ERASMUS MINI-COURSE ON HOPF ALGEBRAS'

Contents

All rings in this note are considered to be associative and unital unless otherwise stated. Ring homomorphisms are supposed to be unital, meaning that the identity element of one ring is mapped to the identity element of the other.

1. Lecture: Representations of Lie algebras g and their enveloping algebra U(g)

Let $\mathbb{K}$ be a field. A ring A is called a $\mathbb{K}$-algebra, if there exists a ring homomorphism $\eta : \mathbb{K} \to Z(A)$, where $Z(A)$ denotes the center of the ring A. Then A becomes a vector space over $\mathbb{K}$ with scalar multiplication given by

$$\lambda \cdot a := \eta(\lambda)a, \tag{1}$$

for all $\lambda \in \mathbb{K}$ and $a \in A$. We will usually suppress η and write simply λa to denote $\lambda \cdot a$. The field $\mathbb{K}$ itself is of course a $\mathbb{K}$-algebra, with $\eta = id_{\mathbb{K}}$. Also any field extension $\mathbb{E}$ of $\mathbb{K}$ is a $\mathbb{K}$-algebra, where $\eta : \mathbb{K} \subseteq \mathbb{E}$ is the inclusion map. Furthermore, if A is a $\mathbb{K}$-algebra, then also polynomial rings $A[x_1, \dots, x_n]$ and matrix rings $M_n(A)$ are $\mathbb{K}$-algebras.

We will introduce now Lie algebras and a good reference on that subject is the book by Erdmann and Wildon [1].

Definition 1.1 (Lie Algebra)**.** *Let $\mathbb{K}$ be a field. A Lie algebra over $\mathbb{K}$ is an $\mathbb{K}$-vector space L, together with a bilinear map, the* Lie bracket $[\ ,\ ] : L \times L \to L$, *satisfying the following properties:*

(L1) $[x, x] = 0$, *for all* $x \in L$

(L2) $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$, *for all* $x, y, z \in L$

Condition (L2) is known as the *Jacobi identity*. As the Lie bracket $[-, -]$ is bilinear, we have

$$0 = [x + y, x + y] = [x, x] + [x, y] + [y, x] + [y, y] = [x, y] + [y, x]. \tag{2}$$

Hence condition $(L1)$ implies

(L1') $[x, y] = -[y, x]$, for all $x, y \in L$.

In case char($\mathbb{K}$) $\neq 2$, then $(L1')$ implies $(L1)$ by choosing $x = y$.

Definition 1.2 (Homomorphism of Lie algebras). *Given a $\mathbb{K}$-linear map $f : L_1 \to L_2$ between to Lie algebras $(L_1, [,]_1)$ and $(L_2, [,]_2)$ is said to be a homomorphism of Lie algebras if f preserves the brackets, i.e.*

$$[f(x), f(y)]_2 = f([x, y]_1), \tag{3}$$

for all $x, y \in L$.

Example 1.3 (Abelian Lie algebra). *Any vector space L can be made into a Lie algebra by setting $[x, y] = 0$, for all $x, y \in L$ (where 0 shall denote the zero vector of L).*

Example 1.4 (Vector Product). *Let $L = \mathbb{R}^3$ and consider the vector product $[,] : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$ with $[u, v] := u \times v$, for vectors $u, v \in \mathbb{R}^3$. In coordinates, $u = (u_1, u_2, u_3)$ and $v = (v_1, v_2, v_3)$ this means:*

$$[u, v] := u \times v = (u_2v_3 - u_3v_2, u_3v_1 - u_1v_3, u_1v_2 - u_2v_1). \tag{4}$$

Clearly $[u, u] = 0$ holds. One checks $u \times (v \times w) = (u \cdot w)v - (u \cdot v)w$, where $u \cdot v$ is the scalar product, and concludes the Jacobi identity. Thus $(\mathbb{R}^3, \times)$ is a Lie algebra. For the canonical basis vectors e_1, e_2, e_3 of $\mathbb{R}^3$ we have

$$[e_1, e_2] = e_3, \qquad [e_1, e_3] = -e_2, \qquad [e_2, e_3] = e_1. \tag{5}$$

Example 1.5 (Algebra as Lie algebra with Commutator). *Let A be any $\mathbb{K}$-algebra. Then $(A, [,])$ is a Lie algebra, where $[,]$ is the commutator bracket, i.e.*

$$[a, b] = ab - ba, \tag{6}$$

for all $a, b \in A$. Clearly, $[a, a] = 0$ holds and the Jacobi identity holds because for all $a, b, c \in A$:

$$\begin{aligned} [a, [b, c]] + [b, [c, a] + [c, [a, b]] &= a(bc - cb) - (bc - cb)a + b(ca - ac) - (ca - ac)b + c(ab - ba) - (ab - ba)c \\ &= abc - acb - bca + cba + bca - bac - cab + acb + cab - cba - abc + bac \\ &= 0. \end{aligned}$$

Example 1.6 (Matrix Lie algebras). *Consider $A = M_n(\mathbb{K})$, the vector space of $n \times n$-matrices with entries in $\mathbb{K}$. Since A is also an associative algebra, A is a Lie algebra with commutator bracket. Note that a $\mathbb{K}$-basis of A is given by the elementary matrices E_{ij}, with $1 \leq i, j \leq n$. One easily checks*

$$[E_{ij}, E_{kl}] = E_{ij}E_{kl} - E_{kl}E_{ij} = \delta_{jk}E_{il} - \delta_{li}E_{kj}, \tag{7}$$

where δ_{ij} denotes the Kronecker symbol with $\delta_{ij} = 1$ if $i = j$ and $\delta_{ij} = 0$ otherwise. This Lie algebra is usually denoted by $\mathfrak{gl}_n(\mathbb{K})$ or $\mathfrak{gl}(n, \mathbb{K})$ and called general linear Lie algebra. For $n = 2$, we have the 4 basis elements $x = E_{11}, e = E_{12}, f = E_{21}, y = E_{22}$. Hence the non-zero brackets are given by

$$[e, f] = x - y, \qquad [e, y] = e = [x, e], \qquad [f, x] = f = [y, f]. \tag{8}$$

Example 1.7 (Special linear algebra). *A subspace of $\mathfrak{gl}_n(\mathbb{K})$ is the space $\mathfrak{sl}_n(\mathbb{K})$ of all matrices with zero trace. Recall that the trace $tr(x)$ of a matrix $x = (x_{ij})$ is the sum of entries of the main diagonal and that $tr(xy) = tr(yx)$ for two $n \times n$-matrices x and y. Thus $tr([x, y]) = 0$. Hence the restriction of the commutator bracket to $\mathfrak{sl}_n(\mathbb{K})$ turns this space into a Lie algebra, called* special linear algebra.

For example, if $n = 2$, then a basis for $\mathfrak{sl}_2(\mathbb{K})$ is given by

$$e = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \qquad f = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \qquad h = x - y = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{9}$$

The non-zero brackets of these elements are given by the Serre relations:

$$[e, f] = h, \qquad [h, e] = 2e, \qquad [h, f] = -2f. \tag{10}$$

Example 1.8 (Strictly upper triangular matrices). *A subspace of $\mathfrak{sl}_n(\mathbb{K})$ is the space $\mathfrak{T}_n(\mathbb{K})$ of all strictly upper triangular matrices, i.e.*

$$\mathfrak{T}_n(\mathbb{K}) = \operatorname{span}\left\{E_{ij} \,:\, i < j\right\}. \tag{11}$$

Then $T_n(\mathbb{K})$ becomes a Lie algebra with the commutator bracket. The three dimensional Heisenberg Lie algebra is defined as $\mathfrak{h} := T_3(\mathbb{K})$, which has basis

$$x = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \qquad y = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \qquad z = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}. \tag{12}$$

The brackets are given by

$$[x, y] = z, \qquad [x, z] = 0, \qquad [y, z] = 0. \tag{13}$$

Definition 1.9 (Derivations). *A derivation of a $\mathbb{K}$-algebra A is a $\mathbb{K}$-linear map $\delta : A \to A$ that satisfies the* Leibniz rule

$$\delta(ab) = a\delta(b) + \delta(a)b, \tag{14}$$

for all $a, b \in A$.

Note that if δ is a derivation of a $\mathbb{K}$-algebra A and $c \in Z(A)$ is an element of A, then $\overline{\delta} := c\delta$ defined as $\overline{\delta}(x) = c\delta(x)$ is again a derivation, because for $a, b \in A$:

$$\overline{\delta}(ab) = c\delta(ab) = c\,(a\delta(b) + \delta(a)b) = a\overline{\delta}(b) + \overline{\delta}(a)b$$

using that c commutes with a. In particular, given scalars $\lambda_1, \lambda_2 \in \mathbb{K}$ and derivations δ_1, δ_2 of A it is easy to verify that $\lambda_1\delta_1 + \lambda_2\delta_2$ is again a derivation of A.

Definition 1.10 (Lie algebra of derivations). *Let A be a $\mathbb{K}$-algebra and $\operatorname{Der}_{\mathbb{K}}(A)$ the space of all derivations of A. Then $\operatorname{Der}_{\mathbb{K}}(A)$ is a Lie algebra with the commutator bracket (using the composition of functions), i.e. for $\delta_1, \delta_2 \in \operatorname{Der}_{\mathbb{K}}(A)$:*

$$[\delta_1, \delta_2] = \delta_1 \circ \delta_2 - \delta_2 \circ \delta_1 \tag{15}$$

Example 1.11 (Derivations in Polynomial rings). *Let $A = \mathbb{K}[x_1, \dots, x_n]$ be the polynomial ring in n variables. Then the usual partial derivations $\frac{\partial}{\partial x_i}$, for $1 \le i \le n$, are derivations of A. Let $f_1, \dots, f_n \in A$ be polynomials, then*

$$\delta = f_1 \frac{\partial}{\partial x_i} + \cdots + f_n \frac{\partial}{\partial x_n} \tag{16}$$

is a derivation, since A is commutative. Moreover, given any $\delta \in \operatorname{Der}_{\mathbb{K}}(A)$ we set $f_i := \delta(x_i)$. Then by induction, using the Leibniz rule, one shows that $\delta(x_i^m) = mx^{m-1}f_i = f_i\frac{\partial}{\partial x_i}(x_i^m)$. For an arbitrary monomial $w = x_1^{m_1} \cdots x_n^{m_n}$ one concludes similarly

$$\delta(w) = f_1 \frac{\partial}{\partial x_1}(w) + \cdots + f_n \frac{\partial}{\partial x_n}(w). \tag{17}$$

Thus $\operatorname{Der}_{\mathbb{K}}(A) = \sum_{i=1}^n A\frac{\partial}{\partial x_i}$ is a finitely generated as A-module (actually free of rank n for a polynomial ring).

Example 1.12. *In contrast to the last example, the Skolem-Noether Theorem says that the Lie algebra of derivation* $\operatorname{Der}_{\mathbb{K}}(A)$*, for $A = M_n(\mathbb{K})$ consists only of* inner derivations, *i.e. derivations of the form $\delta(a) = [a, x] = ax - xa$, for some element $x \in A$.*

Definition 1.13 (Representations of Lie algebras). *Given a Lie algebra $\mathfrak{g}$ over a field $\mathbb{K}$. A representation of $\mathfrak{g}$ on a vector space V is a homomorphism of Lie algebras $\rho : \mathfrak{g} \to \operatorname{End}(V)$, where $\operatorname{End}(V)$ is seen as a Lie algebra with commutator bracket. In case V is finite dimensional one can identify the Lie algebra $\operatorname{End}(V)$ with the general linear algebra $\mathfrak{gl}(n, \mathbb{K}) =: \mathfrak{gl}(V)$.*

Example 1.14 (the adjoint map). *The adjoint map of a (finite dimensional) Lie algebra $\mathfrak{g}$ is*

$$\mathrm{ad} : \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g}), \qquad x \mapsto (\mathrm{ad}\, x) : [y \mapsto [x, y]] \tag{18}$$

This map is a homomorphism of Lie algebras, due to the Jacobi identity:

$$[(\mathrm{ad}x), (\mathrm{ad}y)](z) = [x, [y, z]] - [y, [x, z]] = [z, [y, x]] = [[x, y], z] = (\mathrm{ad}[x, y])(z). \tag{19}$$

Hence ad *turns* $\mathfrak{g}$ *into a representation over* $\mathfrak{g}$

2. Lecture: Representing $U(\mathfrak{g})$ as ring extensions for small examples

Definition 2.1 (Free Algebra). *The free algebra over a set X is the vector space $T\langle X\rangle$ over $\mathbb{K}$ with basis the words $w = x_1 \cdots x_m$ with letters $x_i \in X$, The multiplication is given by concatenation of words, i.e. for words $v = x_1 \cdots x_m$ and $w = y_1 \cdots y_n$ of length m and n one defines the word $vw = x_1 \cdots x_m y_1 \cdots y_n$ of length $n + m$ as their product. By definition there exists an* empty word *ω, i.e. a word of length 0, which serves as identity element of the multiplication.*[1]

Theorem 2.2 (Universal Property of the free algebra). *For any set X, algebra A and function $f : X \to A$, there exists a unique* algebra *homomorphism $\widetilde{f} : T\langle X\rangle \to A$, such that $\widetilde{f}(x) = f(x)$, for all $x \in X$.*

Proof. Defne $\widetilde{f} : T(X) \to A$ by $\widetilde{f}(x_1 \dots x_m) := f(x_1) \cdots f(x_m)$, for all words $x_1 \cdots x_m$ in X. One checks $\widetilde{f}(vw) = f(x_1) \cdots f(x_m) f(y_1) \cdots f(y_m) = \widetilde{f}(v)\widetilde{f}(w)$, for $w = x_1 \cdots x_m$ and $w = y_1 \cdots y_n$. The uniqueness is left to the reader. □

Definition 2.3 (Enveloping Algebra). *Let $\mathfrak{g}$ be a finite dimensional Lie algebra with bracket $[-, -]$ and basis X. The* universal enveloping algebra *of $\mathfrak{g}$ is defined as*

$$U(\mathfrak{g}) = \frac{T\langle X\rangle}{\langle xy - yx - [x, y] : x, y \in X\rangle}. \tag{20}$$

Moreover, $i : \mathfrak{g} \to U(\mathfrak{g})$ with $i(x) = \overline{x}$, for $x \in \mathfrak{g}$, is a Lie algebra homomorphism.

