obviously B is an invariant subset of $E^{\otimes d}$ under S_d-action (by permuting the factors). Two vectors from B are in the same S_d-orbit if and only if the number of factors equal to e_i agree in the two basis vectors for each i. In particular every orbit contains a (unique) element of the form $e^\mu = e_1^{\otimes \mu_1} \otimes \ldots \otimes e_n^{\otimes \mu_n}$ for some $\mu = (\mu_1, \ldots, \mu_n) \in \mathbb{N}_0^n$ with $\sum_{i=1}^n \mu_i = d$. Let $a^\mu := \sum_{\omega \in S_d / S_{\mu_1} \times \ldots \times S_{\mu_n}} \omega(e^\mu)$. It is easy to see that $\{a^\mu \mid \mu \in \mathbb{N}_0^n, \sum_{i=1}^n \mu_1 = d\}$ forms a basis of $\left(E^{\otimes d}\right)^{S_d}$.

Let $\mathrm{Sym} := \left(E^{\otimes d}\right)^{S_d}$ and $U := \left\{x^{\otimes d} \,\middle|\, x \in X\right\}$. We have to show that $U = \mathrm{Sym}$.

"$\subseteq$" Obvious.

"$\supseteq$" It is enough to show that if $f\colon \mathrm{Sym} \to k$ is k-linear then $f|_u = 0$ implies $f = 0$. To see this, assume $U \subsetneq \mathrm{Sym}$ and pick a basis $\{u_i \mid i \in I\}$ of U and extend it by u_j $(j \in J)$ to a basis of Sym. Then

$$f(u_s) = \begin{cases} 0 & \text{if } s \in I \\ 1 & \text{if } s \in J \end{cases}$$

with $s \in I \cup J$ defines a map $\mathrm{Sym} \to k$ such that $f|_U = 0$ but $f \neq 0$.

Let now $f\colon \mathrm{Sym} \to k$ be k-linear such that $f|_U = 0$. Then $f(x \otimes \ldots \otimes x) = 0$ for all $x \in X$. Write $x = \sum_{i=1}^n x_i e_i$. Then

$$x \otimes \ldots \otimes x = \sum_{\substack{\mu \in \mathbb{N}_0^n, \\ \sum_{i=1}^n \mu_i = d}} x_1^{\mu_1} \cdots x_n^{\mu_n} a^\mu.$$

Consider $p \in \mathcal{P}_k(E)$ defined by

$$p\left(\sum_{i=1}^n y_i e_i\right) = \sum_{\substack{\mu \in \mathbb{N}_0^n, \\ \sum_{i=1}^n \mu_i = d}} f(a^\mu) y_1^{\mu_1} \cdots y_n^{\mu_n}.$$

Then in particular

$$0 = f(x \otimes \ldots \otimes x) = \sum_{\substack{\mu \in \mathbb{N}_0^n, \\ \sum_{i=1}^n \mu_i = d}} f(x_1^{\mu_1} \cdots x_n^{\mu_n} a^\mu) = \sum_{\substack{\mu \in \mathbb{N}_0^n, \\ \sum_{i=1}^n \mu_i = d}} f(a^\mu) x_1^{\mu_1} \cdots x_n^{\mu_n} = p(x).$$

Therefore $p(x) = 0$ for all $x \in X$, and $p = 0$ (as an element in $\mathcal{P}_k(E)$). This implies $f(a^\mu) = 0$ for all $\mu \in \mathbb{N}_0^n$ with $\sum_{i=1}^n \mu_i = d$. Thus $f = 0$ since the a^μ form a basis of Sym. □

Corollary VI.7. *Let k be a field of* char $= 0$ *(in particular $|k| = \infty$). Let V be a finite-dimensional k-vector space and $d \in \mathbb{N}$. Then $V^{\otimes d}$ is a representation of $S_d \times \mathrm{GL}(V)$ and we have a decomposition of representations of $S_d \times \mathrm{GL}(V)$*

$$V^{\otimes d} \cong \bigoplus_{\lambda \in \Lambda} S_\lambda L(\lambda)$$

where S_λ are the pariwise non-isomorphic representations of S_d and the $L(\lambda)$ are the pariwise non-isomorphic representations of $\mathrm{GL}(V)$ *for some labelling set Λ. If* $\dim V \geq d$ *then $\{S_\lambda \mid \lambda \in \Lambda\} = \mathrm{Irr}(S_d)$.*

Proof. The DOUBLE CENTRALIZER THEOREM and the SCHUR-WEYL DUALITY imply all statements except of the last one by applying Lemma VI.8 to $kS_d \to \langle S_d \rangle$ and $k\,\mathrm{GL}(V) \to \langle \mathrm{GL}(V) \rangle$.

For the last statement assume $\dim_k V \geq d$. Then we can pick a basis $e_1, \ldots, e_n$ of V $(n \geq d)$. Then

$$\begin{aligned} \beta\colon kS_d &\to \mathrm{End}_k\left(V^{\otimes d}\right) \\ g &\mapsto \left(v_1 \otimes \ldots v_d \mapsto v_{g^{-1}(1)} \otimes \ldots \otimes v_{g^{-1}(d)}\right) \end{aligned}$$

is injective since the action of $\sum_{g \in S_d} a_g g \in kS_d$ on $e_1 \otimes \ldots \otimes e_d$ is given by $\sum_{g \in S_d} a_g e_{g^{-1}(1)} \otimes \ldots e_{g^{-1}(d)}$ and the summands are linearly independent. Thus $kS_d \subseteq \mathrm{End}_k(V^{\otimes d})$ is a subalgebra. Hence the assumptions of the DOUBLE CENTRALIZER THEOREM hold for $A = kS_d$ and we get $\{S_\lambda \mid \lambda \in \Lambda\} = \mathrm{Irr}(S_d)$ (Specht modules). □

Lemma VI.8. *Let $\gamma\colon A \to B$ be a surjective algebra homomorphisms over a field k. If M is an irreducible B-module then it is also an irreducible A-module by pulling back the action via γ.*

Proof. If M has no proper B-submodule then it has also no proper A-submodule because γ is surjective. □

Problem. We want to describe the labelling set of irreducible representations of S_d (up to isomorphism)

Definition. Let k be a field and A a k-algebra.

