Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG
Algebra and Number Theory
Mathematics department

PD Dr. Ralf Holtkamp
Prof. Dr. C. Schweigert
Hopf algebras
Winter term 2014/2015

Sheet 2

Problem 1 (Quotient modules)**.** Let A be a unital $\mathbb{K}$-algebra[1] and M, N modules[2] over A.

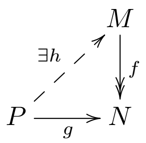
1. Let $U \subset M$ a submodule. Show that the quotient vector space M/U is endowed with a natural structure of an A-module by
$$a.(x + U) := (a.x) + U.$$
Show that the $\mathbb{K}$-linear map $\pi : M \to M/U, x \mapsto x + U$ is A-linear.

2. Let $f : M \to N$ be a morphism of A-modules and show that there is a unique A-linear map $F : M/U \to N$ with $F \circ \pi = f$, if $U \subset \ker(f)$.

3. Let $g : M \to N$ be a surjective morphism of A-modules. Show that $\ker(g)$ is a submodule of M and that the A-modules $M/\ker(g)$ and N are isomorphic.

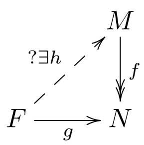
4. The algebra A can be itself considered as a left (resp. right) A-module (how?). A submodule of A is called a *left (resp. right) ideal*. If a subspace of A is both a left and a right ideal, we say that it is a *two sided ideal*. Show that the quotient vector space A/I is a $\mathbb{K}$-algebra with $(a+I)\cdot(b+I) := ab+I$, if and only if I is a two-sided ideal.

Problem 2 (Projective modules)**.** Let A be a unital $\mathbb{K}$-algebra. A (left) A-module P is *projective* if: for every pair of A-modules (M, N), every surjective A-linear map $f : M \to N$ and every A-linear map $g : P \to N$, there exists an A-linear map $h : P \to M$ such that: $g = f \circ h$. This is summarized by the following diagram:



1. A A-module is *free* if it is isomorphic to a (possibly infinite) direct sum of copies of A (ie if it admits an A-base). Prove that if a A-module is free, it is projective.

Solution. *Let F be a free A-module and let $X = (x_i)_{i \in I}$ an A-base of F. Consider a diagram:*



We might define h on the element of X (there is then one and only one way to extend it into a A-module map). For each element x in X we choose one pre-image of $g(x)$ by f and we define it to be the image of x by h. It is straightforward to check that this gives the A-module map what we wanted. Note that we used the axiom of choice. □

[1] If not otherwise specified, in the exercises sheets, an algebra is unital.
[2] If not otherwise specified, in the exercises sheets, a module is a left module.

2. In this question, we consider B the set of diagonal 2×2 matrices with coefficient in $\mathbb{K}$ endowed with the classical matrix product. It is obviously a $\mathbb{K}$-algebra. We consider P the sub-module of B which consist of matrices with their upper-lefter coefficient equal to 0. Is P free? Is P is projective?

Solution. The module P is not free, because if it would be, its $\mathbb{K}$-dimension would be a multiple of the $\mathbb{K}$-dimension of B and this is not the case. Let us show that P is a projective A-module. Let us denote by e_1 and e_2 the two elements of A given by:

$$e_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \textit{and} \quad e_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

and b the element of P given by:

$$p = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Let us consider the diagram:

$$\begin{array}{ccc} & & M \\ & & \downarrow{\scriptstyle f} \\ F & \xrightarrow[g]{} & N \end{array}$$

let m be a pre-image of $g(p)$ by f. We define $h(\lambda p) = \lambda e_2 m$. It is clearly a A-module map (because $e_1 e_2 = 0$) and we have: $f(h(p)) = f(e_2 m) = e_2 f(m) = e_2 g(p) = g(e_2 p) = g(p)$. Hence P is projective. □

3. Let P be a projective module. Construct a free module F and a surjective A-linear map $\pi : F \to P$. Prove that P is isomorphic to a direct summand of F.