Suppose $\mathfrak{g}$ has basis $X = \{x_1, \dots, x_n\}$. Note that if $\mathfrak{g}$ is Abelian, i.e. $[-, -] \cong 0$, then $U(\mathfrak{g}) = \mathbb{K}[x_1, \dots, x_n]$ is the commutative polynomial ring in n variables, which as a vector space has an ordered basis $\{x_1^{m_1} \cdots x_n^{m_n} : m_i \geq 0\}$. In general, if $j > i$, then $x_j x_i = x_i x_j + [x_j, x_i]$. Hence any element $x_j x_i$ of length 2 can be reordered to $x_i x_j$, with $i < j$, plus an element of length 1. Therefore it is clear that the set $\{x_1^{m_1} \cdots x_n^{m_n} : m_i \geq 0\}$, consisting of so-called *standard monomials* is always a generating set of $U(\mathfrak{g})$ as $\mathbb{K}$-vector space. Although it is not obvious, that this set is also a basis, the *Poincaré-Birkhoff-Witt Theorem* says exactly that, namely that the set of standard monomials is always a basis of $U(\mathfrak{g})$ as $\mathbb{K}$-vector space, independent of $\mathfrak{g}$ being Abelian or not. As a consequence, one concludes that $i : g \to U(\mathfrak{g})$ is injective and that we can identify the elements of $\mathfrak{g}$ with their representatives in $U(g)$. The universal enveloping algebra has the following universal property:

Theorem 2.4 (Universal Property of $U(\mathfrak{g})$). *Let $\mathfrak{g}$ be a Lie algebra and A an associative algebra. For any homomorphism of Lie algebras $f : \mathfrak{g} \to A$, where A is considered a Lie algebra with commutator bracket, there exists a unique homomorphism of associative algebras $\overline{f} : U(\mathfrak{g}) \to A$ such that $f(x) = \overline{f}(x)$, for all $x \in \mathfrak{g}$.*

Proof. Let X be a basis of $\mathfrak{g}$. By the universal property of the free algebra $T\langle X\rangle$, Theorem 2.2, there exists a unique algebra homomorphism $\widetilde{f} : T\langle X\rangle \to A$, extending f. For any $x, y \in \mathfrak{g}$ we calculate:

$$\widetilde{f}(xy - yx - [x, y]) = f(x)f(y) - f(y)f(x) - f([x, y]) = [f(x), f(y)] - f([x, y]) = 0, \tag{21}$$

[1] The free algebra is nothing but the monoid algebra of the monoid of words in X over $\mathbb{K}$.

since f is a homomorphism of Lie algebras. Hence $\widetilde{f}(I) = 0$, for $I = \langle xy - yx - [x, y] : x, y \in \mathfrak{g}\rangle$ and there exists a unique (well-defined) algebra homomorphism $\overline{f} : U(\mathfrak{g}) = T(\mathfrak{g})/I \to A$ with $\overline{f}(w + I) = \widetilde{f}(w)$, for words w, and which satisfies, $\overline{f}(x + I) = \widetilde{f}(x) = f(x)$. □

Theorem 2.5 (Representations of Lie algebras as modules over $U(\mathfrak{g})$)**.** *Let V be a vector space.*

(1) If $\rho : \mathfrak{g} \to \mathrm{End}(V)$ is a representation over $\mathfrak{g}$, then by the universal property of $U(\mathfrak{g})$ there exists a unique homomorphism of associative algebras $\overline{\rho} : U(\mathfrak{g}) \to \mathrm{End}(V)$, which turns V into a (left) $U(\mathfrak{g})$-module, by

$$h \cdot v = \overline{\rho}(h)(v), \tag{22}$$

for all $v \in V$ and $h \in U(\mathfrak{g})$.

(2) Conversely, if V is a left $U(\mathfrak{g})$-module, then we define

$$\rho : \mathfrak{g} \to \mathrm{End}(V), \qquad \rho(x) = [v \mapsto x \cdot v]. \tag{23}$$

Proof. (1) is clear, since a ring homomorphism $\overline{\rho} : U(\mathfrak{g}) \to \mathrm{End}(V)$ turns V into a left $U(\mathfrak{g})$-module.

(2) Note that given $x, y \in \mathfrak{g}$, then in $U(\mathfrak{g})$ we have $xy - yx = [x, y]$. Hence for all $v \in V$:

$$[\rho(x), \rho(y)](v) = (\rho(x)\rho(y) - \rho(y)\rho(x))(v) = x \cdot y \cdot v - y \cdot x \cdot v = [x, y] \cdot v = \rho([x, y])(v). \tag{24}$$

This shows that ρ is a representation of $\mathfrak{g}$. □

Theorem 2.6 (Tensor product)**.** *Let $\mathfrak{g}$ be a Lie algebra.*

(1) There exist unique algebra homomorphisms $\Delta : U(\mathfrak{g}) \to U(\mathfrak{g}) \otimes U(\mathfrak{g})$ and $\epsilon : U(\mathfrak{g}) \to \mathbb{K}$, such that

$$\Delta(x) = 1 \otimes x + x \otimes 1, \qquad \epsilon(x) = 0, \tag{25}$$

for all $x \in \mathfrak{g}$.

(2) Given two left $U(\mathfrak{g})$-modules M, N their tensor product $M \otimes N$ is again a left $U(\mathfrak{g})$-module by

$$x \cdot (m \otimes n) = (x \cdot m) \otimes n + m \otimes (x \cdot n) \tag{26}$$

for all $x \in \mathfrak{g}$, $m \in M$ and $n \in N$.

Proof. (1) Consider the linear map $\Delta' : \mathfrak{g} \to U(\mathfrak{g}) \otimes U(\mathfrak{g})$ defined by (25), then Δ' is a homomorphism of Lie algebras, because for all $x, y \in \mathfrak{g}$:

$$\begin{aligned}
[\Delta'(x), \Delta'(y)] &= (1 \otimes x + x \otimes 1)(1 \otimes y + y \otimes 1) - (1 \otimes y + y \otimes 1)(1 \otimes x + x \otimes 1) \\
&= (1 \otimes xy + y \otimes x + x \otimes y + xy \otimes 1) - (1 \otimes yx + x \otimes y + y \otimes x + yx \otimes 1) \\
&= 1 \otimes (xy - yx) + xy - yx \otimes 1 \\
&= \Delta'([x, y]).
\end{aligned}$$

By the universal property of $U(\mathfrak{g})$, Theorem 2.4, there exists a unique algebra homomorphism $\Delta : U(\mathfrak{g}) \to U(\mathfrak{g}) \otimes U(\mathfrak{g})$ extending Δ'.

Similarly, if we let $\epsilon' : \mathfrak{g} \to \mathbb{K}$ be the linear map that sends x to 0, then ϵ' is a homomorphism of Lie algebras and there exists a unique algebra homomorphism $\epsilon : U(\mathfrak{g}) \to \mathbb{K}$ extending ϵ'.

(2) Since $[x, y] \cdot m = (xy - yx) \cdot m$, for any m of an $U(\mathfrak{g})$-module M and $x, y \in \mathfrak{g}$, we conclude $[x, y] \cdot (m \otimes n) = (xy - yx) \cdot (m \otimes n)$, for all $x, y \in \mathfrak{g}$, $m \in M$ and $n \in N$. This shows that the action $\cdot : \mathfrak{g} \to \mathrm{End}(M \otimes N)$ given by (26) is a homomorphism of Lie algebras and hence there exists a unique algebra homomorphism $\cdot : U(\mathfrak{g}) \to \mathrm{End}(M \otimes N)$ that defines a left $U(\mathfrak{g})$-module structure on $M \otimes N$. □

Theorem 2.7 (Enveloping algebras of finite dimensional Lie algebras are Noetherian)**.** *The enveloping algebra $U(\mathfrak{g})$ of a finite dimensional Lie algebra $\mathfrak{g}$ is Noetherian domain.*

Proof. (sketch) $U(\mathfrak{g})$ is filtered by the total degree of the standard monomials, i.e.

$$F_k := \operatorname{span}\left\{ x_1^{m_1} \cdots x_n^{m_n} \ : \ \sum_{i=1}^{n} m_i = k \right\}.$$

Then $F_0 = \mathbb{K}$, $F_1 = \mathfrak{g}$. In particular $F_k F_l \subseteq F_{k+l}$, $F_i \subseteq F_j$, for $i \leq j$ and $\bigcup F_k = U(\mathfrak{g})$. Thus $\{F_k\}_{k\geq 0}$ is a filtration of $U(\mathfrak{g})$. One can therefore form the *associated graded ring*

$$\operatorname{gr} U(\mathfrak{g}) = \bigoplus_{k\geq 0} F_k/F_{k-1}, \tag{27}$$

where $F_{-1} := \{0\}$. An element $a \in U(\mathfrak{g})$ is said to have degree k if $a \in F_k \setminus F_{k-1}$. We call $\overline{a} = a + F_{k-1} \in \operatorname{gr}U(\mathfrak{g})$ the leading term of a. Note that $\overline{a} = 0$ if and only if $a = 0$. Let $b \in U(\mathfrak{g})$ be an element of degree l, then we define

$$\overline{a}\overline{b} := ab + F_{k+l-1}.$$

We easily see that $\mathbb{K}[x_1, \dots, x_n] \simeq \operatorname{gr}U(\mathfrak{g})$, as algebras, where the isomorphism is given by

$$x_1^{m_1} \cdots x_n^{m_n} \mapsto x_1^{m_1} \cdots x_n^{m_n} + F_{m_1+\cdots+m_n}.$$

Thus, $\operatorname{gr}U(\mathfrak{g})$ is a Noetherian domain of Krull dimension equal to $\dim(\mathfrak{g})$. The general Theory on graded rings tells us that if the associated graded ring $\operatorname{gr}U(\mathfrak{g})$ is Noetherian, then so is the graded ring $U(\mathfrak{g})$ (see [5, 1.6.9]). Moreover, if $ab = 0$ in $U(\mathfrak{g})$, then $\overline{ab} = \overline{a}\overline{b}$ in $\operatorname{gr}U(\mathfrak{g}) \simeq \mathbb{K}[x_1, \dots, x_n]$. Hence $a = 0$ or $b = 0$, i.e. $U(\mathfrak{g})$ is a domain. □

Open Problem 2.8. *It is not known whether given a field $\mathbb{K}$ and a Lie algebra $\mathfrak{g}$ such that $U(\mathfrak{g})$ is Noetherian, $\mathfrak{g}$ must be finite dimensional.*

Representing $U(\mathfrak{g})$ as Ore extensions. Let σ be an automorphism of an algebra R. A linear map $\delta : R \to R$ is called a σ-derivation if for all $a, b \in R$:

$$\delta(ab) = \sigma(a)\delta(b) + \delta(a)b. \tag{28}$$

Clear δ is a derivation if and only if it is an *id*-derivation.

Theorem 2.9 (Ore extension)**.** *Given an algebra R, an automorphism $\sigma \in \operatorname{Aut}(R)$ and a σ-derivation δ, there exists a ring $S = R[x; \sigma, \delta]$, such that S is free as left R-module with basis $\{x^i : i \geq 0\}$, such that*

$$xa = \sigma(a)x + \delta(a) \tag{29}$$

for all $a \in R$. The ring $R[x; \sigma, \delta]$ is called an Ore extension of R.

Ore extensions can be realized as a subring of the abelian group of $\mathbb{Z}$-endomorphisms of $R[x]$ (see [5, 1.2.3]. Furthermore, it is known that Ore extensions of Noetherian domains are Noetherian domains. The proof is very similar to Hilbert's basis theorem (see [5, 1.2.9]).

Example 2.10 (Two dimensional Lie algebras)**.** *Suppose* $\operatorname{char}(\mathbb{K}) \neq 2$ *and let* $\mathfrak{g} = \operatorname{span}(x, y)$ *be a Lie algebra with basis $\{x, y\}$. Then*

$$[x, y] = ax + by, \tag{30}$$

for $a, b \in \mathbb{K}$. If $a = b = 0$, then $\mathfrak{g}$ is abelian and $U(\mathfrak{g}) = \mathbb{K}[x, y]$.

Suppose $b \neq 0$ [2] *Set $x' := b^{-1}x$ and $y' = ab^{-1}x + y$, then*

$$[x', y'] = b^{-2}a[x, x] + b^{-1}[x, y] = ab^{-1}x + y = y' \tag{31}$$

[2] if $b = 0$ and $a \neq 0$, then we can simply exchange x and y.