- $[A, A] := \langle \{ab - ba \mid a, b \in A\} \rangle \subseteq A$.
- If V is a finite-dimensional A-module then its *character* χ_V is defined as

$$\begin{aligned} \chi_V \colon A &\to k \\ a &\mapsto \mathrm{Tr}(\pi_a) \end{aligned}$$

where $\pi_a\colon V \to V, v \mapsto av$.

Theorem VI.9. *Let k be an algebraically closed field and A a k-algebra.*

1) *If V_i $(i \in I)$ are pairwise non-isomorphic finite-dimensional irreducible A-modules then $\chi_{V_i}\colon A \to k$ $(i \in I)$ define linearly independent elements in $({}^{A}/{}_{[A,A]})^*$.*

2) *If A is a finite-dimensional semisimple algebra then the characters χ_V for $V \in \operatorname{Irr}(A)$ form a basis of $({}^{A}/{}_{[A,A]})^*$.*

A special case is

Theorem VI.10. *Let k be an algebraically closed field with $\operatorname{char} k = 0$ and G a finite group.*

- $|\operatorname{Irr}(kG)|$ *is the number of conjugacy classes of G.*
- $|\operatorname{Irr}(kG)| = \dim \mathrm{Z}(kG)$.

Consider the special special case $G = S_d$. Then $g, h \in S_d$ are in the same conjugacy class iff g and h have the same cycle type. Hence

$$\{\text{cycle types of } S_d\} \xleftrightarrow{1:1} \{\text{partitions of } d\} \xleftrightarrow{1:1} \operatorname{Irr}(S_d).$$

Proof of Theorem VI.9.

1) If V is a finite-dimensional irreducible A-module then $\chi_V(ab - ba) = \operatorname{Tr}(\pi_a\pi_b - \pi_b\pi_a) = 0$. Therefore χ_V factors through $[A,A]$ and χ_V induces an element in $({}^{A}/{}_{[A,A]})^*$.

   Let $\sum_{i\in J} \lambda_{V_i}\chi_{V_i} = 0$ with $J \subseteq I$ finite. By Proposition V.21

$$\begin{aligned} A &\to \sum_{i\in J} \operatorname{End}_k(V_i) \\ a &\mapsto ((v_i)_{i\in J} \mapsto (av_i)_{i\in J}) \end{aligned}$$

   is surjective. In particular the identity $1_j \in \operatorname{End}_k(V_j)$ has a preimage $a_j \in A$ for all $j \in J$. Hence

$$0 = \sum_{i\in J} \lambda_{V_i}\chi_{V_i}(a_j) = \lambda_{V_j} \underbrace{\dim V_j}_{\neq 0}$$

   and thereore $\lambda_{V_j} = 0$ for all $j \in J$.

2) Left to the reader. $\square$

[December 3, 2018]

[December 6, 2018]

Algebraic groups

Motivation. If G is a finite group then G is a subgroup of some permutation group S_n (e.g. $n = |G|$). We want to generalize this by replacing S_n with $\mathrm{GL}_n(\mathbb{R})$ and finite groups by compact subgroups of $\mathrm{GL}_n(\mathbb{R}) \subseteq \mathbb{R}^{n^2}$.

VII. Linear algebraic groups and affine algebraic groups

Fact. Let $K \subseteq \mathrm{GL}_n(\mathbb{R})$ be a compact subgroup. Then there exist $f_1, \dots, f_s \in k[X_{11}, \dots, X_{nn}]$ such that $K = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid \forall 1 \leq i \leq s : f_i(A) = 0\}$.

For example $\mathrm{O}_n(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid A^T A = 1 = AA^T\}$.

Warning: The converse is not true, e.g.

$$\mathrm{SL}_2(\mathbb{R}) = \{A \in \mathrm{GL}_2(\mathbb{R}) \mid \det A = 1\} = \left\{ \begin{pmatrix} a & b \\ c & c \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) \;\middle|\; ad - bc - 1 = 0 \right\}.$$

Convention. From now on, let k be an algebraically closed field.

Definition. A *linear algebraic group G* (over k) is a subgroup of $\mathrm{GL}_n(k)$ which is the common zero set of a set M of polynomials in $k[X_{11}, \dots, X_{nn}]$, i.e.

$$G = \{A \in \mathrm{GL}_n(k) \mid \forall f \in M : f(A) = 0\}.$$

Examples.

1) $\mathrm{GL}_n(k)$ is the zero set of the zero polynomial.

2) $\mathrm{SL}_n(k) = \{A \in \mathrm{GL}_n(k) \mid \det(A) - 1 = 0\}$.

3) Finite subgroups of $\mathrm{GL}_n(k)$.

4) Diagonal matrices in $\mathrm{GL}_n(k)$, as we can write them as $\{A \in \mathrm{GL}_n(k) \mid \forall 1 \leq i \neq j \leq n : P_{ij}(A) = 0\}$ with $P_{ij}(X_{11}, \dots, X_{nn}) = X_{ij}$.

5) Uper triangular matrices in $\mathrm{GL}_n(k)$. More generally *standard parabolic subgroups*.

6) The orthogonal group $\mathrm{O}_n(k) = \{A \in \mathrm{GL}_n(k) \mid A^T = 1_n = AA^T\}$.