Solution. We consider the free module F with A-base given by all the elements of P (this is very different from the module P) and the surjective A-map π defined by $\pi(x) = x$ for element of P (this is NOT the identity map!). We consider the diagram

$$\begin{array}{ccc} & {\scriptstyle \exists h} \nearrow & F \\ & & \downarrow{\scriptstyle \pi} \\ P & \xrightarrow[\mathrm{id}_P]{} & P \end{array}$$

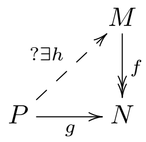
Let us prove that $F \simeq P \oplus \ker \pi$: the map ϕ_1 and ϕ_2 are clearly A-module maps and inverse from each others:

$$\begin{array}{rccc} \phi_1 : & F & \to & P \oplus \ker \pi \\ & x & \mapsto & (\pi(x), x - h \circ \pi(x)) \end{array} \qquad \begin{array}{rccc} \phi_2 : & P \oplus \ker \pi & \to & F \\ & (y_1, y_2)x & \mapsto & h(y_1) + y_2 \end{array}$$

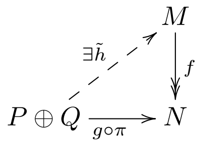
□

4. Prove that if a A-module is isomorphic to a direct summand of a free A-modules, then it is projective.

Solution. *Let P and Q be two A-modules such that $P \oplus Q = F$ is a free A-module. We will show that P is projective. Let us consider a diagram:*



We want to construct the map h. Let us denote by $\pi : P \oplus Q \to P$ (resp. $\iota : P \to P \oplus Q$) the canonical projection (resp. injection). Thanks to the first question, we have:



One easily check that defining $h = \tilde{h}\iota$ make the first diagram commutes (because $\iota \circ \pi = \mathrm{id}_P$). □

Problem 3. Let G be a finite group, $\mathbb{C}[G]$ its associated $\mathbb{C}$-algebra. A $\mathbb{C}[G]$-module is also called a representation of G (:= Darstellung von G).

1. Let M be a finite dimensional $\mathbb{C}[G]$-module. Prove that the $\mathbb{C}[G]$-module structure of M induces a group homomorphism $\rho_M : G \to \mathrm{End}(M)$. Prove the reciprocal statement: if V is a vector space and $\rho : G \to \mathrm{End}(V)$ a group homomorphism, prove that we can endow V with a structure of $\mathbb{C}[G]$-module.
2. Let M be a finite dimensional $\mathbb{C}[G]$-module and N a sub-module of N. Let us consider N' a supplement of M as a vector space (in general N' is NOT a $\mathbb{C}[G]$-module), and denote $p : M \to N'$ the projection on N'. By using the map
$$\pi := \frac{1}{\#G} \sum_{g \in G} \rho_M(g) \circ p \circ \rho_M(g)^{-1},$$
prove[3] that we can find a submodule N'' of M such that $M = N \oplus N''$.
3. Let M_1 and M_2 be two simple $\mathbb{C}[G]$-module and $f : M_1 \to M_2$ a morphism of $\mathbb{C}[G]$-modules. Suppose that f is different from 0. Prove that M_1 and M_2 are isomorphic.
4. With the same notations and the same hypothesis as the previous question, and by considering the eigenvalues of f, prove that f is an homothety[4].

Problem 4 (Garside structure of the braid group)**.** Let $n \geq 3$, in this problem, we will study some combinatorial aspect of the braid group presented in the lecture:

$$B_n = \left\langle \sigma_1, \dots, \sigma_{n-1} \;\middle|\; \begin{array}{ll} \sigma_i\sigma_j = \sigma_j\sigma_i & \text{for } 1 \leq i, j \leq n-1 \text{ and } |i-j| \geq 2 \\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} & \text{for } 1 \leq i \leq n-2 \end{array} \quad \sigma_i \right\rangle.$$

It is important to distinguish two notions: a *word*[5] in the letters $(\sigma_i)_{1 \leq i \leq n-1}$ and $(\sigma_j^{-1})_{1 \leq j \leq n-1}$ represents an *element* of B_n, but one element of B_n is represented by many (actually infinitely many) words. Two words are *equivalent* if they represent the same word. A word is *positive* if it is written only with the letters $(\sigma_i)_{1 \leq i \leq n-1}$. An element is *positive* if it can be represented by a positive word. Two words w and

[3] If A is an algebra, we say that a A-module N is *simple* if N does not contain non-trivial sub-modules. And that an object is *indecomposable* if it cannot be expressed as a direct sum of two sub-modules. This question shows that in the case of group algebras for finite groups, these two notions coincide (why?), this is NOT true in general.