Hence, after a change of basis from $\{x, y\}$ *to* $\{x', y'\}$*, we can assume that any non-abelian two dimensional Lie algebra* $\mathfrak{g}$ *has a basis* $\{x, y\}$ *with* $[x, y] = y$*. The enveloping algebra* $U(\mathfrak{g})$ *can be described as an Ore extension where* $R = \mathbb{K}[y]$*,* $\sigma = id$ *and* $\delta = y\frac{\partial}{\partial y}$ *is the derivation of* R *sending* y *to* y *(check that this is a derivation of* R*):*

$$U(\mathfrak{g}) = \mathbb{K}[y][x; \mathrm{id}, y\frac{\partial}{\partial y}]. \tag{32}$$

Alternatively, we could set $R = \mathbb{K}[x]$ *and consider the automorphism* σ *of* $\mathbb{K}[x]$ *defined by* $\sigma(x) = x - 1$*. Then* $[x, y] = y$ *is equivalent to* $yx = (x - 1)y = \sigma(x)y$*. Thus, we obtain*

$$U(\mathfrak{g}) = \mathbb{K}[x][y; \sigma, 0]. \tag{33}$$

Example 2.11 (Heisenberg Lie algebra)**.** *The three dimensional Heisenberg Lie algebra* $\mathfrak{h}$ *can be seen as the Lie algebra with basis* x, y, z *such that* $[x, y] = z$*. It can be realized as a Lie algebra of matrices, where*

$$x = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \qquad y = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \qquad z = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}. \tag{34}$$

Let $R = \mathbb{K}[y, z]$ *and set* $\sigma = id$ *and* $\delta = z\frac{\partial}{\partial y}$*. Then* $\delta(y) = z$ *and*

$$U(\mathfrak{h}) = \mathbb{K}[y, z][x; z\frac{\partial}{\partial y}]. \tag{35}$$

Although the description of $U(\mathfrak{h})$ *looks very similar to* $U(\mathfrak{g})$*, with* $\mathfrak{g}$ *the two-dimensional non-abelian Lie algebra, they are quite different. For instance,* $\mathfrak{h}$ *is a so-called nilpotent Lie algebra, i.e.* $[\mathfrak{h}, [\mathfrak{h}, \mathfrak{h}]] = 0$*, while* $\mathfrak{g}$ *is not, since* $[\mathfrak{g}, \mathfrak{g}] = \mathbb{K}y$ *and* $[\mathfrak{g}, \mathbb{K}y] = \mathbb{K}[y]$*. Note, that* $Z(U(\mathfrak{h})) = \mathbb{K}[z]$*, while* $Z(U(\mathfrak{g})) = \mathbb{K}$*.*

Example 2.12 ($\mathfrak{sl}_2$)**.** *The three dimensional special linear Lie algebra* $\mathfrak{sl}_2$ *can be seen as the Lie algebra with basis* e, f, h *such that the Serre relation hold (see Example 1.7):*

$$[e, f] = h, \qquad [h, e] = 2e, \qquad [h, f] = -2f. \tag{36}$$

Our aim is to express $U(\mathfrak{sl}_2)$ *as an iterated Ore extension. Set* $R = \mathbb{K}[h]$ *and define the automorphism* σ *of* $\mathbb{K}[h]$ *by* $\sigma(h) = h-2$*. Then* $[h, e] = 2e$ *is equivalent to* $eh = he-2e = \sigma(h)e$*. Let* $S = \mathbb{K}[h][e; \sigma]$ *and define an automorphism* τ *of* S *by setting* $\tau(h) = h + 2$ *and* $\tau(e) = e$*. In order to guarantee that there exists such an automorphism, we must assure* $\tau(eh) = \tau(\sigma(h)e)$*. We have on the left side* $\tau(eh) = e(h + 2) = he - 2e + 2e = he$*, while on the right side we have* $\tau(\sigma(h)e) = \tau(he - 2e) = (h + 2)e - 2e = he$*. Thus,* $\tau(eg) = \tau(\sigma(h)e)$ *holds and we can define the automorphism* τ*.*

Furthermore, we define a τ*-derivation* δ *as* $\delta(h) = 0$ *and* $\delta(e) = -h$*, i.e.* $\delta = -h\frac{\partial}{\partial e}$*. We need to check that* δ *is indeed a* τ*-derivation and will do so only on the generators:*

$$\delta(eh) = \tau(e)\delta(h) + \delta(e)h = -h^2 = (h + 2)(-h) - 2(-h) = \tau(h)\delta(e) + \delta(h)e - 2\delta(e) = \delta(\sigma(h)e).$$

Hence we can form the Ore extension $S[f; \tau, \delta]$ *and have that* $fe = \tau(e)f + \delta(e) = ef - h$*, which is equivalent to* $[e, f] = h$*. We also have* $fh = \tau(h)f + \delta(h) = (h + 2)f$*, which is equivalent to* $[h, f] = -2f$*. Thus we can establish an isomorphism*

$$U(\mathfrak{sl}_2) \simeq \mathbb{K}[h][e; \sigma][f; \tau, \delta] \tag{37}$$

3. Lecture: Group representations and group algebras.

Definition 3.1 (Semigroup ring)**.** *Given a ring* R *and a semigroup* S*. The* semigroup ring $R[S]$ *is defined as follows:*

(1) *As set, $R[S]$ is equal to the direct sum $R^{(S)}$, which is the set of elements $f = (r_s)_{s\in S}$ such that there exists a finite subset $F \subseteq S$ with $r_s = 0$ for all $s \in S \setminus F$. The support of such element f is defined as* $\sup(f) = \{s \in S \mid r_s \neq 0\}$. *Elements of $R[S]$ are written as finite sums $f = \sum r_s\bar{s}$, where $\bar{s}$ is a placeholder for the* coefficient *r_s and where it is understood, that only finitely many coefficients r_s are non-zero.*

(2) *The addition of two elements $f = \sum a_s\bar{s}$ and $g = \sum b_s\bar{s}$ in $R[S]$ is defined as*

$$f + g = \sum (a_s + b_s)\bar{s}. \tag{38}$$

(3) *The multiplication of two elements $f = \sum a_s\bar{s}$ and $g = \sum b_s\bar{s}$ in $R[S]$ is defined as*

$$fg = \sum c_s\bar{s}, \qquad \text{with} \qquad c_s = \left(\sum_{s_1s_2=s} a_{s_1}b_{s_2}\right) \tag{39}$$

Since $\sup(f)$ *and* $\sup(g)$ *are finite, there are only finitely many coefficients c_s that are non-zero and each coefficient $c_n = \sum_{s_1s_2=s} a_{s_1}b_{s_2}$ has only a finite number of non-zero summands.*

If R is unital, with neutral element 1 *and S is a monoid, with neutral element e, then $R[S]$ is unital with neutral element* $1\bar{e}$.

Example 3.2. *Let R be a ring.*

(1) *Let $S = \{e\}$ be the trivial semigroup. Then $R[S] = \{a\bar{e} \mid a \in R\}$ is isomorphic to R.*

(2) *Let $S = \mathbb{N} = \{x^n \mid n \geq 0\}$ and multiplication $x^nx^m = x^{n+m}$ for all numbers $n, m \geq 0$. Then*

$$R[\mathbb{N}] = \left\{ \sum_{n=0}^{\infty} a_nx^n \mid a_n \in R \text{ and only finitely many } a_n \text{ are non-zero} \right\} =: R[x] \tag{40}$$

is the polynomial ring over R in one variable. Note that the multiplication is given by

$$\left(\sum_{n=0}^{\infty} a_nx^n\right)\left(\sum_{n=0}^{\infty} b_nx^n\right) = \left(\sum_{n=0}^{\infty} c_nx^n\right) \tag{41}$$

and $c_n = \sum_{x^ix^j=x^n} a_ib_j = \sum_{i=0}^n a_ib_{n-i}$.

(3) *Let $S = \mathbb{N}^k = \{x_1^{n_1}\cdots x_k^{n_k} \mid n_i \geq 0\}$ be the monoide with $\left(x_1^{n_1}\cdots x_k^{n_k}\right)\left(x_1^{m_1}\cdots x_k^{m_k}\right) := x_1^{n_1+m_1}\cdots x_k^{n_k+m_k}$, then*

$$\begin{aligned} R[\mathbb{N}^k] &= \left\{ \sum_{n_1=0}^{\infty}\cdots\sum_{n_k=0}^{\infty} a_{(n_1,\ldots,n_k)}x_1^{n_1}\cdots x_n^{n_k} \mid a_{(n_1,\ldots,n_k)} \in R \text{ and } a_{(n_1,\ldots,n_k)} = 0 \text{ for almost all} \right\} \\ &=: R[x_1,\ldots,x_n] \end{aligned}$$

Theorem 3.3 (Universal property of the semigroup ring)**.** *Let S be a semigroup and R a ring. For any ring homomorphism $f : R \to R'$ from R to another ring R' and for any function of semigroups $g : S \to R'$ between S and the semigroup $(R', \cdot)$ such that $f(r)g(s) = g(s)f(r)$ for all $r \in R$ and $s \in S$. There exists a unique ring homomorphism $\overline{f} : R[S] \to R'$ such that $\overline{f}(r\bar{s}) = f(r)g(s)$. If f and g are unital, then so is $\overline{f}$.*

Proof. Since any element of $R[S]$ can be uniquely written as $\gamma = \sum_{s\in S} r_s\bar{s}$ with only finitely many coefficients non-zero, we can define $\overline{f} : R[S] \to R'$ by

$$\overline{f}(\gamma) := \sum_{s\in S} f(r_s)g(s). \tag{42}$$

Since $\overline{f}$ is already defined to preserve sums, it is a homomorphism of the additive groups of $R[S]$ and R'. Hence, it is only necessary to check the multiplicativity of $\overline{f}$ at elements of the form $r\bar{s}$. Let $r_1, r_2 \in R$ and $s_1, s_2 \in S$. Then

$$\begin{aligned} \overline{f}((r_1\overline{s_1})(r_2\overline{s_2})) &= \overline{f}(r_1r_2\overline{s_1s_2}) \\ &= f(r_1r_2)g(s_1s_2) \qquad \text{by definition of } \overline{f} \end{aligned}$$

$$
\begin{aligned}
&= f(r_1)f(r_2)g(s_1)g(s_2) && \text{since } f \text{ and } g \text{ are multiplicative}\\
&= f(r_1)g(s_1)f(r_2)f(s_2) && \text{by hypothesis the images of } f \text{ and } g \text{ commute}\\
&= \overline{f}(r_1\overline{s_1})\overline{f}(r_2\overline{s_2}).
\end{aligned}
$$

Suppose there exists another ring homomorphism $h : R[S] \to R'$ such that $h(r\overline{s}) = f(r)g(s)$, then for any $\gamma = \sum_{s\in S} r_s\overline{s} \in R[S]$ also

$$h(\gamma) = \sum_{s\in S} h(r_s\overline{s}) = \sum_{s\in S} f(r_s)g(s) = \overline{f}(\gamma). \tag{43}$$

Hence $h = \overline{f}$. ☐

Note that if R is commutative and $f : R \to Z(R')$ is any ring homomorphism from R to the center of R', then the hypothesis $f(r)g(s) = g(s)f(r)$ is automatically satisfied.

Definition 3.4 (Polycyclic-by-finite groups)**.** *A polycyclic-by-finite group is a group G that admits a normal series*

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G, \tag{44}$$

such that G_i is normal in G_{i+1} and G_{i+1}/G_i is infinite cyclic with G_n/G_{n-1} being finite.

Theorem 3.5. *If R is a left Noetherian ring and G is polycyclic-by-finite group, then $R[G]$ is left Noetherian.*

Proof. see [5] ☐

Open Problem 3.6. *It is not known whether given a field $\mathbb{K}$ and a group G such that $\mathbb{K}[G]$ is Noetherian, G must be polycyclic-by-finite.*

Definition 3.7 (Group representation)**.** *Let G be a finite group and $\mathbb{K}$ a field. A* representation *of G on a vector space V is a group homomorphism $\rho : G \to GL(V) = \{f : V \to V : f \text{ is a linear isomorphism }\}$.*

Example 3.8. *For example if $G = \mathbb{Z}_4 = \langle g : g^4 = e\rangle$, then a representation of G on $V = \mathbb{R}^2$ is for example given by the rotation matrix $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in GL(\mathbb{R}^2)$, i.e. $\rho : G \to GL(\mathbb{R}^2)$ with $\rho(g) = A$, $\rho(g^2) = A^2$, $\rho(g) = A^3$ and $\rho(e)$ being the identity matrix.*

Representations of a group G on a vector space V turns V into a left $\mathbb{K}[G]$-module by defining

$$\lambda : \mathbb{K}[G] \times V \to V, \qquad \left(\sum a_g\overline{g}, v\right) \mapsto \sum a_g\rho(g)(v) \tag{45}$$

Conversely, any left $\mathbb{K}[G]$-module structure λ on V defines a representation of G on V, by setting

$$\rho(g)(v) := \lambda(\overline{g}, v) =: \overline{g}\cdot v, \tag{46}$$

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

Hence, if one wants to study group representations, one can equally consider modules over the group algebra.

Theorem 3.9. *Let $\mathbb{K}$ be a field, G a group and $\mathbb{K}[G]$ its group algebra.*

(1) There exist unique algebra homomorphisms $\Delta : \mathbb{K}[G] \to \mathbb{K}[G] \otimes \mathbb{K}[G]$ and $\epsilon : \mathbb{K}[G] \to \mathbb{K}$ defined by

$$\Delta(g) = g \otimes g, \qquad \epsilon(g) = 1, \tag{47}$$

for all $g \in G$.

(2) For any left $\mathbb{K}[G]$-modules, M and N, the tensor product $M \otimes N$ is a left $\mathbb{K}[G]$-module using Δ, i.e.

$$g \cdot (m \otimes n) = \Delta(g)(m \otimes n) = (g \cdot m) \otimes (g \cdot n) \tag{48}$$

for all $g \in G, m \in M, n \in N$.

Proof. left to the reader. ☐

4. Lecture: Maschke's Theorem for group algebras and block decomposition.

Definition 4.1 (semisimple Modules). *A module M is semisimple if any submodule N of M has a complement in M, i.e. there exists a submodule L of M such that $M = N \oplus L$.*

It is a standard fact that a left R-module M is semisimple if and only if any short exact sequence

$$0 \to N \to M \to L \to 0 \tag{49}$$

splits. In particular, a ring R is called (left) semisimple if and only if every left (and right) R-module is semisimple.

The Wedderburn-Artin Theorem characterizes semisimple rings as finite products of matrix rings over division rings.

Theorem 4.2 (Wedderburn-Artin Theorem). *The following statements are equivalent for a ring R:*

(1) Every left R-module is semisimple, i.e. R is semisimple.
(2) R is a left Artinian ring and $Jac(R) = 0$.
(3) R is isomorphic to a finite direct product of matrix rings over division rings.