7) Symplectic groups

$$\mathrm{Sp}_{2n} = \{A \in \mathrm{GL}_{2n}(k) \mid A^T J A = J\} \quad \text{with} \quad J = \begin{pmatrix} 0 & E_n \\ -E_n & 0 \end{pmatrix}.$$

8) Intersections of linear algebraic groups are again linear algebraic.

We now want for instance that $\mathrm{GL}_1(k) = k^\times$ is isomorphic to

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \,\middle|\, a \in k^\times \right\} \subseteq \mathrm{GL}_2(k).$$

Definition. An *affine algebraic group* (over k) is an affine algebraic variety $(G, k[G])$ (over k) together with a group structure such that

$$\begin{aligned} \mu\colon G \times G &\to G \\ (g,h) &\mapsto gh \end{aligned} \qquad\qquad \begin{aligned} \mathrm{inv}\colon G &\to G \\ g &\mapsto g^{-1} \end{aligned}$$

are morphisms of affine algebraic varieties.

Definition. An *affine algebraic variety* (over k) is a pair $(X, k[X])$ where

- X is a set and
- $k[X]$, the *algebra of regular functions*, is a finitely generated subalgebra of $\mathrm{Maps}(X, k)$ such that

$$\begin{aligned} \Phi\colon X &\to \mathrm{Hom}_{\mathrm{Alg}}(k[X], k) \\ x &\mapsto \mathrm{ev}_x \end{aligned}$$

  is bijective. Here, "subalgebra" means a subalgebra with 1, elements in $\mathrm{Hom}_{\mathrm{Alg}}(k[X], k)$ send 1 to 1, and ev_x is the evaluation at x.

Examples.

1) Consider $X = k^n$ and $k[X] := k[X_1, \ldots, X_n]$ identified with the subalgebra $\mathcal{P}_k(k^n) \subseteq \mathrm{Maps}(k^n, k)$. We want to show that $(X, k[X])$ is an affine variety, the affine space of dimension n.

   Proof. Obviously $k[X]$ is finitely generated. The map

$$\begin{aligned} \Phi\colon X &\to \mathrm{Hom}_{\mathrm{Alg}}(k[X_1, \ldots, X_n], k) \\ y &\mapsto \mathrm{ev}_y \end{aligned}$$

   is a bijection by Hilbert's Nullstellensatz as we have

$$\begin{tikzcd} \{\text{points in } X = k^n\} \arrow[r, leftrightarrow, "1:1"] \arrow[d, leftrightarrow, "\beta"', "1:1"] & \{\text{maximal ideals in } k[X_1, \ldots, X_n]\} \arrow[d, leftrightarrow, "k=\bar{k}"', "1:1"] \\ \left\{\begin{smallmatrix}\text{algebra homomorphisms} \\ k[X_1,\ldots,X_n]\to k\end{smallmatrix}\right\} \arrow[r, leftrightarrow, "1:1"] & \left\{\begin{smallmatrix}\text{kernels of algebra homomorphisms} \\ k[X_1,\ldots,X_n]\to k\end{smallmatrix}\right\} \end{tikzcd}$$

   with β given by $y \mapsto \mathrm{ev}_y$. $\square$

2) $X = \mathrm{pt}$ and $k[X] = \mathrm{Maps}(X, k) = \mathrm{Maps}(\mathrm{pt}, k) = k$. Obviously k is a finitely generated subalgebra of $k = \mathrm{Maps}(\mathrm{pt}, k)$ and $\Phi\colon \mathrm{pt} \to \mathrm{Hom}_{\mathrm{Alg}}(k[X], k)$ is a bijection.

3) X a finite set and $k[X] = \mathrm{Maps}(X, k)$. Then $(X, k[X])$ is an affine algebraic variety.

4) Let $(X, k[X])$ be an affine algebraic variety. Consider a subset $M \subseteq k[X]$ and define the *vanishing set* of M by

$$\mathcal{V}(M) := \{x \in X \mid \forall f \in M : f(x) = 0\}$$

and set $k[\mathcal{V}(M)] = k[X]|_{\mathcal{V}(M)}$. We want to show that $(\mathcal{V}(M), k[\mathcal{V}(M)])$ is an affine algebraic variety.

Proof. We have a restriction map $\mathrm{res}\colon k[X] \to k[\mathcal{V}(M)]$ which is obviously an surjective algebra homomorphism by definition. By assumption $k[X]$ is finitely generated, and thus its quotient $k[\mathcal{V}(M)]$ is a finitely generated subalgebra.

It is left to show that

$$\begin{array}{rcl} \tilde{\Phi}\colon \mathcal{V}(M) & \to & \mathrm{Hom}_{\mathrm{Alg}}(k[\mathcal{V}(M)], k) \\ x & \mapsto & \mathrm{ev}_x \end{array}$$

is bijective.

If $f\colon k[\mathcal{V}(M)] \to k$ is an algebra homomorphism then

$$\begin{tikzcd} k[X] \arrow[r, "\mathrm{res}"] \arrow[dr, dashed, "\tilde{f}"'] & k[\mathcal{V}(M)] \arrow[d, "f"] \\ & k \end{tikzcd}$$

defines an algebra homomorphism $\tilde{f} = f \circ \mathrm{res}$. In particular we have $\tilde{f} = \mathrm{ev}_x$ for some $x \in X$ because $(X, k[X])$ is an affine algebraic variety.

For injectivity let $x, y \in \mathcal{V}(M)$ with $\mathrm{ev}_x = ev_y\colon k[\mathcal{V}(M)] \to k$. Then $\tilde{\mathrm{ev}}_x = \tilde{\mathrm{ev}}_y$. But $\tilde{\mathrm{ev}}_x$ must be $\mathrm{ev}_x\colon k[X] \to k$, and the same holds for $\tilde{\mathrm{ev}}_y$. Thus $\mathrm{ev}_x = \mathrm{ev}_y\colon k[X] \to k$, and as Φ is bijective, we get $x = y$.