[4] This is Schur's lemma. Schur (1875 – 1945) was a German mathematician.

[5] the empty word is a word, usually it is denoted by ε.

t are *positively equivalent* if they are positive and if one can go from one to the other by a sequence of positive words each of them obtained from the previous one by one of the following operations on letters (such a sequence is called a *chain*):

$$\begin{aligned} \sigma_i\sigma_j &\longrightarrow \sigma_j\sigma_i & &\text{for } 1 \le i,j \le n-1 \text{ and } |i-j| \ge 2, \\ \sigma_i\sigma_{i+1}\sigma_i &\longrightarrow \sigma_{i+1}\sigma_i\sigma_{i+1} & &\text{for } 1 \le i \le n-2, \\ \sigma_{i+1}\sigma_i\sigma_{i+1} &\longrightarrow \sigma_i\sigma_{i+1}\sigma_i & &\text{for } 1 \le i \le n-2, \end{aligned}$$

In this case we write $w \doteq t$ (and such a notation should indicate that both w and t are positive) and if a chain from w to t has length l, we say that w and t are l-close.

1. Define the notion of length on the set of words. Show we can define a notion of length on the set of positive element.
2. If w is a word, we denote by $\mathrm{rev}(w)$ the word obtained by reading w from right to left (eg if $w = \sigma_1\sigma_2\sigma_3$, then $\mathrm{rev}(w) = \sigma_3\sigma_2\sigma_1$). Let w and t be two words, show that $\mathrm{rev}(wt) = \mathrm{rev}(t)\mathrm{rev}(w)$. Prove that $w \doteq t$ if and only if $\mathrm{rev}(w) \doteq \mathrm{rev}(t)$.
3. We want to prove the following theorem:

   Theorem 1 (Garside, 1965). *Let i and j be two integers of $[1, n-1]$ and w and t two positive words such that $\sigma_i w \doteq \sigma_j t$.*

   - *If $i = j$, then $w \doteq t$.*
   - *If $|i-j| \ge 2$, then there exists a positive word z such that $w = \sigma_j z$ and $t = \sigma_j z$.*
   - *If $|i-j| = 1$, then there exists a positive word z such that $w = \sigma_j\sigma_i z$ and $t = \sigma_j\sigma_i z$.*

   If k and m are two integers, we denote by H_k the theorem restricted to the words of length equal to k, and we denote by H_k^m the theorem restricted to the words of length k and which are m-close.
4. Prove H_0 and H_1. Prove the H_k^0 and H_k^1 for every k.
5. Let k and m be integers greater than or equal to 2. We want to prove H_k^m. Let us suppose that $H_{k'}$ holds for every integer k' smaller than k and that $H_k^{m'}$ holds for every m' smaller than m. Let us consider two positive words w and t of length and i and j two integers in $[1, n-1]$. We suppose that $\sigma_i w \doteq \sigma_j t$ and that this two words are m-close. We consider a chain from $\sigma_i w$ to $\sigma_j t$ of length m. We can pick up an intermediate word $\sigma_p u$ in the chain such that $\sigma_i w$ and $\sigma_p u$ are m'-close with $m' < m$ and $\sigma_p u$ and $\sigma_j t$ are m''-close with $m'' < m$. List all the possible configurations of the indices i, j and p.
6. Choose two[6] of these configurations and prove that the corresponding statement of the theorem for the words w and t.
7. We now admit the theorem 1, prove that the same theorem holds when the multiplication by the generators are on the right of the words instead of the left.
8. Prove the following theorem:

   Theorem 2. *If $u \doteq v$, $r \doteq s$ and $uwr \doteq vts$, then $w \doteq t$.*

Actually Garside showed that, in the braid groups, there is a well defined notion of lower common multiple compatible with a certain order. This is a very strong and special property. From this property one can deduce many result on the braid groups.