Recall that the Jacobson radical of a ring R is defined as

$$Jac(R) = \bigcap \{M \,:\, M \text{ is a left maximal ideal of } R\}.$$

Maschke's Theorem tells us precisely, when a group ring $\mathbb{K}[G]$ is semisimple. Note that for that G has to be finite. The reason is that if $\mathbb{K}[G]$ is semisimple, the trivial $\mathbb{K}[G]$-module $\mathbb{K}$, with $\overline{g} \cdot 1_{\mathbb{K}} = 1_{\mathbb{K}}$, for all $g \in G$, is projective. Hence the augmentation map $\epsilon \,:\, \mathbb{K}[G] \to \mathbb{K}$ given by $\epsilon(\overline{g}) = 1$ splits and there exists $\gamma \,:\, \mathbb{K} \to \mathbb{K}[G]$ and in particular an element $t = \sum_{i=1}^n \lambda_i \overline{h_i} = \gamma(1_{\mathbb{K}}) \in \mathbb{K}[G]$, with $\lambda_i \neq 0$, for all i. Let $g \in G$ and set $f = gh_1^{-1}$. Then

$$\lambda_1 \overline{g} + \sum_{i=2}^{n} \lambda_i \overline{gh_1^{-1}h_i} = \overline{gh_1^{-1}} t = \gamma(\overline{gh_1^{-1}} \cdot 1_{\mathbb{K}}) = \gamma(1_{\mathbb{K}}) = \sum_{i=1}^{n} \lambda_i \overline{h_i}. \tag{50}$$

In particular, as the group elements form a basis of $\mathbb{K}[G]$, we have that $g = h_i$, for some i. In other words $G = \{h_1, \ldots, h_n\}$ and G is finite. Hence, suppose G is finite. Identify $|G| = |G|1_{\mathbb{K}} \in \mathbb{K}$. If $\mathrm{char}(\mathbb{K}) \nmid |G|$, then $|G|$ is non-zero in $\mathbb{K}$ and hence invertible, i.e. $\frac{1}{|G|} \in \mathbb{K}$. Let $\beta \,:\, V \to W$ be any surjective homomprhism of $\mathbb{K}[G]$-modules. Since β is also $\mathbb{K}$-linear, and since V and W are vector spaces, there exists a $\mathbb{K}$-linear section $\gamma \,:\, W \to V$ such that the composition $\beta\gamma = id_W$. If we could define a section as left $\mathbb{K}[G]$-module homomorphism, we would show that any short exact sequence splits and hence $\mathbb{K}[G]$ would be semisimple. This is what we are going to do in case $\mathrm{char}(\mathbb{K}) \nmid |G|$. Define an *averaging function* $\widetilde{\gamma} \,:\, W \to V$ by

$$\widetilde{\gamma}(w) := \frac{1}{|G|} \sum_{g \in G} \overline{g^{-1}} \cdot \gamma\left(\overline{g} \cdot w\right), \qquad \forall w \in W. \tag{51}$$

Then $\widetilde{\gamma}$ is $\mathbb{K}$-linear and also $\mathbb{K}[G]$-linear, because for any $h \in G$ and $w \in W$ we have:

$$\widetilde{\gamma}(\overline{h}w) = \frac{1}{|G|} \sum_{g \in G} \overline{g^{-1}} \cdot \gamma\left(\overline{gh} \cdot w\right) = \frac{1}{|G|} \sum_{g \in G} \overline{hk^{-1}} \cdot \gamma\left(\overline{k} \cdot w\right) = \overline{h}\widetilde{\gamma}(w),$$

where we use that the multiplication of an element with h yields a permutation of the elements of the group. Furthermore,

$$\begin{aligned}
\beta\left(\widetilde{\gamma}(w)\right) &= \beta\left(\frac{1}{|G|} \sum_{g \in G} \overline{g^{-1}} \cdot \gamma\left(\overline{g} \cdot w\right)\right) \\
&= \frac{1}{|G|} \sum_{g \in G} \overline{g^{-1}} \cdot \beta\left(\gamma\left(\overline{g} \cdot w\right)\right) = \frac{1}{|G|} \sum_{g \in G} \overline{g^{-1}} \cdot \left(\overline{g} \cdot w\right) = \frac{1}{|G|} \left(\sum_{g \in G} \overline{g^{-1}g}\right) \cdot w = w
\end{aligned}$$

This means, that $\widetilde{\gamma}$ splits β. Hence we proved that if $\mathrm{char}(K) \nmid |G|$, then any short exact sequence of $\mathbb{K}[G]$-modules splits and $\mathbb{K}[G]$ is semisimple. In the language of group representations, a representations V is called *irreducible* if it is simple as $\mathbb{K}[G]$-module. V is called *completely reducible* if and only if V is a semisimple $\mathbb{K}[G]$-module.

Theorem 4.3 (Maschke[3]). *Let $\mathbb{K}$ be a field. Then $\mathbb{K}[G]$ is semisimple, i.e. every representation over G is completely reducible, if and only if G is finite and* $\mathrm{char}(\mathbb{K}) \nmid |G|$.

Proof. We have already shown that if $\mathrm{char}(\mathbb{K}) \nmid |G|$ and G is finite, then $\mathbb{K}[G]$ is semisimple. Conversely, assume $\mathbb{K}[G]$ is semisimple. We have already seen that G has to be finite. Consider the left ideal $I = \sum_{g\in G} \mathbb{K}[G](\overline{g} - \overline{e})$. Then $\mathbb{K}[G]/I = \mathbb{K}(\overline{e} + I) \simeq \mathbb{K}$ is one-dimensional. Moreover,

$$\overline{h} \cdot (\overline{e} + I) = \overline{h} + I = \overline{e} + I, \qquad \forall h \in G.$$

Suppose $\mathbb{K}[G]$ is semisimple, then the canonical map $\epsilon : \mathbb{K}[G] \to K[G]/I$ splits and there exists $\beta : \mathbb{K}[G]/I \to \mathbb{K}[G]$ such that $\overline{e} + I = \epsilon(\beta(\overline{e} + I))$. Let $x = \beta(\overline{e} + I)$. Then $x = \sum_{g\in G} a_g \overline{g}$ for some $a_g \in \mathbb{K}$. Since $\overline{h} \cdot (\overline{e} + I) = \overline{e} + I$, also $\overline{h}x = x$. This means that

$$\sum_{g\in G} a_g \overline{g} = x = \overline{h}x = \sum_{g\in G} a_g \overline{hg} = \sum_{g\in G} a_{h^{-1}g} \overline{g}. \tag{52}$$

Therefore, all the coefficients of x are equal, i.e. $a_h = a_e$, for any $h \in H$. Let $\lambda = a_e$. Then $x = \lambda \sum_{g\in G} \overline{g}$. Applying ϵ yields

$$\overline{e} + I = \epsilon(x) = \lambda \left(\sum_{g\in G} \overline{g} + I \right) = \lambda |G| (\overline{e} + I).$$

This shows that $1 = \lambda|G|$ and in particular $|G| \neq 0$ in $\mathbb{K}$, i.e. $\mathrm{char}(\mathbb{K}) \nmid |G|$. □

Example 4.4. *Combining Maschke's Theorem with the Wedderburn-Artin Theorem, we have that any group ring $\mathbb{K}[G]$ of a finite group G over a field $\mathbb{K}$ with $\mathrm{char}(\mathbb{K}) \nmid |G|$ must be isomorphic to a direct sum of matrix rings over division rings, i.e.*

$$\mathbb{K}[G] \simeq M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k). \tag{53}$$

The matrix rings $M_{n_i}(D_i)$ are called the blocks of $\mathbb{K}[G]$. Moreover, up to isomorphism there are only k non-isomorphic simple $\mathbb{K}[G]$-modules, i.e. irreducible representations, of dimension $n_1[D_1 : \mathbb{K}], \dots, n_k[D_k : \mathbb{K}]$. Note that there exists always at least one 1-dimensional representation of G, i.e. we must have $D_i = \mathbb{K}$ and $n_i = 1$ for some i.

Some examples: Let $G = C_4 = \langle g : g^4 = e\rangle$ be the cyclic group of order 4 and $\mathbb{K} = \mathbb{Q}$. Then $\mathbb{Q}[C_4] \simeq \mathbb{Q}\times\mathbb{Q}\times\mathbb{Q}(i)$, because $\mathbb{Q}[C_4] \simeq \mathbb{Q}[x]/\langle x^4 - 1\rangle$ sending g to the coset of x modulo $x^4 - 1$. Since $x^4 - 1 = (x-1)(x+1)(x^2+1) \in \mathbb{Q}[x]$, we get (using the Chinese reminder theorem)

$$\mathbb{Q}[C_4] \simeq \mathbb{Q}[x]/\langle x - 1\rangle \times \mathbb{Q}[x]/\langle x + 1\rangle \times \mathbb{Q}[x]/\langle x^2 + 1\rangle \simeq \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}(i). \tag{54}$$

If instead of $\mathbb{Q}$ we take the group ring over $\mathbb{C}$, then $x^2 + 1$ decomposes further an we obtain $\mathbb{C}[C_4] \simeq \mathbb{C}\times\mathbb{C}\times\mathbb{C}\times\mathbb{C}$.

As the smallest non-commutative example we might take $G = S_3$ and $K = \mathbb{C}$. Then $\mathbb{C}[S_3]$ is semisimple and must decompose into a direct product of matrix rings $M_{n_i}(\mathbb{C})$ (note that as $\mathbb{C}$ is algebraically closed, $D_i = \mathbb{C}$). In particular the sum of dimensions of the matrix rings n_i^2 must be equal to 6 and since S_3 is non-Abelian, not all n_i can be equal to 1. Hence the only possibility of dimensions is $1 + 1 + 2^2 = 6$, i.e. $\mathbb{C}[S_3] \simeq \mathbb{C}\times\mathbb{C}\times M_2(\mathbb{C})$. We can also read off from this decomposition, that there any irreducible S_3-representation has dimension 1 or 2 and that there exist exactly two non-isomorphic 1-dimensional irreducible S_3-modules and exactly one 2-dimensional one.

[3]Heinrich Maschke (1853-1908), Biography: MacTutor

The number of conjugacy classes and the dimensions of the centres of finite dimensional division algebras allows us to estimate the number of different blocks of a group ring $\mathbb{K}[G]$. Recall that the relation

$$x \sim y \qquad :\Leftrightarrow \qquad \exists g \in G: \; y = gxg^{-1}$$

is an equivalence relation $\sim$ on a group G and partitions the group into equivalence classes, called *conjugacy classes.*

Lemma 4.5. *Let $\mathbb{K}$ be a field and G a finite group.*

(1) For any conjugacy class $C = [x]_\sim = \{gxg^{-1} : g \in G\}$, the element

$$\underline{C} = \sum_{y \in C} \overline{y}$$

is a central element of the group ring, i.e. $\underline{C} \in Z(\mathbb{K}[G])$.

(2) Let $C_1, \dots, C_k$ be the set of all conjugacy classes of G. Then $(\underline{C_1}, \cdots, \underline{C_k})$ is a $\mathbb{K}$-basis of the centre $Z(\mathbb{K}[G])$ of $\mathbb{K}[G]$.

Proof. (1) Let $h \in G$. For any $y = gxg^{-1} \in C$ we have $hyh^{-1} = y' \in C$, i.e. $hy = y'h$. Thus $hC = Ch$ and

$$\overline{h}\underline{C} = \sum_{y \in C} \overline{hy} = \sum_{y' \in C} \overline{y'h} = \underline{C}\overline{h}. \tag{55}$$

Hence, $\underline{C}$ is central in $\mathbb{K}[G]$.

(2) The elements $\{\overline{g} : g \in G\}$ form an $\mathbb{K}$-basis of $\mathbb{K}[G]$. Thus $\{\underline{C_1}, \dots, \underline{C_k}\}$ is a $\mathbb{K}$-linearly independent set and we only need to show that it is also a generating set of $Z(\mathbb{K}[G])$. Let $x \in Z(\mathbb{K}[G])$. Then x can be written as:

$$x = \sum_{i=1}^{k} \left(\sum_{y \in C_i} r_{i,y} \overline{y} \right), \qquad r_{i,y} \in \mathbb{K}. \tag{56}$$

For all $h \in G$ we have $\overline{h}x = x\overline{h}$, i.e.

$$\sum_{i=1}^{k} \left(\sum_{y \in C_i} r_{i,y} \overline{y} \right) = x = \overline{h}x\overline{h^{-1}} = \sum_{i=1}^{k} \left(\sum_{y \in C_i} r_{i,y} \overline{hyh^{-1}} \right) = \sum_{i=1}^{k} \left(\sum_{y' \in hC_ih^{-1}} r_{i,y'} \overline{y'} \right). \tag{57}$$

Since $C_i = hC_ih^{-1}$, we have that all coefficients $r_{i,y}$ of the same conjugacy class are equal, i.e. there exists $r_i \in \mathbb{K}$ with $r_i = r_{i,y}$, for all $y \in C_i$. Hence $x = \sum_{i=1}^k r_i \underline{C_i}$, showing that $(\underline{C_1}, \dots, \underline{C_k})$ is an $\mathbb{K}$-basis for $Z(\mathbb{K}[G])$. ☐

As a Corollary we can estimate the number of blocks of $\mathbb{K}[G]$ in the semisimple case.

Corollary 4.6. *Let G be a finite group and $\mathbb{K}$ a field such that* $\mathrm{char}(K) \nmid |G|$ *and*

$$R \simeq M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k) \tag{58}$$

with finite dimensional division algebras $D_1, \dots, D_k$. Let m be the number of different conjugacy classes. Then

$$m = [Z(D_1) : \mathbb{K}] + \cdots + [Z(D_k) : \mathbb{K}], \tag{59}$$

where $[Z(D) : \mathbb{K}]$ denotes the dimension of the centre $Z(D)$ of D as a $\mathbb{K}$-vector space. In particular, the number of blocks, e.g. the number of non-isomorphic irreducible representations, is bounded by the number of conjugacy classes, with equality if $Z(D_i) = \mathbb{K}$ for all i.