For surjectivity let $h \in \mathrm{Hom}_{\mathrm{Alg}}(k[\mathcal{V}(M)], k)$. Define $\tilde{h} := h \circ \mathrm{res}$, and we have $\tilde{h} = \mathrm{ev}_x$ for some $x \in X$.

$x \in \mathcal{V}(M)$: For $f \in k[\mathcal{V}(M)]$ pick $f' \in k[X]$ such that $f'|_{\mathcal{V}(M)} = f$. Then $\mathrm{ev}_x(f) = f(x)$ and $h(f) = h(\mathrm{res}(f)) = \tilde{h}(f) = \mathrm{ev}_x(f) = f(x)$ for all $f \in k[\mathcal{V}(M)]$. Thus $\mathrm{ev}_x = h$.

$x \notin \mathcal{V}(M)$: Then there exists an $f \in M \subseteq k[X]$ with $g(x) \neq 0$ but $g|_{\mathcal{V}(M)} = 0$. Now consider

$$\begin{tikzcd} k[X] \arrow[r, "\mathrm{res}"] \arrow[dr, "\mathrm{ev}_x"'] & k[\mathcal{V}(M)] \arrow[d, "h"] \\ & k \end{tikzcd}$$

and we get $g \mapsto \operatorname{res}(g) = 0 \mapsto h(0) = 0$ and $g \mapsto \operatorname{ev}_x(g) = g(x) \neq 0$ which is a contradiction.

Thus any $h \in \operatorname{Hom}_{\mathrm{Alg}}(k[X], k)$ has a preimage. $\square$

5) Let $(X, k[X])$ be an affine algebraic variety and $f \in k[X]$. Define $X_f := \{x \in X \mid f(x) \neq 0\}$ and $k[X_f] := k[X]|_{X_f}[f^{-1}]$ (localisation at f). Then $(X_f, k[X_f])$ is an affine algebraic variety.

As a consequence every linear algebraic group is an affine algebraic group.

Proposition VII.1. *Given a linear algebraic group $X = G$ (over k) we can find some $k[X]$ such that $(X, k[X])$ is an affine algebraic variety.*

Proof. Consider $Y = k^{n^2} = \mathrm{M}_{n\times n}(k)$. Now $(Y, k[Y])$ with $k[Y] = k[X_{11}, \ldots, X_{nn}]$ and $\mathrm{GL}_n(k) \subseteq Y$ with $k[\mathrm{GL}_n(k)] = k[X_{\det}]$ are affine algebraic varieties. Thus $(\mathcal{V}(M) = G, k[\mathcal{V}(M)] = k[G])$ is an affine algebraic variety. $\square$

Definition. Let $(X, k[X])$ and $(Y, k[Y])$ be affine algebraic varieties. A *morphism* (of affine algebraic varieties) from $(X, k[X])$ to $(Y, k[Y])$ is a map $f\colon X \to Y$ such that $f^*\colon k[Y] \to k[X]$ where

$$\begin{aligned} f^*\colon k[Y] \subseteq \operatorname{Maps}(Y,k) &\to \operatorname{Maps}(X,k) \\ h &\mapsto h \circ f. \end{aligned}$$

If $\operatorname{im} f^* \subseteq k[X]$ we also write $f^\natural$. Hence a morphism is a pair $(f, f^\natural)$.

Warning. Consider $k = \overline{\mathbb{F}_p}$ and the Frobenius map $\mathrm{Fr}\colon k \to k$. Then Fr is a morphism $(k, k[k])$ which is bijective, but not an isomorphism.

[December 6, 2018]

[December 10, 2018]

Lemma VII.2. *There is a bijection*

$$\begin{aligned} \left\{\begin{matrix} \textit{morphisms of affine} \\ \textit{algebraic varieties} \\ f\colon (X,k[X])\to(Y,k[Y]) \end{matrix}\right\} &\xleftrightarrow{1:1} \left\{\begin{matrix} \textit{algebra homomorphisms} \\ k[Y]\to k[X] \end{matrix}\right\} \\ (f, f^\natural) &\mapsto f^* = f^\natural \\ (\varphi_g\colon X \to Y, \varphi_g^*) &\leftarrow g \end{aligned}$$

where $\varphi_g(x) \in Y$ for $x \in X$ such that

$$\begin{tikzcd} k[Y] \arrow[r, "g"] \arrow[dr, dashed, "\operatorname{ev}_{\varphi_g(x)}"'] & k[X] \arrow[d, "\operatorname{ev}_x"] \\ & k \end{tikzcd}$$

commutes. The bijection is compatible with composition and the identities are mapped to each other.

Notation. We denote

$$\mathrm{Hom}_{\mathrm{Var}}(X,Y) = \left\{ f\colon (X,k[X]) \to (Y,k[Y]) \;\middle|\; \begin{smallmatrix} f \text{ is a morphism of} \\ \text{affine algebraic varieties} \end{smallmatrix} \right\}.$$

Remark. Behind Lemma VII.2 is an equivalence of categories

$$\begin{array}{ccc} \left\{ \begin{smallmatrix} \text{affine algebraic varieties} \\ \text{over } k \text{ with morphisms} \end{smallmatrix} \right\} & \xleftrightarrow{1:1} & \left\{ \begin{smallmatrix} \text{finitely generated } k\text{-algebras} \\ \text{without nilpotent elements} \end{smallmatrix} \right\} \\ (X,k[X]) & \mapsto & k[X] \\ (f,f^\natural) & \mapsto & f^* = f^\natural \end{array}$$

identifying $\mathrm{Hom}_{\mathrm{Var}}(X,Y)$ with $\mathrm{Hom}_{\mathrm{Alg}}(k[Y],k[X])$.

