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
$$a.(x+U) := (a.x) + U \quad .$$
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:

$$\begin{tikzcd}
 & M \arrow[d, "f"] \\
P \arrow[ur, dashed, "\exists h"] \arrow[r, "g"'] & N
\end{tikzcd}$$

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

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?

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.

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

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.

[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. 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 notion: 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 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*):

$$\begin{array}{rll} \sigma_i\sigma_j & \longrightarrow \sigma_j\sigma_i & \text{for } 1 \leq i,j \leq n-1 \text{ and } |i-j| \geq 2, \\ \sigma_i\sigma_{i+1}\sigma_i & \longrightarrow \sigma_{i+1}\sigma_i\sigma_{i+1} & \text{for } 1 \leq i \leq n-2, \\ \sigma_{i+1}\sigma_i\sigma_{i+1} & \longrightarrow \sigma_i\sigma_{i+1}\sigma_i & \text{for } 1 \leq i \leq n-2, \end{array}$$

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 $|i-j| \geq 2$, 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.

[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.

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.

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.

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.

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.

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.

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

[6] The proof are very similar for every configurations...
[7] We use the axiom of choice.
[8] We use it again.