[6] The proof are very similar for every configurations. . .

Problem 5. A functor $F : \mathcal{C} \to \mathcal{D}$ is *essentially surjective* if for every object W of $\mathcal{D}$, there exists an object U of $\mathcal{C}$ such that $F(U) \simeq W$.

A functor $F : \mathcal{C} \to \mathcal{D}$ is *faithful (resp. fully faithful)* if for every pair of objects (U_1, U_2) of C, the map $F : \mathrm{Hom}(U_1, U_2) \to \mathrm{Hom}(F(U_1), F(U_2))$ is injective (resp. bijective).

A functor $F : \mathcal{C} \to \mathcal{D}$ is an *equivalence of categories* if there exists a functor $G : \mathcal{D} \to \mathcal{C}$ and two natural isomorphisms $\eta : \mathrm{id}_{\mathcal{D}} \to F \circ G$ and $\theta : G \circ F \to \mathrm{id}_{\mathcal{C}}$.

In this problem, we intend to prove the following theorem:

Theorem 3. *A functor $F : \mathcal{C} \to \mathcal{D}$ is an equivalence of categories if and only if it is fully faithful and essentially surjective.*

1. We first suppose that F is an equivalence of categories. Prove that F is essentially surjective.

   Solution. Let W be an object of $\mathcal{D}$, we want to find an object U of $\mathcal{C}$ such that $F(U) \simeq U$. We consider $G(W)$, $\eta(U)$ gives us an isomorphism between W and $F(G(W))$, hence F is essentially surjective. □

2. Let U_1 and U_2 be two objects of $\mathcal{C}$. Show that θ (we use the notations introduced in the definitions) induces a bijection between $\mathrm{Hom}(G \circ F(U_1), G \circ F(U_2))$ and $\mathrm{Hom}(U_1, U_2)$. Prove that F is faithful. Prove that G is faithful.

   Solution. The maps $\theta(U_1)$ (resp. $\theta(U_2)$) is an ismorphism between $G \circ F(U_2)$ and U_2 (resp. $G \circ F(U_1)$ and U_1), hence the map:

$$\begin{array}{cccc} \tilde{\theta}: & \mathrm{Hom}(U_1, U_2) & \to & \mathrm{Hom}(G \circ F(U_1), G \circ F(U_2)) \\ & f & \mapsto & \theta(U_2)^{-1} \circ f \circ \theta(U_1) \end{array}$$

   is a bijection. We have the following commutative (why does it commutes ?) diagram:

$$\begin{array}{ccc} \mathrm{Hom}(U_1, U_2) & \xrightarrow{F} & \mathrm{Hom}(F(U_1), F(U_2)) \\ & \searrow^{\tilde{\theta}} & \downarrow G \\ & & \mathrm{Hom}(G \circ F(U_1), G \circ F(U_2)) \end{array}$$

   This proves that $F : \mathrm{Hom}(U_1, U_2) \to \mathrm{Hom}(F(U_1), F(U_2))$ is an injection. This is valid for every pair of objects (U_1, U_2), hence F is faithful. The functor G is faithful because it is just like F, an equivalence of category. □

3. Let U_1 and U_2 be two objects of $\mathcal{C}$ and $g : F(U_1) \to F(U_2)$ a morphism of $\mathcal{C}$. Compute $F(\theta(U_2) \circ G(g) \circ \theta(U_1)^{-1})$. Prove that F is fully faithful.