Proof of Lemma VII.2. We show that the maps are inverse to each other.

$(f,f^\natural) \mapsto f^\natural \mapsto \varphi_{f^\natural}$: Let $h \in k[Y]$ and $x \in X$. Then we have

$$\mathrm{ev}_{\varphi^\natural(x)}(h) = \mathrm{ev}_x \circ f^\natural(h) = \mathrm{ev}_x \circ f^*(h) = ev_x(h \circ f) = (h \circ f)(x) = \mathrm{ev}_{f(x)}(h)$$

which yields $\mathrm{ev}_{\varphi_{f^\natural}(x)} = \mathrm{ev}_{f(x)}$ and $\varphi_{f^\natural}(x) = f(x)$ as $(Y,k[Y])$ is an affine algebraic variety. Thus $f^\natural = f$.

$g \mapsto \varphi_g \mapsto \varphi_g^*$: Let $h \in K[Y]$ and $x \in X$. We get

$$\varphi_g^*(h)(x) = (h \circ \varphi_g)(x) = \mathrm{ev}_{\varphi_g(x)}(h) = \mathrm{ev}_x(g(h)) = g(h)(x) = \varphi_g^*(h) = g(h)$$

and therefore $\varphi_g^* = g$ (in particular also $\varphi_g^*\colon k[Y] \to k[X]$, so $\varphi_g^* = \varphi_g^\natural$ and the inverse map is well-defined).

The compatibility with composition and identity maps is obvious. □

Theorem VII.3. *Every affine algebraic variety is isomorphic to some* $(\mathcal{V}(M), k[\mathcal{V}(M)])$ *where* $M \subseteq k[T_1,\dots,T_n]$.

Proof. Let $(X,k[X])$ be an affine algebraic variety. Then $k[X]$ is a finitely generated commutative k-algebra. Let $a_1,\dots,a_n$ be generators. Then there exists a surjective algebra homomorphism $\pi\colon k[T_1,\dots,T_n]$ sending T_i to a_i. Now define

$$\begin{aligned} f\colon X &\to k^* \\ x &\mapsto (\pi(T_1)(x),\dots,\pi(T_n)(x)). \end{aligned}$$

We get $f^* = \pi$ (with $k[k^n] = k[T_1,\dots,T_n]$) as we have $f^*(T_i)(x) = T_i(f(x)) = \pi(T_i)(x) =$ for all $x \in X$ and $1 \le i \le n$ and both f^* and π are algebra homomorphisms.

Let $M = \ker\pi$. Hence $\operatorname{im} f \subseteq \mathcal{V}(M)$, as we have $\varphi(f(x)) = f^*(\varphi)(x) = \pi(\varphi)(x) = 0$ for $\varphi \in M = \ker\pi$ and $x \in X$. Note that $\sqrt{\ker\pi} = \ker\pi$ (since $p^r \in \ker\pi \Leftrightarrow \pi(p^r) = 0 \Leftrightarrow (\pi(p))^r = 0 \Leftrightarrow \pi(p) = 0$).

We have a surjective algebra homomorphism

$$\begin{array}{rcl} k[T_1,\dots,T_n] & \to & k[\mathcal{V}(M)] \\ f & \mapsto & f|_{\mathcal{V}(M)} \end{array}$$

with the kernel

$$\mathcal{I}(\mathcal{V}(M)) = \{f \in k[T_1,\dots,T_n] \mid \forall x \in \mathcal{V}(M) : f(x) = 0\} = \sqrt{M} = \sqrt{\ker \pi} = M$$

using Hilbert's Nullstellensatz. Hence $k[\mathcal{V}(M)] = {}^{k[T_1,\dots,T_n]}\!/_{M} = {}^{k[T_1,\dots,T_n]}\!/_{\ker \pi}$, and $(f, f^\natural)$ defines an isomorphism $(X, k[X]) \to (\mathcal{V}(M), k[\mathcal{V}(M)])$ using Lemma VII.2. □

Consequence. Let $(X, k[X])$ be an affine algebraic variety. Via this identification X is a topological space with the Zariski topology. One can show that this is independent (up to isomorphism of topological spaces) from the chosen realisation.

Lemma VII.4. *Every morphism of affine algebraic varieties is continuous.*

Proof. Let $f\colon (X, k[X]) \to (Y, k[Y])$ be a morphism. We have to show that the preimages of closed subset are closed. Let $Z \subseteq Y$ be closed. Then $Z = \mathcal{V}(N) \cap Y$ for some subset of polynomials N. Now

$$\begin{aligned} f^{-1}(Z) &= \{x \in X \mid f(x) \in \mathcal{V}(N)\} = \{x \in X \mid \forall \varphi \in N : \varphi(f(x)) = 0\} \\ &= \{x \in X \mid \forall \varphi \in N : f^*(\varphi)(x) = 0\} = \{x \in X \mid x \in \mathcal{V}(f^*(N))\}. \end{aligned}$$

Using $f^* = f^\natural$ we get $f^*(N) \subseteq k[X] = k[T_1,\dots,T_n]|_{\mathcal{V}(M)}$ and thus $f^{-1}(Z) = \mathcal{V}(f^*(N)) \cap X$ is closed. □

VIII. Products and Hopf algebras

Goal. We are interested in relations between linear algebraic groups and affine algebraic groups as affine algebraic varieties.