Proof. By Lemma 4.5, $\dim(Z(\mathbb{K}[G]) = m$ and by the Wedderburn-Artin decomposition

$$Z(\mathbb{K}[G]) \simeq Z(M_{n_1}(D_1)) \times \cdots \times Z(M_{n_k}(D_k)) \simeq Z(D_1) \times \cdots \times Z(D_k) \tag{60}$$

we conclude that $m = \dim(Z(\mathbb{K}[G])) = \sum_{i=1}^k [Z(D_i) : K]$. Since the number k of blocks is the number of non-isomorphic simple $\mathbb{K}[G]$-modules and since $[Z(D_i) : \mathbb{K}] \geq 1$ the last statement follows. ☐

Example 4.7. *Let G be a finite Abelian group. Then two group elements are conjugated if and only if they are equal. Hence the number of conjugacy classes is $|G|$. However, the number of blocks of $K[G] = Z(K[G])$ also depends on the finite field extensions of K.*

(1) $\mathbb{C}[G] = \mathbb{C} \times \cdots \times \mathbb{C} = \mathbb{C}^n$, *where $n = |G|$, since $\mathbb{C}$ is algebraically closed.*
(2) $\mathbb{R}[G] = \mathbb{R}^k \times \mathbb{C}^m$ *such that $n = k + 2m$, for some $m \geq 0$ and $k \geq 1$, since $\mathbb{R}$ and $\mathbb{C}$ are the only finite field extensions. For example, if $G = C_4$ is the cyclic group of 4 elements, then $\mathbb{R}[C_4] = \mathbb{C} \times \mathbb{R} \times \mathbb{R}$, in which case we have that the number of non-isomorphic simples is strictly less than the conjugacy classes of the group.*
(3) *There are many finite field extension of $\mathbb{K} = \mathbb{Q}$ as well as of a finite field $\mathbb{K} = GF(p^n)$, which may occur in the Wedderburn decomposition of a group ring. For example if $G = C_5$ is the cyclic group of order 5, then $\mathbb{Q}[C_5] = \mathbb{Q}(\alpha)\times\mathbb{Q}$, where α is a primitive 5th root of unity. A similar situation occurs if $\mathbb{K} = \mathbb{F}_2$ is the field of two elements, since then $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$ is a factorisation into irreducible plynomials and hence $\mathbb{F}_2[C_5] \simeq \mathbb{F}_2(\alpha) \times \mathbb{F}_2$ for a primitive 5th root of unity α over $\mathbb{F}_2$. However, if $\mathbb{K} = GF(4)$ is the field with 4 elements, then $\mathbb{K}[C_5] \simeq \mathbb{K}(\alpha) \times \mathbb{K}(\beta) \times \mathbb{K}$ decomposes into three fields, where $\mathbb{K}(\alpha)$ and $\mathbb{K}(\beta)$ are field extensions of degree 2 over $\mathbb{K}$.*

Example 4.8. *Let $G = S_3 = \{id, \alpha, \beta, \beta^2, \alpha\beta, \alpha\beta^2\}$ be the group of permutations on three letters, with $\alpha = (12)$ and $\beta = (123)$, then S_3 has three conjugacy classes: $[id] = \{id\}$, $[\alpha] = \{\alpha, \alpha\beta, \alpha\beta^2\}$ and $[\beta] = \{\beta, \beta^2\}$. Hence $\mathbb{C}[S_3]$ has three blocks and their sizes n_1, n_2, n_3 must satisfy $n_1^2 + n_2^2 + n_3^2 = 6$. Thus only one of the $n_i's$ can be different from 1, i.e.*

$$\mathbb{C}[S_3] \simeq M_2(\mathbb{C}) \times \mathbb{C} \times \mathbb{C}. \tag{61}$$

Example 4.9. *Let $G = D_4 = \{id, \tau, \tau^2, \tau^3, \alpha, \alpha\tau, \alpha\tau^2, \alpha\tau^3\}$ be the dihedral group D_4, i.e. the symmetry group on the square, with $\alpha = (12)(34)$ and $\tau = (1234)$, then D_4 has five conjugacy classes: $[id]$, $[\alpha] = \{\alpha, \alpha\tau^2\}$, $[\alpha\tau] = \{\alpha\tau, \alpha\tau^3\}$, $[\tau] = \{\tau, \tau^3\}$ and $[\tau^2] = \{\tau^2\}$. Hence $\mathbb{C}[D_4]$ has five blocks and their sizes n_1, n_2, n_3, n_4, n_5 must satisfy $\sum_{i=1}^5 n_i^2 = 8$. Since $\mathbb{C}[D_4]$ has at leasy one 1-dimensional representation, at least one of the $n_i's$ must be 1 and the only possibility is that one of the $n_i's$ is equal to 2, while the rest is equal to 1, i.e.*

$$\mathbb{C}[D_4] \simeq M_2(\mathbb{C}) \times \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathbb{C}. \tag{62}$$

5. Lecture: Introduction to Hopf algebras bialgebras, convolution product.

A Hopf algebra is an algebra and a coalgebra such that their structures are compatible. Recall that the multiplication and the identity of a $\mathbb{K}$-algebra A can be understood as having $\mathbb{K}$-linear homomorphisms $\mu : A \to A \otimes A$ and $\eta : \mathbb{K} \to A$ such that μ is associative and $\epsilon(1)$ is the identity of A with respect to the multiplication. In diagrams this means

$$\begin{tikzcd}
A \otimes A \otimes A \arrow[r, "\mu\otimes id"] \arrow[d, "id\otimes\mu"'] & A \otimes A \arrow[d, "\mu"] \\
A \otimes A \arrow[r, "\mu"'] & A
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathbb{K} \otimes A \arrow[r, "\eta\otimes id"] & A \otimes A \arrow[d, "\mu"] & A \otimes \mathbb{K} \arrow[l, "id\otimes\eta"'] \\
& A \arrow[ul, "\simeq"] \arrow[ur, "\simeq"'] &
\end{tikzcd}$$

Definition 5.1. *A coassociative coalgebra with counit is a K-vector space C with K-linear maps*

$$\Delta : C \to C \otimes C \text{ the comultiplication}, \qquad \varepsilon : C \longrightarrow K \text{ the counit},$$

such that the following diagrams are commutative:

$$\begin{tikzcd}
C \arrow[r, "\Delta"] \arrow[d, "\Delta"'] & C \otimes C \arrow[d, "id\otimes\Delta"] \\
C \otimes C \arrow[r, "\Delta\otimes id"'] & C \otimes C \otimes C
\end{tikzcd}
\qquad
\begin{tikzcd}
K \otimes C & C \otimes C \arrow[l, "\varepsilon\otimes id"'] \arrow[r, "id\otimes\varepsilon"] & C \otimes K \\
& C \arrow[ul, "\simeq"] \arrow[u, "\Delta"] \arrow[ur, "\simeq"'] &
\end{tikzcd}$$

We will use the so-called Sweedler-notation for the comultiplication of an element c:

$$\Delta(c) = \sum_{(c)} c_1 \otimes c_2 \in C \otimes C. \tag{63}$$

If C is a K-coalgebra and A is a K-algebra, then $\mathrm{Hom}_K(C, A)$ becomes a K-algebra by the *convolution product*:

$$(f \star g)(c) := \sum_{(c)} f(c_1)g(c_2) \tag{64}$$

for all $f, g \in \mathrm{Hom}(C, A)$ and $c \in C$. If ε is the counit of C and $\eta : K \to A$ the unit of A, then $\eta \circ \varepsilon \in \mathrm{Hom}(C, A)$ is the unit of this algebra. In particular $C^* = \mathrm{Hom}(C, K)$ is a K-algebra with unit ε.

Definition 5.2. *A K-algebra B is called* K-bialgebra *if B is a K-coalgebra such that the comultiplication and counit are algebra maps. A K-bialgebra H is called* Hopfalgebra, *if the identity id $\in \mathrm{End}(H)$ has an inverse S w.r.t. the convolution product. S is called the antipode of H. and one has*

$$\sum_{(h)} h_1 S(h_2) = \varepsilon(h) = \sum_{(h)} S(h_1)h_2.$$

Example 5.3. *We list some examples of Hopf algebras*

(1) *Let G be a group. Then $K[G]$ is a Hopf algebra with $\Delta(\overline{g}) = \overline{g} \otimes \overline{g}$ and $\epsilon(\overline{g}) = 1$ and $S(\overline{g}) = \overline{g^{-1}}$ for all $g \in G$.*
(2) *Let X be a set. Then the free algebra $\mathbb{K}\langle X\rangle$ is a Hopf algebra with*

$$\Delta(x) = 1 \otimes x + x \otimes 1, \qquad \epsilon(x) = 0, \qquad S(x) = -x,$$

for any $x \in X$. In particular, if $\mathfrak{g}$ is a Lie algebra over K. Then $H = U(\mathfrak{g})$ is a Hopf algebra with the same coalgebra structure as the free algebra.
(3) *Let G be an algebraic group and $H = \mathcal{O}(G)$ its coordinate ring. Then*

$$\begin{array}{ll} \Delta : \mathcal{O}(G) \to \mathcal{O}(G \times G) \simeq \mathcal{O}(G) \times \mathcal{O}(G) & f \mapsto [(g, h) \mapsto f(gh)] \\ \epsilon : \mathcal{O}(G) \to K & \epsilon(f) = f(1) \\ \epsilon : \mathcal{O}(G) \to \mathcal{O}(G) & f \mapsto [g \to f(g^{-1})] \end{array}$$

Proposition 5.4. *Let H be a bialgebra and M, N left H-module. Then $M \otimes N$ is a left H-module by the action*

$$h \cdot (m \otimes n) := \Delta(h)(m \otimes n) := \sum_{(h)} (h_1 \cdot m) \otimes (h_2 \cdot n), \tag{65}$$

for any $m \in M, n \in N$ and $h \in H$, where $\Delta(h) = \sum_{(h)} h_1 \otimes h_2$ in Sweedler's notation.

Proof. There exists a unique algebra homomorphism $\psi : \mathrm{End}(M) \otimes End(N) \to \mathrm{End}(M \otimes N)$ given by

$$\psi(f \otimes g)(m \otimes n) := f(m) \otimes g(n). \tag{66}$$

Let $\lambda^M : H \to \mathrm{End}(M)$ denote the algebra homomorphisms associated to the left H-module structure on M, i.e. $\lambda^M(h)(m) = h \cdot m$, for $m \in M$ and $h \in H$. Similarly, let $\lambda^N : H \to End(N)$ denote the H-action on N. Then the composition of the algebra homomorphisms

$$\psi \circ (\rho^M \otimes \rho^N) \circ \Delta : H \to H \otimes H \to \mathrm{End}(M) \otimes End(N) \to \mathrm{End}(M \otimes N) \tag{67}$$

is an algebra homomorphism. Explicitly, for $m \in M, n \in N$ and $h \in H$ we calculate:

$$\left(\psi \circ (\rho^M \otimes \rho^N) \circ \Delta(h)\right)(m \otimes n) = \sum_{(h)} \rho^M(h_1)(m) \otimes \rho^N(h_2)(n) = \sum_{(h)} (h_1 \cdot m) \otimes (h_2 \cdot n). \tag{68}$$

□

Note that the field $\mathbb{K}$ is also a left H-module, called the trivial H-module, with H-action $h \cdot 1_{\mathbb{K}} = \epsilon(h)$. For any left H-module M we define:

$$M^H = \{m \in M \mid \forall h \in H : h \cdot m = \epsilon(h)m\}.$$

We have an isomorphism of vector spaces $\mathrm{Hom}_H(\mathbb{K}, M) \longrightarrow M^H$, given by $f \mapsto f(1)$, which is actually a functorial isomorphism between $\mathrm{Hom}_H(\mathbb{K}, -)$ and $(-)^H$.

For $M = H$, we set $\int_l^H = H^H = \{t \in H : \forall h \in H : ht = \epsilon(h)t\}$. Using the right H-module action, we set $\int_r^H = \{t \in H : \forall h \in H : th = \epsilon(h)t\}$.

6. Lecture: Representations of Hopf algebras and tensor categories.

Definition 6.1. *Let H be a Hopf algebra over $\mathbb{K}$. A $\mathbb{K}$-module V is called a (right)* Hopf module *for H, if it satisfies the three conditions:*

(1) V is a right H-module.
(2) V is a right H-comodule.
(3) Compatibility condition: $\Delta_V(v \cdot h) = \sum (v_0 \cdot h_1) \otimes (v_1 \cdot h_2)$, $\forall h \in H, v \in V$.

If V, W are Hopf modules,a $\mathbb{K}$-linear map $f : V \to W$ is said to be a Hopf module map if it is both a module and comodule map.

The compatibility condition for a Hopf module says that $\Delta_V : V \to V \otimes H$ is a morphism of right H-modules, with $V \otimes H$ carrying the right H-module structure as above. Denote by $\mathcal{M}_H^H$ the category of right H-Hopf modules. The *fundamental theorem* of Hopf algebras, proved by Larson and Sweedler in 1969, says that $\mathcal{M}_H^H$ is equivalent to the category of all $\mathbb{K}$-vector spaces (see [3]).

If V is a right Hopf module, the invariant and covariant submodules of V are defined, respectively, to be and

$$V^H = \{v \in V : v \cdot h = \epsilon(h)v, \forall h \in H\} \qquad V^{coH} = \{v \in V : \Delta_V(v) = v \otimes 1_H\}. \tag{69}$$

Given a $\mathbb{K}$-module W, the tensor product $W \otimes H$ can be made into a H-Hopf module by setting

$$(w \otimes h) \cdot g = w \otimes hg, \ \ \forall w \in W, h, g \in H \qquad \Delta_{W \otimes H} = \mathrm{id}_W \otimes \Delta_H. \tag{70}$$

Hopf modules of that form are called trivial The following theorem asserts that all Hopf modules are trivial.

Theorem 6.2 (Fundamental Theorem of Hopf modules (Larson-Sweedler, 1969))**.** *Let V be a right H-Hopf module. Then the multiplication map*

$$\rho : V^{coH} \otimes H \to V, \qquad v \otimes h \mapsto v \cdot h \tag{71}$$

is an isomorphism of Hopf modules, where $V^{coH} \otimes H$ is considered a trivial Hopf module.

Proof. The map $\phi : V \to V^{coH}$ with $\phi(v) = \sum v_0 \cdot S(v_1)$ is well defined.