   Solution. As suggested by the previous question we will use the fact that G is faithful: Let us compute $G(F(\theta(U_2) \circ G(g) \circ \theta(U_1)^{-1}))$. With the previous notation it is equal to $G(F(th\tilde{e}ta^{-1}(G(d))))$. As previously said, the application induced by $G \circ F$ on $\mathrm{Hom}(U_1, U_2)$ is equal to $th\tilde{e}ta$. Hence we have:

$$G(F(\theta(U_2) \circ G(g) \circ \theta(U_1)^{-1})) = G(g).$$

   From the previous question, we know that G is faithful, hence $g = F(\theta(U_2) \circ G(g) \circ \theta(U_1)^{-1})$. This is valid for any pair of objects (U_1, U_2) and any morphism in $\mathrm{Hom}(U_1, U_2)$. This prove that F is fully faithful. □

4. We now suppose that F is essentially surjective and fully faithful. We want to define a functor $G : \mathcal{D} \to \mathcal{C}$ and two natural isomorphisms $\eta : \mathrm{id}_{\mathcal{D}} \to F \circ G$ and $\theta : G \circ F \to \mathrm{id}_{\mathcal{C}}$. For every object W of $\mathcal{D}$ we choose[7] an object $G(W)$ of $\mathcal{C}$ such that $F(G(W))$ is isomorphic to W and we choose[8] an isomorphism $\eta(W) : W \to F(G(W))$. If g is a morphism in the category $\mathcal{D}$, what is the "natural" definition of $G(g)$? Prove that with this definition, G is indeed a functor and $\eta : \mathrm{id}_{\mathcal{D}} \to F \circ G$ a natural transformation.

Solution. We want G to be a functor and η a natural transformation. This means in particluar, that for any pair of objects (W_1, W_2) and any morphism in $\mathrm{Hom}(W_1, W_2)$*, the following diagram should commute:*

$$\begin{array}{ccc} W_1 & \xrightarrow{\eta(W_1)} & F(G(W_1)) \\ \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle F(G(g))} \\ W_2 & \xrightarrow{\eta(W_2)} & F(G(W_2)). \end{array}$$

Since the application induced by F on $\mathrm{Hom}(U_1, U_2)$ *is bijective and the maps $\eta(W_1)$ and $\eta(W_2)$ are isomorphisms, we can define: $G(g) = F^{-1}(\eta(W_2) \circ g \circ \eta(W_1)^{-1})$. With this definition G is a functor. Indeed, we have $G(\mathrm{id}_{W_1}) = \mathrm{id}_{G(W_1)} if$ and if $g_1 : W_1 \to W_2$ and $g_2 : W_2 \to W_3$:*

$$\begin{aligned} G(g_2 \circ g_1) &= F^{-1}(\eta(W_3) \circ g_2 \circ g_1 \eta(W_1)^{-1}) \\ &= F^{-1}(\eta(W_3) \circ g_2 \eta(W_2)^{-1} \circ \eta(W_2) \circ g_1 \eta(W_1)^{-1}) \\ &= F^{-1}(\eta(W_3) \circ g_2 \eta(W_2)^{-1}) \circ F^{-1}(\eta(W_2) \circ g_1 \eta(W_1)^{-1}) \\ &= G(g_2) \circ G(g_1). \end{aligned}$$

(Be careful with the different meaning of F^{-1}). furthermore η is a natural transformation (because we did everything for it), and even a natural isomorphism between $\mathrm{id}_{\mathcal{D}}$ and $F \circ G$. □

5. What is the "natural" definition of $\theta : G \circ F \to \mathrm{id}_{\mathcal{C}}$? Prove that F is an equivalence of category.

Solution. For each object U of $\mathcal{C}$, we should define a morphism $\theta(U)$ from $G \circ F(U)$ to U such that all the squares

$$\begin{array}{ccc} G \circ F(U_1) & \xrightarrow{\theta(W_1)} & F(G(W_1)) \\ {\scriptstyle F \circ G(f)}\downarrow & & \downarrow{\scriptstyle f} \\ G \circ F(U_2) & \xrightarrow{\theta(U_2)} & U_2 \end{array}$$

commutes. The natural way to define $\theta(U)$ is to use, once more, the fact that F is fully faithful: it induces a bijection between $\mathrm{Hom}(G \circ F(U), U)$ *and* $\mathrm{Hom}(F \circ G \circ F(U), F(U))$*. Hence we define: $\theta(U) = F^{-1}(\eta(F(U))^{-1})$. With this definition, η is clearly a natural isomorphisms between $\mathrm{id}_{\mathcal{C}}$ and $G \circ F$.* □

[7] We use the axiom of choice.
[8] We use it again.