Definition. Let $(X_i, k[X_i])$ for $i \in I = \{1,2\}$ be affine algebraic varieties. Then let

$$(X_1 \mathbin{\dot\cup} x_2, k[X_1 \mathbin{\dot\cup} x_2]) \quad \text{with} \quad k[X_1 \mathbin{\dot\cup} X_2] := \{f\colon X_1 \mathbin{\dot\cup} X_2 \to k \mid \forall i \in I : f|_{X_i} \in k[X_i]\}$$

be the *coproduct* of $(X_1, k[X_1])$ and $(X_2, k[X_2])$ and

$$(X_1 \times X_2, k[X_1 \times X_2]) \quad \text{with} \quad k[X_1 \times X_2] := \left\langle \bigcup_{i \in I} \operatorname{im}\left(p_i^*|_{k[X_i]}\right) \right\rangle \subseteq \operatorname{Maps}(X_1 \times X_2, k)$$

the *product* where $p_i\colon X_1 \times X_2 \to X_i$ are the canonical projections.

Proposition VIII.1. *Let $(X_i, k[X_i])$ for $i \in I = \{1,2\}$ be affine algebraic varieties.*

0) *The (co)product is an affine algebraic variety and satisfies the following universal properties for any affine algebraic variety $(Z, k[Z])$.*

1) *If $f_i \in \mathrm{Hom}_{\mathrm{Var}}(X_i, Z)$ then there exists a unique $h \in \mathrm{Hom}_{\mathrm{Var}}(X_1 \dot\cup X_2, Z)$ such that*

$$\begin{tikzcd} X_1 \arrow[r, hook, "\mathrm{incl}_1"] \arrow[dr, "f_1"'] & X_1 \dot\cup X_2 \arrow[d, dashed, "\exists! h"] & X_2 \arrow[l, hook', "\mathrm{incl}_2"'] \arrow[dl, "f_2"] \\ & Z & \end{tikzcd}$$

commutes.

2) *If $f_i \in \mathrm{Hom}_{\mathrm{Var}}(Z, X_i)$ then there exists a unique $h \in \mathrm{Hom}_{\mathrm{Var}}(Z, X_1 \times X_2)$ such that*

$$\begin{tikzcd} X_1 & X_1 \times X_2 \arrow[l, two heads, "p_1"'] \arrow[r, two heads, "p_2"] & X_2 \\ & Z \arrow[ul, "f_1"] \arrow[u, dashed, "\exists! h"] \arrow[ur, "f_2"'] & \end{tikzcd}$$

commutes.

Proof.

0) Let $\mathbb{1}_{X_i} \in \mathrm{Maps}(X_1 \dot\cup X_2, k)$ be defined by

$$\mathbb{1}_{X_i}(w) = \begin{cases} 1 & \text{if } w \in X_i, \\ 0 & \text{otherwise.} \end{cases}$$

$\mathbb{1}_{X_i}|_{X_i}$ is the unit in $k[X_i]$, and $\mathbb{1}_{X_i}|_{X_j}$ $(i \neq j)$ is the zero map in $k[X_j]$, and we have $\mathbb{1}_{X_i} \in k[X_1 \dot\cup X_2]$. Now $\mathbb{1}_{X_1} + \mathbb{1}_{X_2} = 1 \in k[X_1 \dot\cup X_2]$, where 1 is the unit in $\mathrm{Maps}(X_1 \dot\cup X_2, k)$.

For $h \in k[X_1]$ define $\tilde h \in \mathrm{Maps}(X_1 \dot\cup X_2, k)$ by $\tilde h|_{X_2} = h$

1)

2) Left to the reader. ☐

TO BE CONTINUED

[December 10, 2018]

[December 13, 2018]

TO BE INSERTED

[December 13, 2018]

[December 17, 2018]

TO BE INSERTED

[December 17, 2018]

[December 20, 2018]

TO BE INSERTED

[December 20, 2018]

[January 11, 2019]

IX. Linearization of algebraic groups

Definition. Let $(G, k[G])$ be an affine algebraic group and $(X, k[X])$ be an affine algebraic variety. An *action of* $(G, k[G])$ *on* $(X, k[X])$ is a morphism

$$\begin{aligned} \alpha\colon G \times X &\to X \\ (g, x) &\mapsto g.x. \end{aligned}$$

(we say that G acts on X as affine algebraic varieties) such that $e.x = x$ and $(g.h).x = g.(h.x)$ for all $x \in X$. We then write $G \circlearrowright^{\alpha} X$ or $G \circlearrowright X$ and call the action *algebraic* (in contrast to an ordinary action of a group on a set).

Remark. One can define orbits, fixed points, transitive actions, ... as usual.

Definition. Let $G \circlearrowright X$ and $Y, Z \subseteq X$. Then we define

- $\mathrm{Trans}_G(Y, Z) := \{g \in G \mid \forall y \in Y : g.y \in Y\}$, the *transporter from* Y *to* Z, and
- $\mathrm{C}_G(Y) := \bigcap_{y \in Y} G_y$ where $G_y := \{g \in G \mid g.y = y\}$, the *stabilizer of* Y *respectively* $y \in Y$.

Lemma IX.1. *Let* $(X, k[X]), (X', k[X']), (Y, k[Y]), (Y', k[Y'])$ *be affine algebraic varieties.*

1) *For any* $y \in Y$ *the maps* $X \to X \times Y, x \mapsto (x, y)$ *and* $X \to Y \times X, x \mapsto (y, x)$ *are morphisms.*
2) *If* $\varphi_1\colon X \to X'$ *and* $\varphi_2\colon Y \to Y'$ *are morphisms, then*

$$\begin{aligned} \varphi_1 \times \varphi_2\colon X \times Y &\to X' \times Y', \\ (x, y) &\mapsto (\varphi_1(x), \varphi_2(y)) \end{aligned}$$

is a morphism.

Proof. Left to the reader. □

Proposition IX.2. *Let* $G \circlearrowright^{\alpha} X$ *and* $Y, Z \subseteq X$ *subsets with* Z *closed.*

1) $\mathrm{Trans}_G(Y, Z) \subseteq G$ *is closed.*

2) $\mathrm{C}_G(Y) \subseteq G$ *and* $G_y \subseteq G$ *is closed for any* $y \in Y$.