For $v \in V$ we calculate:

$$\Delta_V(\phi(v)) = \sum \Delta_V(v_{(0)} \cdot S(v_1)) = \sum v_{(0)} \cdot S(v_3) \otimes v_1 S(v_2) = \sum v_{(0)} \cdot S(v_2) \otimes \epsilon(v_1) = v(0) \cdot S(v_1) \otimes 1_H = \phi(v) \otimes 1_H$$

Hence, $\phi(v) \in V^{coH}$. Furthermore, $(\phi \otimes \mathrm{id})\Delta_V : V \to V^{coH} \otimes H$ is the inverse of ρ, because for $v \in V$, we have

$$\rho \circ (\phi \otimes \mathrm{id})\Delta_V(v) = \phi(v_{(0)}) \cot v_1 = v_{(0)} \cdot S(v_1)v_2 = v_{(0)}\epsilon(v_1) = v.$$

If $v \in V^{coH}$ and $h \in H$, then

$$(\phi \otimes \mathrm{id})\Delta_V \circ \rho(v \otimes h) = \sum \phi((v \cdot h)_0) \otimes (v \cdot h)_1 = \sum \phi(v \cdot h_1) \otimes h_2 = \sum v \cdot h_1 S(h_2) h_3 = v \otimes h.$$

□

Let H be a finite dimensional Hopf algebra. We have seen that any right H-comodule is a left H^*-module. In case H is finite dimensional, then H^*-module is a also a H-comodule, by $\Delta_{H^*} : H^* \to H^* \otimes H$ given by $\Delta_{H^*}(f) = \sum f_{(0)} \otimes f_1$ if and only if $(p * f)(h) = \sum p(f_1) f_{(0)}(h)$, for all $p \in H^*, h \in H$. On the other hand, we have that H^* is a right H-module, via $(f \cdot h)(g) := f(gS(h)))$, for all $f \in H^*$ and $h, g \in H$.

Theorem 6.3 (Larson - Sweedler, 1969)**.** . *Let H be a finite dimensional Hopf algebra over $\mathbb{K}$. Then*

(1) H^* is a right Hopf module.
(2) $\dim \int_l^H = \dim \int_r^H = 1$
(3) The antipode S is bijective, and $S(\int_l^H) = \int_r^H$
(4) For any $0 \neq \lambda \in \int_l^{H^*}$, the map $H \to H^*$, given by $h \mapsto h \bullet \lambda$, is an isomorphism of left H-modules.

Proof. (1) is left to the reader.

(2+3) Consider the Hopf module structure on H^*. By the fundamental theorem we have $(H^*)^{coH} \otimes H \simeq H^*$. And, as H is finite dimensional, we get $\dim((H^*)^{coH}) = 1$. Note that $f \in (H^*)^{coH}$ if and only if $\Delta_{H^*}(f) = f \otimes 1_H$ if and only if for all $p \in H^*$ and $h \in H$: $(p * f)(h) = p(1)f(h) = \epsilon_{H^*}(p)f(h)$, which is saying $p * f = \epsilon_{H^*}(p)f$, i.e. $f \in \int_l^{H^*}$. Replacing H^* by H we also have $\dim(\int_l^H) = 1$.

By the Fundamental Theorem we have the isomorphism $\int_l^{H^*} \otimes H \to H^*$ by multiplication, i.e. $\lambda \otimes h \mapsto \lambda \bullet h$. If $h \in \mathrm{Ker}(S)$, then $\lambda \bullet h = S(h) \cdot h = 0$. Thus $h = 0$, which shows that S is injective and as H is finite dimensional, S is bijective.

Since $S(\int_r^H) \subseteq \int_l^H$, as well as $S(\int_l^H) \subseteq \int_r^H$, S injective and $\dim(\int_l^H) = 1$, we obtain $S(\int_l^H) = \int_r^H$.

(4) The Fundamental Theorem and $\dim(\int_l^{H^*}) = 1$ shows again for any $0 \neq \lambda \in \int_l^{H^*}$: $H^* = \lambda \bullet H = S(H) \cdot \lambda$. As S is bijective, $H \cdot \lambda = H^*$. □

The existence of the isomorphism $H \to H^*$ says that H is a *Frobenius Algebras.*

Let $\mathbb{K}$ be a field, G a finite group and $R = \mathbb{K}[G]$ its group ring. The linear functional $\varphi : \mathbb{K}[G] \to \mathbb{K}$ defined by $\varphi\left(\sum_{g \in G} \lambda_g \overline{g}\right) = \lambda_e$ satisfies that it does not contain any non-zero left (nor right) ideal of $\mathbb{K}[G]$. Because for all $x = \sum_{g \in G} \lambda_g \overline{g} \in \mathrm{Ker}(\varphi)$ and $h \in G$ we have

$$0 = \varphi(\overline{h^{-1}}x) = \varphi\left(\sum_{g \in G} \lambda_g \overline{h^{-1}g}\right) = \varphi\left(\sum_{k \in G} \lambda_{hk}\overline{k}\right) = \lambda_h.$$

The importance of this map is that it establishes an isomorphism between $\mathbb{K}[G]$ and $\mathbb{K}[G]^* := \mathrm{Hom}(\mathbb{K}[G], \mathbb{K})$.

Given an algebra A over a field $\mathbb{K}$, A^* becomes a left and right A-module by

$$(a \cdot f)(x) := f(xa), \qquad (f \cdot a)(x) = f(ax), \qquad \forall f \in A^*, a, x \in A$$

With these actions, A^* becomes actually an injective left and right A-module, because if I is a right ideal of A and $f : I \to A^*$ is a right A-linear map. Considering I as a subspace of A, we have a decomposition $A = I \oplus I'$ for some subspace I'. Define $\varphi \in A^*$ by $\varphi(a) = f(a)(1)$ if $a \in I$ and $\varphi(a) = 0$ if $a \in I'$. Then for any $a \in I$ using the A-linearity of f:

$$f(a)(x) = (f(a) \cdot x)(1) = f(ax)(1) = \varphi(ax) = (\varphi \cdot a)(x), \qquad \forall x \in A.$$

Hence $f(a) = \varphi \cdot a$, for any $a \in I$. By Baer's criterion, A^* is an injective right A-module. A similar argument shows that A^* is an injective left A-module.

Theorem 6.4 (Brauer-Nesbitt-Nakayama)**.** *Let A be a finite dimensional algebra over a field $\mathbb{K}$. The following statements are equivalent:*

(a) There exists a $\mathbb{K}$-linear map $\varphi : A \to K$ such that $\mathrm{Ker}(\varphi)$ does not contain any non-zero right ideal.

(b) There exists an isomorphism $\Theta : A \to A^*$ of right A-modules.
(c) There exists a bilinear map $\beta : A \times A \to \mathbb{K}$ that is non-degenerated and associative, i.e. $\beta(ab, c) = \beta(a, bc)$, for all $a, bc \in A$.
(d) Any of the statement (a),(b) holds with "right" being replaced by "left".

Proof. $(a) \Rightarrow (c)$ Define $\beta : A \times A \to \mathbb{K}$ by $\beta(a, b) := \varphi(ab)$. Then β is bilinear and $\beta(ab, c) = \varphi(abc) = \beta(a, bc)$ holds for all $a, b, c \in A$. Moreover if $\beta(a, A) = 0$ for some $a \in A$, then $\varphi(aA) = \beta(a, A) = 0$ implies aA is a right ideal contained in $\mathrm{Ker}(\varphi)$ and hence zero, i.e. $a = 0$. Since A is finite dimensional, a result in Linear Algebra shows that any left non-degenerated bilinear form is also right non-degenerated. Hence β is non-degenerated.

$(c) \Rightarrow (b)$ Define $\Theta : A \to A^*$ by $\Theta(a) := \beta(a, -) : [b \mapsto \beta(a, b)]$. Then Θ is well-defined and K-linear. Moreover, $\Theta(a) = 0$ implies $\beta(a, A) = \Theta(a)(A) = 0$. Since β is non-degenerated, $a = 0$, i.e. Θ is injective and as $\dim(A) = \dim(A^*)$, Θ is bijective. Furthermore, for any $a, a' \in A$:

$$\Theta(aa')(b) = \beta(aa', b) = \beta(a, a'b) = \Theta(a)(a'b) = (\Theta(a) \cdot a')(b), \qquad \forall b \in A.$$

shows $\Theta(aa') = \Theta(a) \cdot a'$. Hence Θ is an isomorphism of right A-modules.

$(b) \Rightarrow (a)$ Define $\varphi : A \to K$ by $\varphi(a) := \Theta(1)(a)$, for all $a \in A$. Then φ is K-linear. For any $a \neq 0$ we have $\Theta(a) \neq 0$. Hence there exists $b \in A$ such that

$$\varphi(ab) = \Theta(1)(ab) = (\Theta(1) \cdot a)(b) = \Theta(a)(b) \neq 0.$$

Hence, $aA \not\subseteq \mathrm{Ker}(\varphi)$.

$(c) \Leftrightarrow (d)$ Since (c) is independent from one side, properties (a) and (b) can be obtained analogously for "left" instead of "right". For instance in $(c) \Rightarrow (b)$ we could have defined $\Theta' : A \to A^*$ with $\Theta'(a) := \beta(-, a) : [b \mapsto \beta(b, a)]$.

□

Definition 6.5. *A finite dimensional algebra A is called a Frobenius algebra if it satisfies any of the conditions of the Brauer-Nesbritt-Nakayama Theorem.*

The Larson-Sweedler Theorem says that for any finite dimensional Hopf algebra H there exist an isomorphism of H-modules $H \simeq H^*$. Hence H is Frobenius.

Corollary 6.6. *A finite dimensional Frobenius algebra is left and right self-injective. In particular, any finite dimensional Hopf algebra, e.g. a group ring of a finite group over a field, is left and right self-injective.*

7. Lecture: Maschke's Theorem for Hopf algebras and Larson-Sweedler Theorem

It is known that finite dimensional Frobenius algebras have global dimension 0 or infinite. Algebras of global dimension 0 are semisimple.

Theorem 7.1 (Maschke's Theorem for Hopf algebras)**.** *The following statements are equivalent for a Hopf algebra H over a field $\mathbb{K}$:*

(a) H is a semisimple artinian $\mathbb{K}$-algebra;
(b) $(-)^H$ is an exact functor;
(c) $\exists t \in \int_l^H$ such that $\epsilon(t) = 1$.

In this case H is finite dimensional.

Proof. $(a) \Rightarrow (b)$ We have seen already that for a left H-module M, $\mathrm{Hom}_H(\mathbb{K}, M) \simeq M^H$, given by $f \mapsto f(1)$. In particular, the functors $(-)^H$ and $\mathrm{Hom}_H(\mathbb{K}, -)$ are isomorphic. If H is semisimple, then $\mathrm{Hom}_H(\mathbb{K}, -)$ is exact.

$(b) \Rightarrow (c)$ For $M = H$, the exactness means that $\epsilon : H \to \mathbb{K}$ splits, i.e. there exists $\gamma \in \mathrm{Hom}_H(\mathbb{K}, H)$, such that $\epsilon(\gamma(1)) = 1$. Set $t = \gamma(1) \in \int_l^H$, then $\epsilon(t) = 1$.

$(c) \Rightarrow (a)$ Let M, N be left H-modules and $f : M \to N$ an epimorphism of left H-modules that splits. Since M and N are vector spaces, there exists a linear map $g : N \to M$ such that $fg = id_N$. Let $t \in \int_l^H$ with $\epsilon(t) = 1$ and define $\tilde{g} : N \to M$ given by

$$\tilde{g}(n) = \sum t_1 g(S(t_2) \cdot n), \qquad \forall n \in N. \tag{72}$$

Then one can check that $\tilde{g}$ is left H-linear. Moreover, using the H-linearity of f, we have for $n \in N$:

$$f(\tilde{g}(n)) = \sum t_1 fg(S(t_2) \cdot n) = \sum t_1 S(t_2) \cdot n = \epsilon(t)n = n.$$

□

Theorem 7.2 (Larson-Radford, 1988). *Let H be a finite dimensional Hopf algebra. Suppose* $\mathrm{char}(\mathbb{K}) = 0$. *Then H is semisimple if and only if H^* is semisimple if and only if $S^2 = \mathrm{id}$.*

Proof. see [2] □

Corollary 7.3 (Finite dimensional commutative or cocommutative Hopf algebras are semisimple)**.** *Let H be a finite dimensional semisimple Hopf algebra over $\mathbb{K}$.*

(1) H is cocommutative if and only if $H = \mathbb{K}[G]$, for some group G.
(2) H is commutative if and only if $H = \mathbb{K}[G]^*$, for some group G.

Semisimple Hopf algebras that are commutative or cocommutative are called trivial

8. Lecture: Constructing semisimple Hopf algebras

This last part is based on my preprint [4]. We will assume $\mathrm{char}(\mathbb{K}) = 0$.

Definition 8.1 (Kac-Paljutkin algebra). *H_8 is the algebra generated by x, y, z over $\mathbb{K}$ subject to*

$$xy = yx, \qquad x^2 = 1 = y^2, \qquad xz = zy, \qquad yz = zx$$
$$z^2 = \frac{1}{2}(1 + x + y - xy)$$

with coalgebra structure given by x and y group-like and

$$\Delta(z) = \frac{1}{2}(1 \otimes 1 + x \otimes 1 + 1 \otimes y - x \otimes y)(z \otimes z), \qquad \epsilon(z) = 1, \qquad S(z) = z.$$

Definition 8.2 (Pansera's algebra). *H_{2n^2} is the algebra generated by x, y, z over $\mathbb{K}$ subject to*

$$xy = yx, \qquad x^n = 1 = y^n, \qquad xz = zy, \qquad yz = zx$$
$$z^2 = \frac{1}{n}\left(\sum_{i,j=0}^{n-1} q^{-ij} x^i y^j\right),$$

where q is a primitive nth root of unity. The coalgebra structure is given by x and y being group-like and

$$\Delta(z) = \frac{1}{n}\left(\sum_{i,j=0}^{n-1} q^{-ij} x^i \otimes y^j\right)(z \otimes z), \qquad \epsilon(z) = 1, \qquad S(z) = z.$$

Proposition 8.3 (Skew-polynomial ring as bialgebra)**.** *Let B be an bialgebra, σ an automorphism of B and $J \in B \otimes B$ an invertible element. Then the following statements are equivalent:*

(a) $B[z;\sigma]$ is a bialgebra with B a subalgebra and $\Delta(z) = J(z \otimes z)$, $\epsilon(z) = 1$;
(b) (σ, J) is a twisted automorphism, i.e.
  (a) $(\Delta \otimes id)(J)(J \otimes 1) = (id \otimes \Delta)(J)(1 \otimes J)$
  (b) $(\epsilon \otimes id)(J) = 1 = (id \otimes \epsilon)(J)$
  (c) $\Delta(\sigma(b)) = J^{-1}(\sigma \otimes \sigma)\Delta(b)J$, for all $b \in B$

(d) $\epsilon\sigma = \epsilon$

Definition 8.4 (Drinfeld twist)**.** *An invertible element $J \in B \otimes B$ is called a Drinfeld twist if*

(1) $(\Delta \otimes id)(J)(J \otimes 1) = (id \otimes \Delta)(J)(1 \otimes J)$
(2) $(\epsilon \otimes id)(J) = 1 = (id \otimes \epsilon)(J)$

Let Σ_m denote the symmetric group on m letters. The standard generators $s_1, \dots, s_{m-1}$ of Σ_m, i.e. the transpositions $s_i = (i, i+1)$, generate a free monoid $M = \langle \overline{s}_1, \dots, \overline{s}_{m-1} \rangle$ that acts on $R = B^{\otimes m}$, with $B = \mathbb{K}\mathbb{Z}_n$, and allows to consider the skew monoid algebra $R\#M$, which in the case $m = 2$ corresponds to the skew polynomial ring $R[z; \sigma]$. The comultiplication of $\overline{s_i}$ can be defined as $\Delta(\overline{s}_i) = J_i(\overline{s}_i \otimes \overline{s}_i)$, for a suitable twist $J_i \in R \otimes R$. Under further assumptions on these twists J_i, we define a Hopf structure on the quotient $R\#M/I$, where I is the ideal generated by the usual relations of the symmetric group, $\overline{s}_i\overline{s}_{i+1}\overline{s}_i = \overline{s}_{i+1}\overline{s}_i\overline{s}_{i+1}$ and $\overline{s}_i\overline{s}_j = \overline{s}_j\overline{s}_i$ for $|i-j| > 1$, but with $\overline{s}_i^2 = t_i := \mu_R(J_i)$, where μ_R is the multiplication of R. The obtained Hopf algebra H is an extension of $\mathbb{K}\Sigma_m$ by R and can be considered a crossed product $R\#_\gamma\Sigma_m$ for a suitable 2-cocycle $\gamma : \Sigma_m \times \Sigma_m \to R^\times$. For $B = \mathbb{K}[\mathbb{Z}_n]$ and $\mathbb{K}$ containing a primitive nth root of unity, we provide twists J_i that satisfy all our assumptions and yield a family of semisimple Hopf algebras $H_{n,m} = \mathbb{K}[\mathbb{Z}_n]^{\otimes m}\#_\gamma\Sigma_m$ of dimension $n^m m!$. The original Kac-Paljutkin Hopf algebra appears as $H_{2,2}$, while Pansera's algebras appear as $H_{n,2}$.

Definition 8.5 (Skew Monoid algebras)**.** *Given a ring R and a monoid M, such that there exists a homomorphism of monoids $\rho : M \to \mathrm{End}(R)$ with $\rho(m)$ being a ring endomorphism of R. Then $S = R \otimes \mathbb{K}[M]$ carries an algebra structure given by*

$$(a \otimes m)(b \otimes n) = a\rho(m)(b) \otimes mn,$$

for $a, b \in R, m, m \in M$. The algebra S is denoted by $R\#M$ and called the skew monoid algebra. We will denote the action of M on R by ${}^m a =: \rho(m)(a)$.

Let $B = \mathbb{K}[\mathbb{Z}_n]$ and q a primitive nth root of unity in $\mathbb{K}$. Set

$$J = \frac{1}{n}\sum_{i,j=0}^{n-1} q^{-ij}x^i \otimes x^j \in B \otimes B$$

then J is a Drinfeld twist of B.

For $1 \le i \le m$ consider the embedding $e_i^m : B \to B^{\otimes m}$.

Lemma 8.6. *$(e_i^m \otimes e_j^m)(J)$ is a twist for $B^{\otimes m} \otimes B^{\otimes m}$, for any $1 \le i < j \le m$.*

Theorem 8.7 (Extension by the symmetric group)**.** *Let $n, m \ge 1$, $B = \mathbb{K}[\mathbb{Z}_n]$, with $\mathbb{Z}_n = \langle x : x^n = 1 \rangle$, q a primitive nth root of unity and $J = \frac{1}{n}\sum_{i,j=0}^{n-1} q^{-ij}x^i \otimes x^j$. Consider the free monoid M on $X = \{s_1, \dots, s_{m-1}\}$, where $s_i = (i, i+1)$ is the transposition in the symmetric group Σ_m. Set $R = B^{\otimes m}$.*

(1) $R\#M$ is a bialgebra with

$$\Delta(\overline{s}_i) = J_i(\overline{s}_i \otimes \overline{s}_i), \qquad \epsilon(\overline{s}_i) = 1,$$

for $1 \le i < m$ and $J_i = (e_i^m \otimes e_{i+1}^m)(J)$.

(2) The ideal I of $R\#M$ generated by

$$\overline{s}_i^2 - t_{s_i}, \qquad \overline{s}_i\overline{s}_{i+1}\overline{s}_i - \overline{s}_{i+1}\overline{s}_i\overline{s}_{i+1}, \qquad \overline{s}_i\overline{s}_j - \overline{s}_j\overline{s}_i, \qquad \forall i, j \text{ with } |i-j| > 1.$$

is a biideal of $R\#M$.

(3) $H = (R\#M)/I$ is a Hopf algebra of dimension $\dim(R)^n n!$ with Hopf subalgebra $R^{\otimes n}$ and Hopf quotient $\mathbb{K}\Sigma_m$. Furthermore,

(a) $\{\overline{w} : w \in \Sigma_m\}$ is an R-basis of H;

(b) *there exists a 2-cocycle $\gamma : \Sigma_m \times \Sigma_m \to Z(R)^\times$ such that $H \simeq R\#_\gamma \Sigma_m$ with multiplication given by*

$$(a\#\overline{w})(b\#\overline{v}) = a\sigma_w(b)\gamma(w,v)\#\overline{wv}. \tag{73}$$

for all $a, b \in R$ and $w, v \in \Sigma_m$, where $\gamma(w,v)$ is a product of elements $\sigma_u(t_s)$, for some $u \in \Sigma_m$ and $s \in X$.

(c) *$\epsilon(\gamma(w,v)) = 1$, for all $w, v \in \Sigma_m$.*

(d) *H is semisimple with integral $\int \sum_{w\in\Sigma_m} \overline{w}$, where $\int$ is the integral of R.*

Proof. See [4]. □

Example 8.8 (Case $m = 3$). *Let q be a primitive third root of unity. Write x for the generator of $B = \mathbb{K}\mathbb{Z}_n$ and $R = B^{\otimes 3} = \mathbb{K}\mathbb{Z}_n \otimes \mathbb{K}\mathbb{Z}_n \otimes \mathbb{K}\mathbb{Z}_n$. Elements of R are linear combinations of monomials $x_1^i x_2^j x_3^k$, where x_1 stands for $x \otimes 1 \otimes 1$, x_2 stands for $1 \otimes x \otimes 1$ and x_3 stands for $1 \otimes 1 \otimes x$. The transpositions $s_1 = (12)$ and $s_2 = (23)$ are generators of Σ_3. Write $\sigma_i = \sigma_{s_i}$ for the corresponding automorphism of R. The twist $J = \sum_{j=0}^{n-1} e_j \otimes x^j$ for $\mathbb{K}\mathbb{Z}_n$ yields two twists*

$$J_{s_1} = \frac{1}{n}\sum_{i,j=0}^{n-1} q^{-ij} x_1^i \otimes x_2^j \qquad \text{and} \qquad J_{s_2} = \frac{1}{n}\sum_{i,j=0}^{n-1} q^{-ij} x_2^i \otimes x_3^j$$

for R. Set $z_1 := \overline{s_1}$ and $z_2 := \overline{s_2}$ for the generator of the free monoid $M = \langle \overline{s_1}, \overline{s_2}\rangle$. The Hopf algebra

$$H_{n,3} = (R\#M)/\langle z_1^2 - t_1, z_2^2 - t_2, z_1z_2z_1 - z_2z_1z_2\rangle = (\mathbb{K}\mathbb{Z}_n)^{\otimes 3} \#_\gamma \Sigma_3 \tag{74}$$

has therefore generators x_1, x_2, x_3, z_1, z_2 subject to $x_ix_j = x_jx_i$ and $x_i^n = 1$, for all i, j and

$$z_1x_1 = x_2z_1, \quad z_1x_2 = x_1z_1, \quad z_1x_3 = x_3z_1$$

$$z_2x_1 = x_1z_2, \quad z_2x_2 = x_3z_2, \quad z_2x_3 = x_2z_2$$

$$z_1z_2z_1 = z_2z_1z_2, \qquad z_1^2 = t_1 := \frac{1}{n}\sum_{i,j=0}^{n-1} q^{-ij}x_1^ix_2^j, \qquad z_2^2 = t_2 := \frac{1}{n}\sum_{i,j=0}^{n-1} q^{-ij}x_2^ix_3^j.$$

While the x_i are group-like, we have

$$\Delta(z_1) = \left(\frac{1}{n}\sum_{i,j=0}^{n-1} q^{-ij}x_1^i \otimes x_2^j\right)(z_1 \otimes z_1) \qquad \Delta(z_2) = \left(\frac{1}{n}\sum_{i,j=0}^{n-1} q^{-ij}x_2^i \otimes x_3^j\right)(z_2 \otimes z_2).$$

$H_{n,3}$ has dimension $6n^3$ and basis $\left\{x_1^ix_2^jx_3^k\overline{w} : 0 \le i, j, l < n,\ \overline{w} \in \{1, z_1, z_2, z_1z_2, z_2z_1, z_1z_2z_1\}\right\}$. The 2-cocycle γ is determined by the multiplication in $H_{n,3}$ and given by $\gamma(\mathrm{id}, w) = \gamma(w, \mathrm{id}) = 1$, for $w \in \Sigma_3$, and the following table. Note that $\sigma_1\sigma_2(t_1) = t_2$ and $\sigma_1(t_2) = \sigma_2(t_1) = \frac{1}{n}\sum_{i,j=0}^{n-1} q^{-ij}x_1^ix_3^j$.

γ	s_1	s_2	s_1s_2	s_2s_1	$s_1s_2s_1$
s_1	t_1	1	t_1	1	t_1
s_2	1	t_2	1	t_2	t_2
s_1s_2	1	$\sigma_2(t_1)$	t_1	$t_1\sigma_2(t_1)$	$t_1\sigma_2(t_1)$
s_2s_1	$\sigma_1(t_2)$	1	$t_2\sigma_1(t_2)$	t_2	$t_2\sigma_1(t_2)$
$s_1s_2s_1$	t_2	t_1	$t_2\sigma_1(t_2)$	$t_1\sigma_2(t_1)$	$t_1t_2\sigma_2(t_1)$

Remark 8.9. *We see, that $H_{n,2}$ embeds into $H_{n,3}$ by sending x, y, z of $H_{n,2}$ to the corresponding elements x_1, x_2, z_1 in $H_{n,3}$. More generally, for $n, m \ge 2$, the algebra $R = \mathbb{K}\mathbb{Z}_n^{\otimes m}$ embeds into $R' = \mathbb{K}\mathbb{Z}_n^{\otimes m+1}$ by sending $a_1 \otimes \cdots \otimes a_m$ into $a_1 \otimes \cdots \otimes a_m \otimes 1_B$. Similarly, Σ_m can be considered a subgroup of Σ_{m+1}, where we identify the generators $s_1, \ldots, s_{m-1}$ with the first $m-1$ generators of Σ_{m+1}. Hence, if $x_1, \ldots, x_m$ denotes the basis of $R = \mathbb{K}\mathbb{Z}_n^{\otimes m+1}$ and $z_1, \ldots, z_{m-1}$ the remaining algebra generators of $H_{n,m}$ and if $x_1', \ldots, x_{m+1}'$ denote the basis of R' and $z_1', \ldots, z_{m+1}'$ the remaining generators of $H_{n,m+1}$, then mapping x_i to x_i' and z_i to z_i' yields an algebra embedding of $H_{n,m}$ into $H_{n,m+1}$, which is also an embedding of Hopf algebras.*

Remark 8.10. *Let $H = H_{n,m}$ and $w \in \Sigma_m$. We claim that the comultiplication of $\overline{w}$ in H looks like $\Delta(\overline{w}) = J(w)(\overline{w} \otimes \overline{w})$ for an invertible element $J(w) \in R \otimes R$ with $\epsilon(\mu_R(J(w))) = 1$. We will prove this by induction on the length of the chosen representation $w = s_{i_1} \dots s_{i_k}$ in the generators $s_1, \dots s_{m-1}$. For $k = 1$, we have $w = s_i$, for some i and by definition $\Delta(z_i) = J_i(z_i \otimes z_i)$ for $z_i = \overline{s_i}$ and $J_i = J_{s_i} = (e_i^m \otimes e_{i+1}^m)(J)$, which is invertible, since J is invertible. Moreover, $\mu_R(J_i) = e_{i,i+1}^m(J) = t_i$ and $\epsilon(t_i) = 1$. Now suppose that $w = s_i v$ has length greater than 1, where $v \in \Sigma_m$ and there exists $J(v) \in R \otimes R$ such that $\Delta(\overline{v}) = J(v)(\overline{v} \otimes \overline{v})$. Then*

$$\Delta(\overline{w}) = J_i(z_i \otimes z_i)J(v)(\overline{v} \otimes \overline{v}) = J_iJ(v)^{\sigma_i}(\overline{w} \otimes \overline{w}), \tag{75}$$

where we denote by $J(w)^{\sigma_i} = (\sigma_i \otimes \sigma_i)(J(w))$. Setting $J(w) = J(s_iv) = J_iJ(v)^{\sigma_i}$ proves our claim, since also $\mu_R(J(w)) = t_i\sigma_i(\mu_R(J(v)))$ has counit 1.