3) $X^G \subseteq Y$ *is closed.*

Proof.

1) Let $y \in Y$. The *orbit map* for y

$$\begin{aligned} \alpha_y \colon G &\to Y \\ g &\mapsto g.y \end{aligned}$$

is a morphism, because $\alpha_y = \alpha \circ (g \mapsto (g, y))$ and the composition of morphisms is again a morphism. On the other hand Z is closed, so $\alpha_y^{-1}(Z)$ is closed, as morphisms are continuous. We have $\alpha_y^{-1}(Z) = \{g \in G \mid g.y \in Z\}$ and now $\mathrm{Trans}_G(Y, Z) = \bigcap_{y \in Y} \alpha_y^{-1}(Z)$ is closed.

2) $G_y = \mathrm{Trans}_G(\{y\}, \{y\})$ is closed since ponts are closed in X. Therefore $\mathrm{C}_g(Y) = \bigcap_{y \in Y}(G_y)$ is also closed.

3) Let $g \in G$ and

$$\begin{aligned} \varphi \colon X &\to X \times X \\ x &\mapsto (x, g.x), \end{aligned}$$

which is a morphism. We get $X^g = \{x \in X \mid g.x = x\} = \varphi^{-1}(\{(x, x) \mid x \in X\})$. Now the “diagonal” $\{(x, x) \mid x \in X\}$ is closed (since it is a zero set) and φ is continuous, so X^g is closed. Hence $X^G = \bigcap_{g \in G} X^g$ is also closed. □

Corollary IX.3. *Let* $(G, k[G])$ *be an affine algebraic group,* $H \subseteq G$ *a closed subgroup and* $x \in G$. *The normalizer* $\mathrm{N}_G(H) = \{g \in G \mid gHg^{-1} \subseteq H\}$ *of* H *and the centralizer* $\mathrm{C}_G(x) = \{g \in G \mid gxg^{-1} = x\}$ *of* x *are closed.*

Proof. Consider conjugation as the group action on G. Then $\mathrm{C}_G(x) = G_x$ and $\mathrm{N}_G(H) = \mathrm{Trans}_G(H, H)$ are closed by Proposition IX.2. □

Warning. Orbits are in general not closed.

For example, consider $G = \mathbb{G}_m = \mathrm{GL}(\mathbb{C}) \circlearrowright \mathbb{C}$ by multiplication. The orbit of 0 is $\{0\}$ (closed), but the orbit of 1 is $\mathbb{C} \setminus \{0\}$ which is not closed, since closed subsets in $\mathbb{C}$ are finite).

Assume $G \circlearrowright^{\alpha} X$ for $g \in G$ consider

$$\begin{aligned} \beta_g \colon X &\to X \\ x &\mapsto g^{-1}.x \end{aligned}$$

(a morphism since $\beta_g = x \mapsto (g, x) \mapsto (g^{-1}, x) \mapsto g^{-1}.x$). Hence we get a comorphism

$$\begin{aligned} \beta_g^* \colon k[X] &\to k[X] \\ f &\mapsto f \circ \beta_g. \end{aligned}$$

Note $\beta_g^*(f)(x) = f(g^{-1}x)$ for all $x \in X$. Moreover $\beta_{gh}^* = \beta_g^* \circ \beta_h^*(f)$ for all $g, h \in G$.

If $(X, k[X]) = (G, k[G])$ is an affine algebraic group, then we can also consider

$$\begin{array}{rcl} \gamma_g \colon G & \to & G \\ x & \mapsto & xg \end{array}$$

and get a comorphism

$$\begin{array}{rcl} \gamma_g^* \colon k[G] & \to & k[G] \\ f & \mapsto & f \circ \gamma_g. \end{array}$$

Note $\gamma_g^*(f)(x) = f(xg)$ for all $g, x \in G$. Moreover $\gamma_{gh}^* = \gamma_g^* \circ \gamma_h^*$.

Definition. For any affine algebraic group $(G, k[G])$ we obtain representations of the (ordinary) group G on $k[G]$

$$\begin{array}{rcl} \lambda \colon G & \to & \mathrm{GL}(k[G]) \\ g & \mapsto & \lambda_g := \beta_g^* \end{array}$$

called *left translation of functions* and

$$\begin{array}{rcl} \rho \colon G & \to & \mathrm{GL}(k[G]) \\ g & \mapsto & \rho_g := \gamma_g^*. \end{array}$$

IX.1. Characterisation of elements in closed subgroups

Lemma IX.4. *Let $(G, k[G])$ be an affine algebraic group, $H \subseteq G$ a closed subgroup and $I = \mathcal{I}(H)$. Then $H = \{g \in G \mid \rho_y(I) \subseteq I\}$.*

Proof.

"$\subseteq$" Let $g \in H$ and $f \in I$. Then $\rho_g(f)(h) = f(hg) = 0$ for all $h \in H$, so $\rho_g(f) \in I$.

"$\subseteq$" Let $\rho_g(I) \subseteq I$. Then for all $f \in I$ we have $0 = \rho_g(f)(e) = f(eg) = f(g)$, so $f(g) = 0$ for all $f \in I$. This implies $g \in H$.

□

MISSING PROOFS, TO BE INSERTED

Proposition IX.5. *Let $G \circlearrowright^\alpha X$ and $F \subseteq k[X]$ a finite-dimensional subspace.*

1) *There exists a finite-dimensional subspace $E \subseteq k[X]$ such that $F \subseteq E$ and E is stable under all left translations of functions (i.e. $\lambda_g(E) \subseteq E$ for all $g \in G$).*

2) *F is stable under all left translations if and only if $\alpha^*(F) \subseteq k[G] \otimes k[X] \cong k[G \times X]$.*

Corollary IX.6. *Let $(G, k[G])$ be an affine algebraic group. Then every subspace $F \subseteq k[G]$ is contained in a finite-dimensional subspace $E \subseteq k[G]$ which is stable under both left and right translations.*

We know that linear algebraic groups are affine algebraic groups.