Thus, given a subgroup N of Σ_m, we can consider the Hopf subalgebra of H generated by R and $\{\overline{w} : w \in N\}$, which we shall denote by $R\#_\gamma N$. Since for any $w \in N$, $\Delta(\overline{w}) = J(w)(\overline{w} \otimes \overline{w}) \in (R\#_\gamma N) \otimes (R\#_\gamma N)$ we conclude that the subalgebra $R\#_\gamma N$ is a semisimple Hopf subalgebra of H.

Example 8.11. *Consider $H_{n,m} = R\#_\gamma\Sigma_m$ with generators as above and consider θ, the product of all $z_i's$, i.e. $\theta = z_1 \cdots z_{m-1}$. Let H be the subalgebra of $H_{n,m}$ generated by R and θ. We claim that H is equal to $R\#_\gamma\langle s\rangle$, where $s = (12 \cdots m)$ is the cycle of length m. Clearly, $\theta = \overline{s}$ and we claim that $\theta^k = \left(\prod_{i=1}^{k-1} \gamma(s^i, s)\right) \overline{s^k}$, for $2 \leq k \leq m$, since inductively, if $\theta^k = c_k\overline{s^k}$, for some $c_k \in R^\times$, then $\theta^{k+1} = c_k\overline{s^k}\,\overline{s} = c_k\gamma(s^k, s)\overline{s^{k+1}}$. Thus $H = R\#_\gamma\langle s\rangle$, as $\left(\prod_{i=1}^{k-1} \gamma(s^i, s)\right) \in R^\times$. Note that $\theta^m = \left(\prod_{i=1}^{m-1} \gamma(s^i, s)\right) =: t \in R^\times$. Hence $H \simeq R[\theta; \sigma]/\langle\theta^m - t\rangle$, where $\sigma = \sigma_s$. In particular, H is generated by $x_1, \dots, x_m$ and θ subject to $\theta x_i = x_{s(i)}\theta$ and $\theta^m = t$. While $\Delta(\theta) = J(s)(\theta \otimes \theta)$, with $J(s)$ as in Remark 8.10. Note that $\theta^{m-1} = \tilde{t}\,\overline{s^{m-1}}$, for $\tilde{t} = t\gamma(s^{m-1}, s)^{-1}$. Since $s^{-1} = s^{m-1}$ we obtain*

$$\theta^{m-1} = \tilde{t}\,\overline{s^{-1}} = \tilde{t}\, z_{m-1} \cdots z_1 = \tilde{t}S(\theta). \tag{76}$$

Hence $S(\theta) = \tilde{t}^{-1}\theta^{m-1} = t^{-1}\gamma(s^{m-1}, s)\theta^{m-1}$. The dimension of H is mn^m. For $m = 2$, we obtain $H' = H_{n,2}$.

Appendix A. Tensor Products

All vector spaces are considered over $\mathbb{K}$. Denote by $\mathrm{Hom}(U, V)$ the set of linear maps from U to V and $\mathrm{End}(U) = \mathrm{Hom}(U, U)$. Let $\{U_i\}_{i\in I}$ be a family of vector spaces. The **direct product** $\prod_{i\in I} U_i$ of this family is the cartesian product of the U_i's equipped with the componentwise addition and scalar multiplication. By definition the elements of $\prod_{i\in I} U_i$ are functions $f : I \mapsto \bigcup_{i\in I} U_i$ such that $f(i) \in U_i$ for any $i \in I$ and we will write $(x_i)_{i\in I}$ to represent the function $f(i) = x_i$. For each $j \in I$, there exist projections

$$\pi_j : \prod_{i\in I} U_i \to U_j \ , \ (x_i)_{i\in I} \mapsto x_j$$

which yields the isomorphism

$$\mathrm{Hom}(W, \prod_{i\in I} U_i) \longrightarrow \prod_{i\in I} \mathrm{Hom}(W, U_i) \tag{77}$$

$$f \longmapsto (\pi_i f)_{i\in I} \tag{78}$$

With this notation we have that the **direct sum** of the $\{U_i\}_{i\in I}$ of all functions that are non-zero just for finitely many $i \in I$.

$$\bigoplus_{i\in I} U_i := \{(x_i)_{i\in I} \mid \exists F \subseteq I \text{ such that } F \text{ is finite and } \forall i \in I \setminus F : x_i = 0\}.$$

For each $j \in I$, there exist an embedding

$$\epsilon_j : U_j \to \bigoplus_{i\in I} U_i \ , \ x \mapsto (\delta_{ij} x)_{i\in I}$$

which yields the isomorphism

$$\mathrm{Hom}(\bigoplus_{i\in I} U_i, W) \longrightarrow \prod_{i\in I} \mathrm{Hom}(U_i, W) \tag{79}$$
$$f \longmapsto (f\epsilon_i)_{i\in I} \tag{80}$$

A map $f : U \times V \to W$ is called **bilinear** if it is additive satisfying

$$f(\lambda u, v) = f(u, \lambda v) = \lambda f(u, v)$$

for all $u \in U, v \in V, \lambda \in \mathbb{K}$. The space of bilinear maps from $U \times V$ to a third vector space W is denoted by $\mathrm{Bil}(U \times V, W)$.

Definition A.1 (Tensor Product). *The tensor product of U and V is a pair (T, i_0), where T is a vector space and $i_0 : U \times V \to T$ is bilinear such that for any vector space W and $g \in \mathrm{Bil}(U \times V, W)$ there exists a unique linear map $h : T \to W$ with $g = hi_0$.*

$$\begin{tikzcd} U \times V \arrow[r, "g"] \arrow[dr, "i_0"'] & W \\ & T \arrow[u, "\overline{g}"'] \end{tikzcd}$$

In other words the map

$$\mathrm{Hom}(T, W) \longrightarrow \mathrm{Bil}(U \times V, W) \ , \ \ h \mapsto hi_0$$

is a bijection.

Obviously, if a tensor product T exists it is unique up to isomorphisms since for two pairs (T, i_0) and (T', j_0), there are unique linear maps $h : T \to T'$ and $h' : T' \to T$ such that $j_0 = hi_0$ and $i_0 = h'j_0$. Thus $i_0 = (h'h)i_0$ and $j_0 = (hh')j_0$. By the uniqueness of the factorization we get $id_T = h'h$ and $id_{T'} = hh'$.

Let $F = \bigoplus_{(u,v)\in U\times V} \mathbb{K} b_{u,v}$ be a vector space with basis $b_{u,v}$, for all $(u, v) \in U \times V$. Define the subspace S generated by all elements

$$\begin{aligned} &b_{u+u',v} - b_{u,v} - b_{u',v}, \\ &b_{u,v+v'} - b_{u,v} - b_{u,v'}, \\ &\lambda b_{u,v} - b_{\lambda u,v}, \\ &\lambda b_{u,v} - b_{u,\lambda v} \end{aligned}$$

for all $u, u' \in U, v, v' \in V, \lambda \in \mathbb{K}$. Set $T := F/S$ and denote by $u \otimes v$ the equivalence class of the element $b_{u,v}$ in T. Check that the map $i_0 : U \times V \to T$ sending $i_0(u, v) := u \otimes v$ is bilinear. Moreover any bilinear map $g : U \times V \to W$ extends to a linear map $\overline{g} : F \to W$ sending $b_{u,v} \mapsto g(u, v)$. Due to the bilinearity of g, $\overline{g}(S) = 0$ and hence we have an induced map $h : T = F/S \to W$. Thus

$$hi_0(u, v) = h(u \otimes v) = \overline{g}(b_{u,v}) = g(u, v).$$

The tensor product of U and V is denoted by $U \otimes V$. By definition we have the bijection

$$\mathrm{Hom}(U \otimes V, W) \simeq \mathrm{Bil}(U \times V, W) \tag{81}$$

Lemma A.2. *Let U, U', V, V' be vector spaces and let $f : U \to U'$ and $g : V \to V'$ be linear maps.*

(1) there exists a unique map

$$f \otimes g : U \otimes V \to U' \otimes V'$$

with $(f \otimes g)(u \otimes v) = f(u) \otimes g(v)$.

(2) if f and g are surjective, then $f \otimes g$ is surjective and $\mathrm{Ker} f \otimes g = \mathrm{Ker} f \otimes V + U \otimes \mathrm{Ker} g$.

Proof. (1) Define $f \times g : U \times V \to U' \otimes V'$ by $(u, v) \mapsto f(u) \otimes g(v)$, which is bilinear. By the universal property of the tensor product, there exists a unique map $f \otimes g : U \otimes V \to U' \otimes V'$.

(2) If $u \in \mathrm{Ker} f$ and $v \in \mathrm{Ker} g$ and $a \in U, b \in V$ are arbitrary, then

$$(f \otimes g)(u \otimes a + b \otimes v) = 0 \otimes g(a) + g(b) \otimes 0 = 0_{U' \otimes V'},$$

so $H := \mathrm{Ker} f \otimes V + U \otimes \mathrm{Ker} g \subseteq \mathrm{Ker} f \otimes g$. Hence $f \otimes g$ factors through H, i.e. there exists a (surjective) map $\phi : (U \otimes V)/H \to U' \otimes V'$ such that $f \otimes g = \phi \pi_H$, where π_H is the canonical projection. Define now a map from $U' \otimes V' \to (U \otimes V)/H$ as follows. For each pair $(x, y) \in U' \times V'$ choose a pair $(u, v) \in U \times V$ such that $f(u) = x$ and $g(v) = y$ and define the map $\psi : U' \times V' \to (U \otimes V)/H$ by $\psi(x, y) = u \otimes v + H$. This map is independent from the choice we made, because if (u_2, v_2) is another pair such that $f(u_2) = x$ and $g(v_2) = y$, then

$$u \otimes v - u_2 \otimes v_2 = (u - u_2) \otimes v + u_2 \otimes (v - v_2) \in H$$

since $f(u - u_2) = 0$ and $g(v - v_2) = 0$. Since this map is bilinear, by the universal property of the tensor product, there exists a (unique) map $\psi : U' \otimes V' \to (U \otimes V)/H$. This map satisfies $\pi_H = \psi(f \otimes g)$. Thus $\mathrm{Ker} f \otimes g \subseteq \mathrm{Ker} \pi_H = H$.

□

Proposition A.3. *Let U, V, W vector spaces and $(U_i)_{i \in I}$ and $(V_i)_{i \in I}$ be families of vector spaces.*

(1) $\mathrm{Hom}(U \otimes V, W) \simeq \mathrm{Hom}(U, \mathrm{Hom}(V, W))$ *by* $f \mapsto [u \mapsto [v \mapsto f(u \otimes v)]]$.

(2) $(U \otimes V) \otimes W \simeq U \otimes (V \otimes W)$ *with* $(u \otimes v) \otimes w \mapsto u \otimes (v \otimes W)$.

(3) $\tau_{U,V} : U \otimes V \simeq V \otimes U$ *with* $u \otimes v \mapsto v \otimes u$.

(4) $\left(\bigoplus_{i \in I} U_i\right) \otimes V \simeq \bigoplus_{i \in I} (U_i \otimes V)$ *with* $(u_i)_{i \in I} \otimes v \mapsto (u_i \otimes v)_{i \in I}$

(5) $\mathbb{K}x \otimes U \simeq U$ *with* $\lambda x \otimes u \mapsto \lambda u$.

(6) If X and Y are bases for U and V resp., then $\{x \otimes y \mid (x, y) \in X \times Y\}$ is a basis for $U \otimes V$. In particular $\dim(U \otimes V) \simeq \dim(U) \dim(V)$.

Proof. We leave (1-3) to the reader.

For (4) we get for all $j \in I$ and projections $\pi_j : \bigoplus_{i \in I} U_i \to U_j$ using Lemma A.2 the homomorphisms

$$(\pi_j \otimes I) : \left(\bigoplus_{i \in I} U_i\right) \otimes V \to U_j \otimes V.$$

Using the inclusions $\epsilon_j : U_j \otimes V \to \bigoplus_{i \in I} (U_i \otimes V)$ we have a linear map

$$\sum_{i \in I} \epsilon_i (\pi_i \otimes I) : \left(\bigoplus_{i \in I} U_i\right) \otimes V \to \bigoplus_{i \in I} (U_i \otimes V)$$

sending $(u_i)_{i \in I} \otimes v$ to $(u_i \otimes v)_{i \in I}$.

For (6) we use (5) and (4) to show that if $U = \bigoplus_{x \in X} \mathbb{K}x$ and $V = \bigoplus_{y \in Y} \mathbb{K}y$ then

$$U \otimes V = \left(\bigoplus_{x \in X} \mathbb{K}x\right) \otimes V \simeq \bigoplus_{x \in X} (\mathbb{K}x \otimes V) \simeq \bigoplus_{x \in X} \bigoplus_{y \in Y} (\mathbb{K}x \otimes \mathbb{K}y) \simeq \mathbb{K}^{X \times Y} \tag{82}$$

□

References

[1] K. Erdmann and M. J. Wildon, *Introduction to Lie Algebras*, 2006.

[2] R. G. Larson and D. E. Radford, *Semisimple cosemisimple Hopf algebras*, American Journal of Mathematics **110** (1988), no. 1, 187–195, DOI 10.2307/2374545.Zbl 0637.16006

[3] R. G. Larson and M. E. Sweedler, *An associative orthogonal bilinear form for Hopf algebras*, American Journal of Mathematics **91** (1969), 75–94, DOI 10.2307/2373270.Zbl 0179.05803

[4] C. Lomp, *Generalized Kac-Paljutkin algebras*, 2025.arXiv:2505.00645

[5] J. C. McConnell and J. C. Robson, *Noncommutative Noetherian rings. With the cooperation of L. W. Small.*, Reprinted with corrections from the 1987 original, Graduate Studies in Mathematics, vol. 30, American Mathematical Society (AMS), Providence, RI, 2001.Zbl 0980.16019