Theorem IX.7. *Let $(G, k[G])$ be an affine algebraic group. Then it is isomorphic to a linear algebraic group.*

[January 11, 2019]

[January 14, 2019]

X. Affine algebraic varieties/groups as topological spaces

Let X be an affine algebraic variety. We want to study X as a topological space with the Zariski topology.

X.1. Generalities

Definition. A topological space X is called

- *noetherian* if open sets satisfy the ascending chain condition: For any chain of open sets $U_1 \subseteq U_2 \subseteq \ldots$ there exists an $i_0 \in \mathbb{N}$ such that $U_i = U_{i_0}$ for all $i \geq i_0$.
- *irreducible* if $X = X_1 \cup X_2$ for some disjoint and closed $X_1, X_2 \subseteq X$ implies $X_1 = X$ or $X_2 = X$.

Remark. Let X be a topological space.

1) If X is irreducible, X is connected.
2) The following are equivalent:
   a) X is irreducible.
   b) Any nonempty open subset of X is dense.
   c) If $U_1, U_2 \subseteq X$ are open and non-empty then $U_1 \cap U_2 \neq \emptyset$.

Lemma X.1. *Let $(X, k[X])$ be an affine algebraic variety. Then X is noetherian.*

Notation. Let X be a topological space and $U \subseteq X$. We write $U \overset{\circ}{\subset} \subset X$ if U is open in X, and $U \overset{c}{\subset} X$ if U is closed in X.

Lemma X.2. *Let X and X' be topological spaces.*

1) *If $Y \subseteq X$ is irreducible, $\overline{Y}$ is irreducible.*

2) *Let* $\varphi\colon X \to X'$ *be continuous. If* X *is irreducible,* $\varphi(X)$ *is irreducible.*

3) *If* X *and* X' *are irreducible,* $X \times X'$ *is irreducible.*

Proposition X.3. *Let* X *be a noetherian topological space.*

1) *There exists an* $r \in \mathbb{N}$ *and irreducible* $X_i \Subset X$ $(1 \leq i \leq r)$ *such that*

$$X = X_1 \cup \cdots \cup X_r. \tag{*}$$

2) *If one assumes moreover that* $X_i \nsubseteq X_j$ *for* $i \neq j$ *then the decomposition* (*) *is unique up to permutation. In this case the* X_i *are called the* irreducible components *of* X *and are maximal irreducible subsets (with respect to inclusion).*

X.2. Identity component

Lemma X.4. *Let* $(G, k[G])$ *be an affine algebraic group. Then there exists exactly one irreducible component* G_0 *containing* $e \in G$*. It is called the* identity component*.*

Definition. An affine algebraic group $(G, k[G])$ is *connected* if $G_0 = G$.

Proposition X.5. *Let* $(G, k[G])$ *be an affine algebraic group.*

1) $G_0 \subseteq G$ *is a closed and maximal subgroup.*

2) $(G : G_0) < \infty$.

3) *The* gG_0 $(g \in G)$ *are the connected and irreducible components.*

4) *Each closed subgroup* $H < G$ *with finite index contains* G_0*.*

Lemma X.6. *Let* $(G, k[G])$ *be an affine algebraic group. Let* $U, V \subseteq G$ *be open and dense. Then* $G = U \cdot V$*.*

Definition. Let X be a topological space and $Y \subseteq X$ a subset. It is called *locally closed* if $Y = U \cap Z$ for some $U \overset{\circ}{\Subset} X$ and $Z \Subset X$. Finite unions of locally closed subsets in X are called *constructible*.

Remark. One can show that {constructible subsets in X} contains all open and closed sets, and it is *closed* under taking finite unions and complements (in fact it is minimal with these properties).

Proposition X.7. *Let* X *be a topological space.*

1) *A constructible set* $Y \subseteq X$ *contains a subset which is closed and open in* $\overline{Y}$*.*

2) *(Chevalley) Images of constructible sets (under morphisms of affine algebraic varieties) are constructible.*

Proposition X.8. *Let $(G, k[G])$ be an affine algebraic group and $H \subseteq G$ a subgroup.*

1) $\overline{H} \subseteq G$ *is a subgroup.*

2) *If H is constructible then $H = \overline{H}$.*

Proposition X.9. *Let $\varphi\colon G \to G'$ be a morphism of affine algebraic groups.*

1) $\ker \varphi \subseteq G$ *is a closed subgroup.*

2) $\operatorname{im} \varphi \subseteq G'$ *is a closed subgroup.*

3) $\varphi(G_0) = \operatorname{im} \varphi$.

XI. More on products

We know that if $(X, k[X])$ and $(Y, k[Y])$ are affine algebraic varieties then $(X \times Y, k[X \times Y])$ (with $k[X \times Y] \cong k[X] \otimes k[Y]$) is an affine algebraic variety.

Warning. The Zariski topology on $X \otimes Y$ is not (in general) the product of the Zariski topology.

For example consider the product $\mathbb{A}^1 \times \mathbb{A}^1$. In the product topology the open sets are unions of $U_1 \times U_2$'s where U_1 and U_2 are open in $\mathbb{A}^1$ in the Zariski topology. The closed sets are $\emptyset$, $Z_1 \times k$, $k \times Z_2$, finite sets and $k \times k$ (where Z_1, Z_2 are closed in the Zariski topology, so finite). But in the Zariski topology of $\mathbb{A}^1 \times \mathbb{A}^1$ things like curves or $\mathcal{I}(x - y)$ are closed.

[January 14, 2019]

[January 18, 2019]

TO BE INSERTED

[January 18, 2019]

[January 21, 2019]

TO BE INSERTED